SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 12 November 2025

Generated on 12 November 2025

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-2025-62596	Youki is a container runtime written in Rust. In versions 0.5.6 and below, youki's apparmor handling performs insufficiently strict write-target validation, and when combined with path substitution during pathname resolution, can allow writes to unintended procfs locations. While resolving a path component-by-component, a shared-mount race can substitute intermediate components and redirect the final target. This issue is fixed in version 0.5.7.	10.0	More Details
CVE-2025-49372	Improper Control of Generation of Code ('Code Injection') vulnerability in VillaTheme HAPPY happy-helpdesk-support-ticket-system allows Remote Code Inclusion.This issue affects HAPPY: from n/a through <= 1.0.7.	10.0	More Details
CVE-2025-64180	Manager-io/Manager is accounting software. In Manager Desktop and Server versions 25.11.1.3085 and below, a critical vulnerability permits unauthorized access to internal network resources. The flaw lies in the fundamental design of the DNS validation mechanism. A Time-of-Check Time-of-Use (TOCTOU) condition that allows attackers to bypass network isolation and access internal services, cloud metadata endpoints, and protected network segments. The Desktop edition requires no authentication; the Server edition requires only standard authentication. This issue is fixed in version 25.11.1.3086.	10.0	More Details
CVE-2025-	Multiple SQL injection vulnerabilitites in ycf1998 money-pos system before commit 11f276bd20a41f089298d804e43cb1c39d041e59 (2025-09-14) allows a remote	10.0	More Details

63689	attacker to execute arbitrary code via the orderby parameter		
CVE-2025-62161	Youki is a container runtime written in Rust. In versions 0.5.6 and below, the initial validation of the source /dev/null is insufficient, allowing container escape when youki utilizes bind mounting the container's /dev/null as a file mask. This issue is fixed in version 0.5.7.	10.0	More Details
CVE-2025-10230	A flaw was found in Samba, in the front-end WINS hook handling: NetBIOS names from registration packets are passed to a shell without proper validation or escaping. Unsanitized NetBIOS name data from WINS registration packets are inserted into a shell command and executed by the Samba Active Directory Domain Controller’s wins hook, allowing an unauthenticated network attacker to achieve remote command execution as the Samba process.	10.0	More Details
CVE-2025-42890	SQL Anywhere Monitor (Non-GUI) baked credentials into the code,exposing the resources or functionality to unintended users and providing attackers with the possibility of arbitrary code execution.This could cause high impact on confidentiality integrity and availability of the system.	10.0	More Details
CVE-2025-6327	Unrestricted Upload of File with Dangerous Type vulnerability in KingAddons.com King Addons for Elementor king-addons allows Upload a Web Shell to a Web Server.This issue affects King Addons for Elementor: from n/a through <= 51.1.36.	10.0	More Details
CVE-2025-53283	Unrestricted Upload of File with Dangerous Type vulnerability in borisolhor Drop Uploader for CF7 - Drag&Drop File Uploader Addon drop-uploader-for-contact-form-7-dragdrop-file-uploader-addon allows Upload a Web Shell to a Web Server.This issue affects Drop Uploader for CF7 - Drag&Drop File Uploader Addon: from n/a through <= 2.4.1.	10.0	More Details
CVE-2025-12539	The TNC Toolbox: Web Performance plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.2. This is due to the plugin storing cPanel API credentials (hostname, username, and API key) in files within the web-accessible wp-content directory without adequate protection in the "Tnc_Wp_Toolbox_Settings::save_settings" function. This makes it possible for unauthenticated attackers to retrieve these credentials and use them to interact with the cPanel API, which can lead to arbitrary file uploads, remote code execution, and full compromise of the hosting environment.	10.0	More Details
CVE-2025-55108	The Control-M/Agent is vulnerable to unauthenticated remote code execution, arbitrary file read and write and similar unauthorized actions when mutual SSL/TLS authentication is not enabled (i.e. in the default configuration). NOTE: The vendor believes that this vulnerability only occurs when documented security best practices are not followed. BMC has always strongly recommended to use security best practices such as configuring SSL/TLS between Control-M Server and Agent.	10.0	More Details
CVE-2025-63601	Snipe-IT before version 8.3.3 contains a remote code execution vulnerability that allows an authenticated attacker to upload a malicious backup file containing arbitrary files and execute system commands.	9.9	More Details
CVE-2025-55343	Quipux 4.0.1 through e1774ac allows authenticated users to conduct SQL injection attacks via busqueda/busqueda.php txt_depe_codi, busqueda/busqueda.php txt_usua_codi, anexos_lista.php radi_temp, Administracion/listas/formArea_ajax.php codDepe, Administracion/listas/formDepeHijo_ajax.php codDepe, Administracion/listas/formDepePadre_ajax.php codInst, asociar_documentos/asociar_borrar_referencia.php radi_nume, asociar_documentos/asociar_documento_buscar_query.php radi_nume, asociar_documentos/asociar_documento_grabar.php txt_radi_nume, asociar_documentos/asociar_documento radi_nume, radicacion/buscar_usuario.php buscar_tipo, radicacion/formArea_ajax.php	9.9	More Details

	codDepe, radicacion/formDepeHijo_ajax.php codDepe, radicacion/formDepePadre_ajax.php codInst, radicacion/ver_datos_usuario.php destinatorio, reportes/reporte_TraspasoDocFisico.php verrad, tx/datos_imprimir_sobre.php txt_usua_codi, tx/datos_imprimir_sobre.php nume_radi_temp, tx/revertir_firma_digital_grabar.php txt_radi_nume, tx/tx_borrar_opcion_imp.php codigo_opc, tx/tx_realizar_tx.php txt_radicados, tx/tx_seguridad_documentos.php txt_radicados, or uploadFiles/cargar_doc_digitalizado_paginador.php txt_depe_codi.		
CVE-2025-62016	Unrestricted Upload of File with Dangerous Type vulnerability in hogash Kallyas kallyas.This issue affects Kallyas: from n/a through <= 4.22.0.	9.9	More Details
CVE-2025-62047	Unrestricted Upload of File with Dangerous Type vulnerability in Case-Themes Case Addons case-addons.This issue affects Case Addons: from n/a through < 1.3.0.	9.9	More Details
CVE-2025-13032	Double fetch in sandbox kernel driver in Avast/AVG Antivirus <25.3 on windows allows local attacker to escalate privelages via pool overflow.	9.9	More Details
CVE-2025-62065	Unrestricted Upload of File with Dangerous Type vulnerability in Rometheme RTMKit rometheme-for-elementor.This issue affects RTMKit: from n/a through <= 1.6.5.	9.9	More Details
CVE-2025-42887	Due to missing input sanitation, SAP Solution Manager allows an authenticated attacker to insert malicious code when calling a remote-enabled function module. This could provide the attacker with full control of the system hence leading to high impact on confidentiality, integrity and availability of the system.	9.9	More Details
CVE-2025-53586	Deserialization of Untrusted Data vulnerability in NooTheme WeMusic noo-wemusic allows Object Injection.This issue affects WeMusic: from n/a through <= 1.9.1.	9.8	More Details
CVE-2025-6325	Incorrect Privilege Assignment vulnerability in KingAddons.com King Addons for Elementor king-addons allows Privilege Escalation.This issue affects King Addons for Elementor: from n/a through <= 51.1.36.	9.8	More Details
CVE-2025-60195	Incorrect Privilege Assignment vulnerability in Vito Peleg Atarim atarim-visual-collaboration allows Privilege Escalation.This issue affects Atarim: from n/a through <= 4.2.	9.8	More Details
CVE-2025-53252	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in zozothemes Zegen zegen allows PHP Local File Inclusion.This issue affects Zegen: from n/a through <= 1.1.9.	9.8	More Details
CVE-2025-62064	Authentication Bypass Using an Alternate Path or Channel vulnerability in Elated-Themes Search & Go search-and-go allows Password Recovery Exploitation.This issue affects Search & Go: from n/a through <= 2.7.	9.8	More Details
CVE-2025-12735	The expr-eval library is a JavaScript expression parser and evaluator designed to safely evaluate mathematical expressions with user-defined variables. However, due to insufficient input validation, an attacker can pass a crafted variables object into the evaluate() function and trigger arbitrary code execution.	9.8	More Details
CVE-2025-27918	An issue was discovered in AnyDesk before 9.0.0. It has an integer overflow and resultant heap-based buffer overflow via a UDP packet during processing of an Identity user image within the Discovery feature, or when establishing a connection between any two clients.	9.8	More Details

CVE-2025-12352	The Gravity Forms plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the copy_post_image() function in all versions up to, and including, 2.9.20. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. This only impacts sites that have allow_url_fopen set to `On`, the post creation form enabled along with a file upload field for the post	9.8	More Details
CVE-2025-11749	The AI Engine plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.1.3 via the /mcp/v1/ REST API endpoint that exposes the 'Bearer Token' value when 'No-Auth URL' is enabled. This makes it possible for unauthenticated attackers to extract the bearer token, which can be used to gain access to a valid session and perform many actions like creating a new administrator account, leading to privilege escalation.	9.8	More Details
CVE-2025-12866	EIP Plus developed by Hundred Plus has a Weak Password Recovery Mechanism vulnerability, allowing unauthenticated remote attacker to predict or brute-force the 'forgot password' link, thereby successfully resetting any user's password.	9.8	More Details
CVE-2025-12868	New Site Server developed by CyberTutor has a Use of Client-Side Authentication vulnerability, allowing unauthenticated remote attackers to modify the frontend code to gain administrator privileges on the website.	9.8	More Details
CVE-2025-11170	The WP移行専用プラグイン for CPI plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the Cpiwm_Import_Controller::import function in all versions up to, and including, 1.0.2. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-11457	The EasyCommerce – AI-Powered, Fast & Beautiful WordPress Ecommerce Plugin plugin for WordPress is vulnerable to Privilege Escalation in versions 0.9.0-beta2 to 1.5.0. This is due to the /easycommerce/v1/orders REST API endpoint not properly restricting the ability for users to select roles during registration. This makes it possible for unauthenticated attackers to gain administrator-level access to a vulnerable site.	9.8	More Details
CVE-2025-12813	The Holiday class post calendar plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 7.1 via the 'contents' parameter. This is due to a lack of sanitization of user-supplied data when creating a cache file. This makes it possible for unauthenticated attackers to execute code on the server.	9.8	More Details
CVE-2025-8324	Zohocorp ManageEngine Analytics Plus versions 6170 and below are vulnerable to Unauthenticated SQL Injection due to the improper filter configuration.	9.8	More Details
CVE-2025-53242	Deserialization of Untrusted Data vulnerability in VictorThemes Seil seil allows Object Injection.This issue affects Seil: from n/a through <= 1.7.1.	9.8	More Details
CVE-2025-60724	Heap-based buffer overflow in Microsoft Graphics Component allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2025-52773	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in hiecor HieCOR Payment Gateway Plugin hcv4-payment-gateway allows SQL Injection.This issue affects HieCOR Payment Gateway Plugin: from n/a through <= 1.5.11.	9.8	More Details
CVE-2025-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Mikado-Themes Dør dor allows PHP Local	9.8	More

39466	File Inclusion.This issue affects Dør: from n/a through <= 2.4.		Details
CVE-2025-20354	A vulnerability in the Java Remote Method Invocation (RMI) process of Cisco Unified CCX could allow an unauthenticated, remote attacker to upload arbitrary files and execute arbitrary commands with root permissions on an affected system. This vulnerability is due to improper authentication mechanisms that are associated to specific Cisco Unified CCX features. An attacker could exploit this vulnerability by uploading a crafted file to an affected system through the Java RMI process. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root.	9.8	More Details
CVE-2025-61304	OS command injection vulnerability in Dynatrace ActiveGate ping extension up to 1.016 via crafted ip address.	9.8	More Details
CVE-2025-47151	A type confusion vulnerability exists in the lasso_node_impl_init_from_xml functionality of Entr'ouvert Lasso 2.5.1 and 2.8.2. A specially crafted SAML response can lead to an arbitrary code execution. An attacker can send a malformed SAML response to trigger this vulnerability.	9.8	More Details
CVE-2025-63334	PocketVJ CP PocketVJ-CP-v3 pvj version 3.9.1 contains an unauthenticated remote code execution vulnerability in the submit_opacity.php component. The application fails to sanitize user input in the opacityValue POST parameter before passing it to a shell command, allowing remote attackers to execute arbitrary commands with root privileges on the underlying system.	9.8	More Details
CVE-2025-49393	Deserialization of Untrusted Data vulnerability in Fetch Designs Sign-up Sheets sign-up-sheets allows Object Injection.This issue affects Sign-up Sheets: from n/a through <= 2.3.2.	9.8	More Details
CVE-2025-64163	DataEase is an open source data visualization analysis tool. In versions 2.10.14 and below, the vendor added a blacklist to filter ldap:// and ldaps://. However, omission of protection for the dns:// protocol results in an SSRF vulnerability. This issue is fixed in version 2.10.15.	9.8	More Details
CVE-2025-64164	Dataease is an open source data visualization analysis tool. In versions 2.10.14 and below, DataEase did not properly filter when establishing JDBC connections to Oracle, resulting in a risk of JNDI injection (Java Naming and Directory Interface injection). This issue is fixed in version 2.10.15.	9.8	More Details
CVE-2025-32222	Improper Control of Generation of Code ('Code Injection') vulnerability in Widgetlogic.org Widget Logic widget-logic allows Code Injection.This issue affects Widget Logic: from n/a through <= 6.0.5.	9.8	More Details
CVE-2025-39463	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes Dessau dessau allows PHP Local File Inclusion.This issue affects Dessau: from n/a through < 1.9.	9.8	More Details
CVE-2025-39467	Path Traversal: '.../...//' vulnerability in Mikado-Themes Wanderland wanderland allows PHP Local File Inclusion.This issue affects Wanderland: from n/a through <= 1.7.1.	9.8	More Details
CVE-2025-39468	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in pantherius Modal Survey modal-survey.This issue affects Modal Survey: from n/a through <= 2.0.2.0.1.	9.8	More Details
CVE-2025-47588	Improper Control of Generation of Code ('Code Injection') vulnerability in acowebs Dynamic Pricing With Discount Rules for WooCommerce aco-woo-dynamic-pricing allows Code Injection.This issue affects Dynamic Pricing With Discount Rules for WooCommerce: from n/a through <= 4.5.9.	9.8	More Details

CVE-2025-48086	Deserialization of Untrusted Data vulnerability in wpdreams Ajax Search Lite ajax-search-lite allows Object Injection.This issue affects Ajax Search Lite: from n/a through <= 4.13.3.	9.8	More Details
CVE-2025-48089	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Rainbow-Themes Education WordPress Theme | HiStudy histudy allows SQL Injection.This issue affects Education WordPress Theme | HiStudy: from n/a through < 3.1.0.	9.8	More Details
CVE-2025-48290	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in bslthemes Kinsley kinsley allows PHP Local File Inclusion.This issue affects Kinsley: from n/a through <= 3.4.4.	9.8	More Details
CVE-2025-12674	The KiotViet Sync plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the create_media() function in all versions up to, and including, 1.8.5. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-48330	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Daman Jeet Real Time Validation for Gravity Forms real-time-validation-for-gravity-forms allows PHP Local File Inclusion.This issue affects Real Time Validation for Gravity Forms: from n/a through <= 1.7.0.	9.8	More Details
CVE-2025-49386	Deserialization of Untrusted Data vulnerability in Scott Reilly Preserve Code Formatting preserve-code-formatting allows Object Injection.This issue affects Preserve Code Formatting: from n/a through <= 4.0.1.	9.8	More Details
CVE-2025-63691	In pig-mesh In Pig version 3.8.2 and below, within the Token Management function under the System Management module, the token query interface (/api/admin/sys-token/page) has an improper permission verification issue, which leads to information leakage. This interface can be called by any user who has completed login authentication, and it returns the plaintext authentication Tokens of all users currently logged in to the system. As a result, ordinary users can obtain the administrator's authentication Token through this interface, thereby forging an administrator account, gaining the system's management permissions, and taking over the system.	9.6	More Details
CVE-2025-64689	In JetBrains YouTrack before 2025.3.104432 misconfiguration in the Junie could lead to exposure of the global Junie token	9.6	More Details
CVE-2025-20358	A vulnerability in the Contact Center Express (CCX) Editor application of Cisco Unified CCX could allow an unauthenticated, remote attacker to bypass authentication and obtain administrative permissions pertaining to script creation and execution. This vulnerability is due to improper authentication mechanisms in the communication between the CCX Editor and an affected Unified CCX server. An attacker could exploit this vulnerability by redirecting the authentication flow to a malicious server and tricking the CCX Editor into believing the authentication was successful. A successful exploit could allow the attacker to create and execute arbitrary scripts on the underlying operating system of an affected Unified CCX server, as an internal non-root user account.	9.4	More Details
CVE-2025-45378	Dell CloudLink, versions 8.0 through 8.1.2, contain vulnerability on restricted shell. A Privileged user with known password can break into command shell of CloudLink server and gain access of shell and escalate privilege, gain unauthorized access of system. If ssh is enabled with web credentials of server, attack is possible through network with known privileged user/password.	9.1	More Details

CVE-2025-64459	An issue was discovered in 5.1 before 5.1.14, 4.2 before 4.2.26, and 5.2 before 5.2.8. The methods `QuerySet.filter()`, `QuerySet.exclude()`, and `QuerySet.get()`, and the class `Q()`, are subject to SQL injection when using a suitably crafted dictionary, with dictionary expansion, as the `_connector` argument. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank cyberstan for reporting this issue.	9.1	More Details
CVE-2025-63690	In pig-mesh Pig versions 3.8.2 and below, when setting up scheduled tasks in the Quartz management function under the system management module, it is possible to execute any Java class with a parameterless constructor and its methods with parameter type String through reflection. At this time, the eval method in Tomcat's built-in class jakarta.el.ELProcessor can be used to execute commands, leading to a remote code execution vulnerability.	9.1	More Details
CVE-2025-46364	Dell CloudLink, versions prior to 8.1.1, contain a vulnerability where a privileged user with known password can run CLI Escape Vulnerability to gain control of system.	9.1	More Details
CVE-2025-64522	Soft Serve is a self-hostable Git server for the command line. Versions prior to 0.11.1 have a SSRF vulnerability where webhook URLs are not validated, allowing repository administrators to create webhooks targeting internal services, private networks, and cloud metadata endpoints. Version 0.11.1 fixes the vulnerability.	9.1	More Details
CVE-2025-12480	Triofox versions prior to 16.7.10368.56560, are vulnerable to an Improper Access Control flaw that allows access to initial setup pages even after setup is complete.	9.1	More Details
CVE-2025-56231	Tonec Internet Download Manager 6.42.41.1 and earlier suffers from Missing SSL Certificate Validation, which allows attackers to bypass update protections.	9.1	More Details
CVE-2025-63416	** exclusively-hosted-service ** A Stored Cross-Site Scripting (XSS) vulnerability in the chat functionality of the SelfBest platform 2023.3 allows authenticated low-privileged attackers to execute arbitrary JavaScript in the context of other users' sessions. This can be exploited to access administrative data and functions, leading to privilege escalation and full compromise of sensitive user data, as demonstrated by the ability to fetch and exfiltrate the contents of the /admin/users endpoint.	9.1	More Details
CVE-2025-58595	Authentication Bypass by Spoofing vulnerability in Saad Iqbal All In One Login change-wp-admin-login allows Identity Spoofing.This issue affects All In One Login: from n/a through <= 2.0.8.	9.1	More Details
CVE-2025-53214	Missing Authorization vulnerability in sertifier Sertifier Certificate & Badge Maker sertifier-certificates-open-badges allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sertifier Certificate & Badge Maker: from n/a through <= 1.21.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-11956	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Proliz Software Ltd. Co. OBS (Student Affairs Information System) allows Stored XSS.This issue affects OBS (Student Affairs Information System): before 25.0401.	8.9	More Details

CVE-2025-64109	Cursor is a code editor built for programming with AI. In versions and below, a vulnerability in the Cursor CLI Beta allowed an attacker to achieve remote code execution through the MCP (Model Context Protocol) server mechanism by uploading a malicious MCP configuration in .cursor/mcp.json file in a GitHub repository. Once a victim clones the project and opens it using Cursor CLI, the command to run the malicious MCP server is immediately executed without any warning, leading to potential code execution as soon as the command runs. This issue is fixed in version 2025.09.17-25b418f.	8.8	More Details
CVE-2025-5803	Missing Authorization vulnerability in e4jvikwp VikBooking Hotel Booking Engine & PMS vikbooking.This issue affects VikBooking Hotel Booking Engine & PMS: from n/a through <= 1.8.2.	8.8	More Details
CVE-2025-4519	The IDonate – Blood Donation, Request And Donor Management System plugin for WordPress is vulnerable to Privilege Escalation due to a missing capability check on the idonate_donor_password() function in versions 2.1.5 to 2.1.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to initiate a password reset for any user (including administrators) and elevate their privileges for full site takeover.	8.8	More Details
CVE-2025-64184	Dosage is a comic strip downloader and archiver. When downloading comic images in versions 3.1 and below, Dosage constructs target file names from different aspects of the remote comic (page URL, image URL, page content, etc.). While the basename is properly stripped of directory-traversing characters, the file extension is taken from the HTTP Content-Type header. This allows a remote attacker (or a Man-in-the-Middle, if the comic is served over HTTP) to write arbitrary files outside the target directory (if additional conditions are met). This issue is fixed in version 3.2.	8.8	More Details
CVE-2025-62630	Due to insufficient sanitization, an attacker can upload a specially crafted configuration file to traverse directories and achieve remote code execution with system-level permissions.	8.8	More Details
CVE-2025-58423	Due to insufficient sanitization, an attacker can upload a specially crafted configuration file to cause a denial-of-service condition, traverse directories, or read/write files, within the context of the local system account.	8.8	More Details
CVE-2025-12036	Out of bounds memory access in V8 in Google Chrome prior to 141.0.7390.122 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-11756	Use after free in Safe Browsing in Google Chrome prior to 141.0.7390.107 allowed a remote attacker who had compromised the renderer process to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-11205	Heap buffer overflow in WebGPU in Google Chrome prior to 141.0.7390.54 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-12485	Improper privilege management during pre-MFA cookie handling in Devolutions Server allows a low-privileged authenticated user to impersonate another account by replaying the pre-MFA cookie.This does not bypass the target account MFA verification step. This issue affects the following versions : * Devolutions Server 2025.3.2.0 through 2025.3.5.0 * Devolutions Server 2025.2.15.0 and earlier	8.8	More Details
CVE-2025-62035	Deserialization of Untrusted Data vulnerability in uxper Togo togo.This issue affects Togo: from n/a through < 1.0.4.	8.8	More Details

CVE-2025-62034	Incorrect Privilege Assignment vulnerability in uxper Togo togo.This issue affects Togo: from n/a through < 1.0.4.	8.8	More Details
CVE-2025-58619	Deserialization of Untrusted Data vulnerability in sbouey Falang multilanguage falang allows Object Injection.This issue affects Falang multilanguage: from n/a through <= 1.3.65.	8.8	More Details
CVE-2023-43000	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.5, iOS 16.6 and iPadOS 16.6, Safari 16.6. Processing maliciously crafted web content may lead to memory corruption.	8.8	More Details
CVE-2025-54719	Deserialization of Untrusted Data vulnerability in NooTheme Yogi - Health Beauty & Yoga noo-yogi allows Object Injection.This issue affects Yogi - Health Beauty & Yoga: from n/a through <= 2.9.2.	8.8	More Details
CVE-2025-53316	Cross-Site Request Forgery (CSRF) vulnerability in Shahjahan Jewel WP GDPR Cookie Consent wp-gdpr-cookie-consent allows Stored XSS.This issue affects WP GDPR Cookie Consent: from n/a through <= 1.0.0.	8.8	More Details
CVE-2025-53246	Missing Authorization vulnerability in Gaurav Aggarwal Backup and Move backup-and-move allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Backup and Move: from n/a through <= 0.1.	8.8	More Details
CVE-2025-49900	Incorrect Privilege Assignment vulnerability in bPlugins Advanced scrollbar advanced-scrollbar allows Privilege Escalation.This issue affects Advanced scrollbar: from n/a through <= 1.1.8.	8.8	More Details
CVE-2025-49394	Missing Authorization vulnerability in bPlugins Image Gallery block – Create and display photo gallery/photo album. 3d-image-gallery allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Image Gallery block – Create and display photo gallery/photo album.: from n/a through <= 1.0.7.	8.8	More Details
CVE-2025-48085	Cross-Site Request Forgery (CSRF) vulnerability in ZIPANG Simple Stripe simple-stripe allows Stored XSS.This issue affects Simple Stripe: from n/a through <= 0.9.17.	8.8	More Details
CVE-2025-48083	Cross-Site Request Forgery (CSRF) vulnerability in andriassundskard wpNamedUsers wpnamedusers allows Stored XSS.This issue affects wpNamedUsers: from n/a through <= 0.5.	8.8	More Details
CVE-2025-48078	Cross-Site Request Forgery (CSRF) vulnerability in Norbert Slick Google Map slick-google-map allows Stored XSS.This issue affects Slick Google Map: from n/a through <= 0.3.	8.8	More Details
CVE-2025-48077	Cross-Site Request Forgery (CSRF) vulnerability in nitinmaurya12 Block Country block-country allows Stored XSS.This issue affects Block Country: from n/a through <= 1.0.	8.8	More Details
CVE-2025-12556	An argument injection vulnerability exists in the affected product that could allow an attacker to execute arbitrary code within the context of the host machine.	8.8	More Details
CVE-2025-10968	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), CWE - 564 - SQL Injection: Hibernate vulnerability in GG Soft Software Services Inc. PaperWork allows Blind SQL Injection, SQL Injection.This issue affects PaperWork: from 6.1.0.9390 before 6.1.0.9398.	8.8	More Details
	Improper Authorization in Elastic Cloud Enterprise can lead to Privilege Escalation where the built-in readonly user can call APIs that should not be allowed. The list of APIs that are affected by this issue is: post:/platform/configuration/security/service-		

CVE-2025-37736	accounts delete:/platform/configuration/security/service-accounts/{user_id} patch:/platform/configuration/security/service-accounts/{user_id} post:/platform/configuration/security/service-accounts/{user_id}/keys delete:/platform/configuration/security/service-accounts/{user_id}/keys/{api_key_id} patch:/user post:/users post:/users/auth/keys delete:/users/auth/keys delete:/users/auth/keys/_all delete:/users/auth/keys/{api_key_id} delete:/users/{user_id}/auth/keys delete:/users/{user_id}/auth/keys/{api_key_id} delete:/users/{user_name} patch:/users/{user_name}	8.8	More Details
CVE-2025-12907	Insufficient validation of untrusted input in Devtools in Google Chrome prior to 140.0.7339.80 allowed a remote attacker to execute arbitrary code via user action in Devtools. (Chromium security severity: Low)	8.8	More Details
CVE-2025-12637	The Elastic Theme Editor plugin for WordPress is vulnerable to arbitrary file uploads due to a dynamic code generation feature in the process_theme function in all versions up to, and including, 0.0.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2024-32011	A vulnerability has been identified in Spectrum Power 4 (All versions < V4.70 SP12 Update 2). The affected application is vulnerable to run arbitrary commands via the user interface. This user interface can be used via the network and allows the execution of commands as administrative application user.	8.8	More Details
CVE-2025-62222	Improper neutralization of special elements used in a command ('command injection') in Visual Studio Code CoPilot Chat Extension allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2025-62220	Heap-based buffer overflow in Windows Subsystem for Linux GUI allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2025-59499	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2025-33186	NVIDIA AIStore contains a vulnerability in AuthN. A successful exploit of this vulnerability might lead to escalation of privileges, information disclosure, and data tampering.	8.8	More Details
CVE-2025-33000	Improper input validation for some Intel QuickAssist Technology before version 2.6.0 within Ring 3: User Applications may allow an escalation of privilege. System software adversary with an authenticated user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	8.8	More Details
CVE-2025-24838	Improper privilege management for some Intel(R) CIP software before version WIN_DCA_2.4.0.11001 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via network access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality	8.8	More Details

	(none), integrity (none) and availability (none) impacts.		
CVE-2025-24299	Improper input validation for some Intel(R) CIP software before version WIN_DCA_2.4.0.11001 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via network access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	8.8	More Details
CVE-2025-9223	Zohocorp ManageEngine Applications Manager versions 178100 and below are vulnerable to authenticated command injection vulnerability due to the improper configuration in the execute program action feature.	8.8	More Details
CVE-2025-12846	The Blocksy Companion plugin for WordPress is vulnerable to authenticated arbitrary file upload in all versions up to, and including, 2.1.19. This is due to insufficient file type validation detecting SVG files, allowing double extension files to bypass sanitization while being accepted as a valid SVG file. This makes it possible for authenticated attackers, with author level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2025-11168	The Mementor Core plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.2.5. This is due to plugin not properly handling the user switch back function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to elevate their privileges by accessing an administrator account through the switch back functionality.	8.8	More Details
CVE-2025-64492	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Versions 8.9.0 and below contain a time-based blind SQL Injection vulnerability. This vulnerability allows an authenticated attacker to infer data from the database by measuring response times, potentially leading to the extraction of sensitive information. It is possible for an attacker to enumerate database, table, and column names, extract sensitive data, or escalate privileges. This is fixed in version 8.9.1.	8.8	More Details
CVE-2025-64519	TorrentPier is an open source BitTorrent Public/Private tracker engine, written in php. In versions up to and including 2.8.8, an authenticated SQL injection vulnerability exists in the moderator control panel (`modcp.php`). Users with moderator permissions can exploit this vulnerability by supplying a malicious `topic_id` (`t`) parameter. This allows an authenticated moderator to execute arbitrary SQL queries, leading to the potential disclosure, modification, or deletion of any data in the database. Although it requires moderator privileges, it is still severe. A malicious or compromised moderator account can leverage this vulnerability to read, modify, or delete data. A patch is available at commit 6a0f6499d89fa5d6e2afa8ee53802a1ad11ece80.	8.8	More Details
CVE-2025-48065	Combodo iTop is a web based IT service management tool. Versions prior to 2.7.13 and 3.2.2 are vulnerable to cross-site scripting when a field with an error contains malicious content. Versions 2.7.13 and 3.2.2 protect rendered HTML content.	8.8	More Details
CVE-2025-47932	Combodo iTop is a web based IT service management tool. Versions prior to 2.7.13 and 3.2.2 are vulnerable to cross-site scripting when a dashboard is rendered via an AJAX call. Versions 2.7.13 and 3.2.2 sanitize the var responsible for the attack.	8.8	More Details
CVE-2025-12438	Use after free in Ozone in Google Chrome on Linux and ChromeOS prior to 142.0.7444.59 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details

CVE-2025-12432	Race in V8 in Google Chrome prior to 142.0.7444.59 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-12429	Inappropriate implementation in V8 in Google Chrome prior to 142.0.7444.59 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-47773	Combodo iTop is a web based IT service management tool. Versions prior to 2.7.13 and 3.2.2 are vulnerable to cross-site scripting when a dashboard is edited via an AJAX call. Versions 2.7.13 and 3.2.2 protect rendered HTML content.	8.8	More Details
CVE-2025-12865	U-Office Force developed by e-Excellence has a SQL Injection vulnerability, allowing authenticated remote attacker to inject arbitrary SQL commands to read, modify, and delete database contents.	8.8	More Details
CVE-2025-12864	U-Office Force developed by e-Excellence has a SQL Injection vulnerability, allowing authenticated remote attacker to inject arbitrary SQL commands to read, modify, and delete database contents.	8.8	More Details
CVE-2025-12161	The Smart Auto Upload Images plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the auto-image creation functionality in all versions up to, and including, 1.2.0. This makes it possible for authenticated attackers, with Contributor-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2025-12779	Improper handling of the authentication token in the Amazon WorkSpaces client for Linux, versions 2023.0 through 2024.8, may expose the authentication token for DCV-based WorkSpaces to other local users on the same client machine. Under certain circumstances, a local user may be able to extract another local user's authentication token from the shared client machine and access their WorkSpace. To mitigate this issue, users should upgrade to the Amazon WorkSpaces client for Linux version 2025.0 or later.	8.8	More Details
CVE-2025-9334	The Better Find and Replace – AI-Powered Suggestions plugin for WordPress is vulnerable to Limited Code Injection in all versions up to, and including, 1.7.7. This is due to insufficient input validation and restriction on the 'rtafar_ajax' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to call arbitrary plugin functions and execute code within those functions.	8.8	More Details
CVE-2025-21078	Use of insufficiently random value of secretKey in Smart Switch prior to version 3.7.68.6 allows adjacent attackers to access backup data from applications.	8.8	More Details
CVE-2025-62210	Improper neutralization of input during web page generation ('cross-site scripting') in Dynamics 365 Field Service (online) allows an authorized attacker to perform spoofing over a network.	8.7	More Details
CVE-2025-62211	Improper neutralization of input during web page generation ('cross-site scripting') in Dynamics 365 Field Service (online) allows an authorized attacker to perform spoofing over a network.	8.7	More Details
CVE-2025-64495	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. In versions 0.6.34 and below, the functionality that inserts custom prompts into the chat window is vulnerable to DOM XSS when 'Insert Prompt as Rich Text' is enabled, since the prompt body is assigned to the DOM sink .innerHtml without sanitisation. Any user with permissions to create prompts can abuse this to plant a payload that could be triggered by other users if they run the corresponding / command to insert the prompt. This issue is fixed in version 0.6.35.	8.7	More Details

CVE-2025-49145	Combodo iTop is a web based IT service management tool. In versions prior to 2.7.13 and 3.2.2, a user that has enough rights to create webhooks (mostly administrators) can drop the database. This is fixed in iTop 2.7.13 and 3.2.2 by verifying callback signature.	8.7	More Details
CVE-2025-12613	Versions of the package cloudinary before 2.7.0 are vulnerable to Arbitrary Argument Injection due to improper parsing of parameter values containing an ampersand. An attacker can inject additional, unintended parameters. This could lead to a variety of malicious outcomes, such as bypassing security checks, altering data, or manipulating the application's behavior. **Note:** Following our established security policy, we attempted to contact the maintainer regarding this vulnerability, but haven't received a response.	8.6	More Details
CVE-2025-12384	The Document Embedder – Embed PDFs, Word, Excel, and Other Files plugin for WordPress is vulnerable to unauthorized access/modification/loss of data in all versions up to, and including, 2.0.0. This is due to the plugin not properly verifying that a user is authorized to perform an action in the "bplde_save_document_library", "bplde_get_all", "bplde_get_single", and "bplde_delete_document_library" functions. This makes it possible for unauthenticated attackers to create, read, update, and delete arbitrary document_library posts.	8.6	More Details
CVE-2025-20343	A vulnerability in the RADIUS setting Reject RADIUS requests from clients with repeated failures on Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to cause Cisco ISE to restart unexpectedly. This vulnerability is due to a logic error when processing a RADIUS access request for a MAC address that is already a rejected endpoint. An attacker could exploit this vulnerability by sending a specific sequence of multiple crafted RADIUS access request messages to Cisco ISE. A successful exploit could allow the attacker to cause a denial of service (DoS) condition when Cisco ISE restarts.	8.6	More Details
CVE-2025-64512	Pdfminer.six is a community maintained fork of the original PDFMiner, a tool for extracting information from PDF documents. Prior to version 20251107, pdfminer.six will execute arbitrary code from a malicious pickle file if provided with a malicious PDF file. The `CMapDB._load_data()` function in pdfminer.six uses `pickle.loads()` to deserialize pickle files. These pickle files are supposed to be part of the pdfminer.six distribution stored in the `cmap/` directory, but a malicious PDF can specify an alternative directory and filename as long as the filename ends in `.pickle.gz`. A malicious, zipped pickle file can then contain code which will automatically execute when the PDF is processed. Version 20251107 fixes the issue.	8.6	More Details
CVE-2025-64484	OAuth2-Proxy is an open-source tool that can act as either a standalone reverse proxy or a middleware component integrated into existing reverse proxy or load balancer setups. In versions prior to 7.13.0, all deployments of OAuth2 Proxy in front of applications that normalize underscores to dashes in HTTP headers (e.g., WSGI-based frameworks such as Django, Flask, FastAPI, and PHP applications). Authenticated users can inject underscore variants of X-Forwarded-* headers that bypass the proxy’s filtering logic, potentially escalating privileges in the upstream app. OAuth2 Proxy authentication/authorization itself is not compromised. The problem has been patched with v7.13.0. By default all specified headers will now be normalized, meaning that both capitalization and the use of underscores (_) versus dashes (-) will be ignored when matching headers to be stripped. For example, both `X-Forwarded-For` and `X_Forwarded-for` will now be treated as equivalent and stripped away. For those who have a rational that requires keeping a similar looking header and not stripping it, the maintainers introduced a new configuration field for Headers managed through the AlphaConfig called `InsecureSkipHeaderNormalization`. As a workaround, ensure filtering and processing logic in upstream services don't treat underscores and hyphens in	8.5	More Details

	Headers the same way.		
CVE-2025-48055	Combodo iTop is a web based IT service management tool. In versions prior to 3.2.2, when displaying content in a browse brick in the user portal, a cross-site scripting attack can occur. This is fixed in versions 3.2.2 and 3.3.0.	8.5	More Details
CVE-2025-28953	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in axiomthemes smart SEO smartSEO allows SQL Injection.This issue affects smart SEO: from n/a through <= 4.0.	8.5	More Details
CVE-2025-60239	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Codexpert, Inc CoSchool LMS coschool allows Blind SQL Injection.This issue affects CoSchool LMS: from n/a through <= 1.4.3.	8.5	More Details
CVE-2025-10714	AXIS Optimizer was vulnerable to an unquoted search path vulnerability, which could potentially lead to privilege escalation within Microsoft Windows operating system. This vulnerability can only be exploited if the attacker has access to the local Windows machine and sufficient access rights (administrator) to write data into the installation path of AXIS Optimizer.	8.4	More Details
CVE-2025-30479	Dell CloudLink, versions prior to 8.2, contain a vulnerability where a privileged user with known password can run command injection to gain control of system.	8.4	More Details
CVE-2025-45379	Dell CloudLink, versions prior to 8.2, contain a vulnerability where a privileged user with known password can run command injection from console to gain shell access of system.	8.4	More Details
CVE-2025-64456	In JetBrains ReSharper before 2025.2.4 missing signature verification in DPA Collector allows local privilege escalation	8.4	More Details
CVE-2025-10907	An arbitrary file upload vulnerability exists in multiple WSO2 products due to insufficient validation of uploaded content and destination in SOAP admin services. A malicious actor with administrative privileges can upload a specially crafted file to a user-controlled location within the deployment. Successful exploitation may lead to remote code execution (RCE) on the server, depending on how the uploaded file is processed. By default, this vulnerability is only exploitable by users with administrative access to the affected SOAP services.	8.4	More Details
CVE-2025-11093	An arbitrary code execution vulnerability exists in multiple WSO2 products due to insufficient restrictions in the GraalJS and NashornJS Script Mediator engines. Authenticated users with elevated privileges can execute arbitrary code within the integration runtime environment. By default, access to these scripting engines is limited to administrators in WSO2 Micro Integrator and WSO2 Enterprise Integrator, while in WSO2 API Manager, access extends to both administrators and API creators. This may allow trusted-but-privileged users to perform unauthorized actions or compromise the execution environment.	8.4	More Details
CVE-2025-57130	An Incorrect Access Control vulnerability in the user management component of ZwiiCMS up to v13.6.07 allows a remote, authenticated attacker to escalate their privileges. By sending a specially crafted HTTP request, a low-privilege user can access and modify the profile data of any other user, including administrators.	8.3	More Details
CVE-2025-64490	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Versions 7.14.7 and prior, 8.0.0-beta.1 through 8.9.0 allow a low-privileged user with a restrictive role to view and create work items through the Resource Calendar and project screens, even when the related modules (Projects, Project Tasks, Tasks, Leads, Accounts, Meetings, Calls) are explicitly set to Disabled/None in Role Management. This indicates inconsistent ACL/RBAC	8.3	More Details

	enforcement across modules and views, resulting in unauthorized data exposure and modification. This issue is fixed in versions 7.14.8 and 8.9.1.		
CVE-2025-64489	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Versions 7.14.7 and prior, 8.0.0-beta.1 through 8.9.0 contain a privilege escalation vulnerability where user sessions are not invalidated upon account deactivation. An inactive user with an active session can continue to access the application and, critically, can self-reactivate their account. This undermines administrative controls and allows unauthorized persistence. This issue is fixed in versions 7.14.8 and 8.9.1.	8.3	More Details
CVE-2025-48090	Path Traversal: '.../...//' vulnerability in CocoBasic Blanka - One Page WordPress Theme blanka-wp allows PHP Local File Inclusion.This issue affects Blanka - One Page WordPress Theme: from n/a through < 1.5.	8.2	More Details
CVE-2025-30255	Out-of-bounds write for some Intel(R) PROSet/Wireless WiFi Software for Windows before version 23.160 within Ring 2: Device Drivers may allow a denial of service. Unprivileged software adversary with an unauthenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via adjacent access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (low) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (high) impacts.	8.2	More Details
CVE-2025-58207	Missing Authorization vulnerability in WP Messiah Ai Image Alt Text Generator for WP ai-image-alt-text-generator-for-wp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ai Image Alt Text Generator for WP: from n/a through <= 1.1.5.	8.2	More Details
CVE-2025-32091	Incorrect default permissions in some firmware for the Intel(R) Arc(TM) B-series GPUs within Ring 1: Device Drivers may allow an escalation of privilege. System software adversary with a privileged user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are not present with special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	8.2	More Details
CVE-2025-35971	Out-of-bounds write for some Intel(R) PROSet/Wireless WiFi Software for Windows before version 23.160 within Ring 2: Device Drivers may allow a denial of service. Unprivileged software adversary with an unauthenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via adjacent access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (low) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (high) impacts.	8.2	More Details
CVE-2025-60198	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in dedalx Saxon - Viral Content Blog & Magazine Marketing WordPress Theme saxon allows PHP Local File Inclusion.This issue affects Saxon - Viral Content Blog & Magazine Marketing WordPress Theme: from n/a through <= 1.9.3.	8.2	More Details
CVE-2025-60199	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in dedalx InHype - Blog & Magazine WordPress Theme inhype allows PHP Local File Inclusion.This issue affects InHype - Blog &	8.2	More Details

	Magazine WordPress Theme: from n/a through <= 1.5.2.		
CVE-2025-27919	An issue was discovered in AnyDesk through 9.0.4. A remotely connected user with the "Control my device" permission can manipulate remote AnyDesk settings and create a password for the Full Access profile without needing confirmation from the counterparty. Consequently, the attacker can later connect without this counterparty confirmation.	8.2	More Details
CVE-2025-60197	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in owenr88 Simple Contact Forms simple-contact-forms allows PHP Local File Inclusion.This issue affects Simple Contact Forms: from n/a through <= 1.6.4.	8.2	More Details
CVE-2025-62014	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ApusTheme ITok itok.This issue affects ITok: from n/a through <= 1.1.42.	8.1	More Details
CVE-2025-62045	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CodexThemes TheGem Theme Elements (for WPBakery) thegem-elements.This issue affects TheGem Theme Elements (for WPBakery): from n/a through <= 5.10.5.1.	8.1	More Details
CVE-2025-39465	Missing Authorization vulnerability in flippercode Advanced Google Maps wp-google-map-gold allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Advanced Google Maps: from n/a through <= 5.8.4.	8.1	More Details
CVE-2025-12497	The Premium Portfolio Features for Phlox theme plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.3.10 via the 'args[extra_template_path]' parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	8.1	More Details
CVE-2025-62055	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Academist academist.This issue affects Academist: from n/a through < 1.3.	8.1	More Details
CVE-2025-9408	System call entry on Cortex M (and possibly R and A, but I think not) has a race which allows very practical privilege escalation for malicious userspace processes.	8.1	More Details
CVE-2025-11959	Files or Directories Accessible to External Parties, Exposure of Private Personal Information to an Unauthorized Actor vulnerability in Premierturk Information Technologies Inc. Excavation Management Information System allows Footprinting, Functionality Misuse.This issue affects Excavation Management Information System: before v.10.2025.01.	8.1	More Details
CVE-2025-62067	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Elated-Themes Savory savory.This issue affects Savory: from n/a through <= 2.5.	8.1	More Details
CVE-2025-11521	The Astra Security Suite – Firewall & Malware Scan plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient validation of remote URLs for zip downloads and an easily guessable key in all versions up to, and including, 0.2. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.1	More Details
CVE-2025-	alexusmai laravel-file-manager 3.3.1 is vulnerable to Cross Site Scripting (XSS). The application permits user-controlled upload, create, and rename of files to HTML and	8.1	More

63307	SVG types and serves those files inline without adequate content-type validation or output sanitization.		Details
CVE-2025-5483	The LC Wizard plugin for WordPress is vulnerable to Privilege Escalation due to a missing capability check in the ghl-wizard/inc/wp_user.php file in versions 1.2.10 to 1.3.0. This makes it possible for unauthenticated attackers to create new user accounts with the administrator role when the PRO functionality is enabled.	8.1	More Details
CVE-2025-30398	Missing authorization in Nuance PowerScribe allows an unauthorized attacker to disclose information over a network.	8.1	More Details
CVE-2025-55278	Improper authentication in the API authentication middleware of HCL DevOps Loop allows authentication tokens to be accepted without proper validation of their expiration and cryptographic signature. As a result, an attacker could potentially use expired or tampered tokens to gain unauthorized access to sensitive resources and perform actions with elevated privileges.	8.1	More Details
CVE-2025-64685	In JetBrains YouTrack before 2025.3.104432 missing TLS certificate validation enabled data disclosure	8.1	More Details
CVE-2025-64287	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Edge-Themes Alloggio - Hotel Booking alloggio allows PHP Local File Inclusion.This issue affects Alloggio - Hotel Booking: from n/a through <= 1.8.	8.1	More Details
CVE-2025-60190	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Hinnerk Altenburg Immocaster WordPress Plugin immocaster allows PHP Local File Inclusion.This issue affects Immocaster WordPress Plugin: from n/a through <= 1.3.6.	8.1	More Details
CVE-2025-58592	Deserialization of Untrusted Data vulnerability in Cozmoslabs TranslatePress translatepress-multilingual allows Object Injection.This issue affects TranslatePress: from n/a through <= 2.10.2.	8.1	More Details
CVE-2025-11458	Heap buffer overflow in Sync in Google Chrome prior to 141.0.7390.65 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2025-62010	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ApusTheme Famita famita allows PHP Local File Inclusion.This issue affects Famita: from n/a through <= 1.54.	8.1	More Details
CVE-2025-60715	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to execute code over a network.	8.0	More Details
CVE-2025-12967	An issue in AWS Wrappers for Amazon Aurora PostgreSQL may allow for privilege escalation to rds_superuser role. A low privilege authenticated user can create a crafted function that could be executed with permissions of other Amazon Relational Database Service (RDS) users. We recommend customers upgrade to the following versions: AWS JDBC Wrapper to v2.6.5, AWS Go Wrapper to 2025-10-17, AWS NodeJS Wrapper to v2.0.1, AWS Python Wrapper to v1.4.0 and AWS PGSQL ODBC driver to v1.0.1	8.0	More Details
CVE-2025-10622	A flaw was found in Red Hat Satellite (Foreman component). This vulnerability allows an authenticated user with edit_settings permissions to achieve arbitrary command execution on the underlying operating system via insufficient server-side validation of command whitelisting.	8.0	More Details

CVE-2025-62452	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to execute code over a network.	8.0	More Details
CVE-2025-62053	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in favethemes Houzez houzez.This issue affects Houzez: from n/a through < 4.2.0.	8.0	More Details
CVE-2025-62204	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	8.0	More Details
CVE-2025-30185	Active debug code for some Intel UEFI reference platforms within Ring 0: Kernel may allow a denial of service and escalation of privilege. System software adversary with a privileged user combined with a low complexity attack may enable data alteration. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (high) and availability (high) impacts.	7.9	More Details
CVE-2025-61832	InDesign Desktop versions 20.5, 19.5.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-60720	Buffer over-read in Windows TDX.sys allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-60727	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-61819	Photoshop Desktop versions 26.8.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61820	Illustrator versions 28.7.10, 29.8.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61826	Illustrator on iPad versions 3.0.9 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61824	InDesign Desktop versions 20.5, 19.5.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61828	Illustrator on iPad versions 3.0.9 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE-2025-61829	Illustrator on iPad versions 3.0.9 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61831	Illustrator versions 28.7.10, 29.8.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61836	Illustrator on iPad versions 3.0.9 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-62199	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-62200	Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-9458	A maliciously crafted PRT file, when parsed through certain Autodesk products, can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-64343	(conda) Constructor is a tool that enables users to create installers for conda package collections. In versions 3.12.2 and below, the installation directory inherits permissions from its parent directory. Outside of restricted directories, the permissions are very permissive and often allow write access by authenticated users. Any logged in user can make modifications during the installation for both single-user and all-user installations. This constitutes a local attack vector if the installation is in a directory local users have access to. For single-user installations in a shared directory, these permissions persist after the installation. This issue is fixed in version 3.13.0.	7.8	More Details
CVE-2025-62201	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-62203	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-62205	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-62216	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-61837	Format Plugins versions 1.1.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-	Format Plugins versions 1.1.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of		More

61838	the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	Details
CVE-2025-10885	A maliciously crafted file, when executed on the victim's machine, can lead to privilege escalation to NT AUTHORITY/SYSTEM due to an insufficient validation of loaded binaries. An attacker with local and low-privilege access could exploit this to execute code as SYSTEM.	7.8	More Details
CVE-2025-61839	Format Plugins versions 1.1.1 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-32008	A vulnerability has been identified in Spectrum Power 4 (All versions < V4.70 SP12 Update 2). The affected application is vulnerable to a local privilege escalation due to an exposed debug interface on the localhost. This allows any local user to gain code execution as administrative application user.	7.8	More Details
CVE-2024-32009	A vulnerability has been identified in Spectrum Power 4 (All versions < V4.70 SP12 Update 2). The affected application is vulnerable to a local privilege escalation due to wrongly set permissions to a binary which allows any local attacker to gain administrative privileges.	7.8	More Details
CVE-2024-32010	A vulnerability has been identified in Spectrum Power 4 (All versions < V4.70 SP12 Update 2). The affected application is vulnerable to extraction of database credentials via a world-readable credential file. This allows an attacker to connect to the database as privileged application user and to run system commands via the database.	7.8	More Details
CVE-2025-40763	A vulnerability has been identified in Altair Grid Engine (All versions < V2026.0.0). Affected products do not properly validate environment variables when loading shared libraries, allowing path hijacking through malicious library substitution. This could allow a local attacker to execute arbitrary code with superuser privileges by manipulating the environment variable and placing a malicious library in the controlled path.	7.8	More Details
CVE-2025-40827	A vulnerability has been identified in Siemens Software Center (All versions < V3.5), Solid Edge SE2025 (All versions < V225.0 Update 10). The affected application is vulnerable to DLL hijacking. This could allow an attacker to execute arbitrary code via placing a crafted DLL file on the system.	7.8	More Details
CVE-2025-61833	Substance3D - Stager versions 3.1.5 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61834	Substance3D - Stager versions 3.1.5 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61835	Substance3D - Stager versions 3.1.5 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-	Privilege context switching error in Windows Administrator Protection allows an		More

2025-60721	authorized attacker to elevate privileges locally.	7.8	Details
CVE-2025-61827	Illustrator on iPad versions 3.0.9 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-64531	Substance3D - Stager versions 3.1.5 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-60710	Improper link resolution before file access ('link following') in Host Process for Windows Tasks allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-23361	NVIDIA NeMo Framework for all platforms contains a vulnerability in a script, where malicious input created by an attacker may cause improper control of code generation. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2025-60718	Untrusted search path in Windows Administrator Protection allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-60703	Untrusted pointer dereference in Windows Remote Desktop allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-60705	Improper access control in Windows Client-Side Caching (CSC) Service allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-23357	NVIDIA Megatron-LM for all platforms contains a vulnerability in a script, where malicious data created by an attacker may cause a code injection issue. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, information disclosure, data tampering.	7.8	More Details
CVE-2025-59514	Improper privilege management in Microsoft Streaming Service allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-59512	Improper access control in Customer Experience Improvement Program (CEIP) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-20010	Use of unmaintained third party components for some Intel(R) Processor Identification Utility before version 8.0.43 within Ring 3: User Applications may allow an escalation of privilege. System software adversary with an authenticated user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	7.8	More Details
CVE-2025-59511	External control of file name or path in Windows WLAN Service allows an authorized attacker to elevate privileges locally.	7.8	More Details

CVE-2025-33178	NVIDIA NeMo Framework for all platforms contains a vulnerability in the bert services component where malicious data created by an attacker may cause a code injection. A successful exploit of this vulnerability may lead to Code execution, Escalation of privileges, Information disclosure, and Data tampering.	7.8	More Details
CVE-2025-60707	Use after free in Multimedia Class Scheduler Service (MMCSS) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-60709	Out-of-bounds read in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-60713	Untrusted pointer dereference in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-61815	InDesign Desktop versions 20.5, 19.5.5 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61818	InCopy versions 20.5, 19.5.5 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61817	InCopy versions 20.5, 19.5.5 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-60714	Heap-based buffer overflow in Windows OLE allows an unauthorized attacker to execute code locally.	7.8	More Details
CVE-2025-61816	InCopy versions 20.5, 19.5.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-61814	InDesign Desktop versions 20.5, 19.5.5 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-59505	Double free in Windows Smart Card allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2025-27713	Out-of-bounds write for some Intel(R) QAT Windows software before version 2.6.0. within Ring 3: User Applications may allow an escalation of privilege. System software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	7.8	More Details

CVE-2025-40816	A vulnerability has been identified in LOGO! 12/24RCE (6ED1052-1MD08-0BA2) (All versions), LOGO! 12/24RCEo (6ED1052-2MD08-0BA2) (All versions), LOGO! 230RCE (6ED1052-1FB08-0BA2) (All versions), LOGO! 230RCEo (6ED1052-2FB08-0BA2) (All versions), LOGO! 24CE (6ED1052-1CC08-0BA2) (All versions), LOGO! 24CEo (6ED1052-2CC08-0BA2) (All versions), LOGO! 24RCE (6ED1052-1HB08-0BA2) (All versions), LOGO! 24RCEo (6ED1052-2HB08-0BA2) (All versions), SIPLUS LOGO! 12/24RCE (6AG1052-1MD08-7BA2) (All versions), SIPLUS LOGO! 12/24RCEo (6AG1052-2MD08-7BA2) (All versions), SIPLUS LOGO! 230RCE (6AG1052-1FB08-7BA2) (All versions), SIPLUS LOGO! 230RCEo (6AG1052-2FB08-7BA2) (All versions), SIPLUS LOGO! 24CE (6AG1052-1CC08-7BA2) (All versions), SIPLUS LOGO! 24CEo (6AG1052-2CC08-7BA2) (All versions), SIPLUS LOGO! 24RCE (6AG1052-1HB08-7BA2) (All versions), SIPLUS LOGO! 24RCEo (6AG1052-2HB08-7BA2) (All versions). Affected devices do not conduct certain validations when interacting with them. This could allow an unauthenticated remote attacker to manipulate the devices IP address, which means the device would not be reachable.	7.6	More Details
CVE-2025-64501	ProsemirrorToHtml is a JSON converter which takes ProseMirror-compatible JSON and outputs HTML. In versions 0.2.0 and below, the `prosemirror_to_html` gem is vulnerable to Cross-Site Scripting (XSS) attacks through malicious HTML attribute values. While tag content is properly escaped, attribute values are not, allowing attackers to inject arbitrary JavaScript code. Applications that use `prosemirror_to_html` to convert ProseMirror documents to HTML, user-generated ProseMirror content, and end users viewing the rendered HTML output are all at risk of attack. This issue is fixed in version 0.2.1.	7.6	More Details
CVE-2025-27917	An issue was discovered in AnyDesk through 9.0.4. Remote Denial of Service can occur because of incorrect deserialization that results in failed memory allocation and a NULL pointer dereference.	7.5	More Details
CVE-2025-62039	Insertion of Sensitive Information Into Sent Data vulnerability in Ays Pro AI ChatBot with ChatGPT and Content Generator by AYS ays-chatgpt-assistant allows Retrieve Embedded Sensitive Data.This issue affects AI ChatBot with ChatGPT and Content Generator by AYS: from n/a through <= 2.6.6.	7.5	More Details
CVE-2025-40744	A vulnerability has been identified in Solid Edge SE2025 (All versions < V225.0 Update 11). Affected applications do not properly validate client certificates to connect to License Service endpoint. This could allow an unauthenticated remote attacker to perform man in the middle attacks.	7.5	More Details
CVE-2025-63560	An issue in KiloView Dual Channel 4k HDMI & 3G-SDI HEVC Video Encoder Firmware v.1.20.0006 allows a remote attacker to cause a denial of service via the systemctrl API System/reFactory component.	7.5	More Details
CVE-2025-27916	An issue was discovered in AnyDesk through 9.0.4. When the connection between two clients is established via an IP address, it is possible to manipulate the data and spoof the AnyDesk ID.	7.5	More Details
CVE-2025-60248	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in WPClever WPC Product Options for WooCommerce wpc-product-options allows PHP Local File Inclusion.This issue affects WPC Product Options for WooCommerce: from n/a through <= 1.8.6.	7.5	More Details
CVE-2025-12197	The The Events Calendar plugin for WordPress is vulnerable to blind SQL Injection via the 's' parameter in versions 6.15.1.1 to 6.15.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details

CVE-2025-63551	A Server-Side Request Forgery (SSRF) vulnerability, achievable through an XML External Entity (XXE) injection, exists in MetInfo Content Management System (CMS) thru 8.1. This flaw stems from a defect in the XML parsing logic, which allows an attacker to construct a malicious XML entity that forces the server to initiate an HTTP request to an arbitrary internal or external network address. Successful exploitation could lead to internal network reconnaissance, port scanning, or the retrieval of sensitive information. The vulnerability may be present in the backend API called by or associated with the path `/admin/#/webset/?head_tab_active=0`, where user-provided XML data is processed.	7.5	More Details
CVE-2025-64173	Apollo Router Core is a configurable graph router written in Rust to run a federated supergraph using Apollo Federation 2. In versions 1.61.11 below, as well as 2.0.0-alpha.0 through 2.8.1-rc.0, a vulnerability allowed for unauthenticated queries to access data that required additional access controls. Router incorrectly handled access control directives on interface types/fields and their implementing object types/fields, applying them to interface types/fields while ignoring directives on their implementing object types/fields when all implementations had the same requirements. Apollo Router customers defining @authenticated, @requiresScopes, or @policy directives inconsistently on polymorphic types (i.e., object types that implement interface types) are impacted. This issue is fixed in versions 1.61.12 and 2.8.1.	7.5	More Details
CVE-2025-12726	Inappropriate implementation in Views in Google Chrome on Windows prior to 142.0.7444.137 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2025-63455	Tenda AX-3 v16.03.12.10_CN was discovered to contain a stack overflow via the shareSpeed parameter in the fromSetWifiGusetBasic function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	7.5	More Details
CVE-2025-64508	Bugsink is a self-hosted error tracking tool. In versions prior to 2.0.5, brotli "bombs" (highly compressed brotli streams, such as many zeros) can be sent to the server. Since the server will attempt to decompress these streams before applying various maximums, this can lead to exhaustion of the available memory and thus a Denial of Service. This can be done if the `DSN` is known, which it is in many common setups (JavaScript, Mobile Apps). The issue is patched in Bugsink version `2.0.5`. The vulnerability is similar to, but distinct from, another brotli-related problem in Bugsink, GHSA-rrx3-2x4g-mq2h/CVE-2025-64509.	7.5	More Details
CVE-2025-64509	Bugsink is a self-hosted error tracking tool. In versions prior to 2.0.6, a specially crafted Brotli-compressed envelope can cause Bugsink to spend excessive CPU time in decompression, leading to denial of service. This can be done if the DSN is known, which it is in many common setups (JavaScript, Mobile Apps). The issue is patched in Bugsink 2.0.6. The vulnerability is similar to, but distinct from, another brotli-related problem in Bugsink, GHSA-fc2v-vcwj-269v/CVE-2025-64508.	7.5	More Details
CVE-2025-64518	The CycloneDX core module provides a model representation of the SBOM along with utilities to assist in creating, validating, and parsing SBOMs. Starting in version 2.1.0 and prior to version 11.0.1, the XML `Validator` used by cyclonedx-core-java was not configured securely, making the library vulnerable to XML External Entity (XXE) injection. The fix for GHSA-683x-4444-jxh8 / CVE-2024-38374 was incomplete in that it only fixed parsing of XML BOMs, but not validation. The vulnerability has been fixed in cyclonedx-core-java version 11.0.1. As a workaround, applications can reject XML documents before handing them to cyclonedx-core-java for validation. This may be an option if incoming CycloneDX BOMs are known to be in JSON format.	7.5	More Details
CVE-2025-	SAP CommonCryptoLib does not perform necessary boundary checks during pre-authentication parsing of manipulated ASN.1 data over the network. This may result	7.5	More

42940	in memory corruption followed by an application crash, hence leading to a high impact on availability. There is no impact on confidentiality or integrity.		Details
CVE-2025-64110	Cursor is a code editor built for programming with AI. In versions 1.7.23 and below, a logic bug allows a malicious agent to read sensitive files that should be protected via cursorignore. An attacker who has already achieved prompt injection, or a malicious model, could create a new cursorignore file which can invalidate the configuration of pre-existing ones. This could allow a malicious agent to read protected files. This issue is fixed in version 2.0.	7.5	More Details
CVE-2025-11451	The Auto Amazon Links – Amazon Associates Affiliate Plugin plugin for WordPress is vulnerable to arbitrary files reads in all versions up to, and including, 5.4.3 via the '/wp-json/wp/v2/aal_ajax_unit_loading' RST API endpoint. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	7.5	More Details
CVE-2025-11452	The Asgaros Forum plugin for WordPress is vulnerable to SQL Injection via the '$_COOKIE['asgarosforum_unread_exclude']' cookie in all versions up to, and including, 3.1.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2025-60574	A Local File Inclusion (LFI) vulnerability has been identified in tQuadra CMS 4.2.1117. The issue exists in the "/styles/" path, which fails to properly sanitize user-supplied input. An attacker can exploit this by sending a crafted GET request to retrieve arbitrary files from the underlying system.	7.5	More Details
CVE-2025-12863	A flaw was found in the xmlSetTreeDoc() function of the libxml2 XML parsing library. This function is responsible for updating document pointers when XML nodes are moved between documents. Due to improper handling of namespace references, a namespace pointer may remain linked to a freed memory region when the original document is destroyed. As a result, subsequent operations that access the namespace can lead to a use-after-free condition, causing an application crash.	7.5	More Details
CVE-2025-64430	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions 4.2.0 through 7.5.3, and 8.0.0 through 8.3.1-alpha.1, there is a Server-Side Request Forgery (SSRF) vulnerability in the file upload functionality when trying to upload a Parse.File with uri parameter, allowing execution of an arbitrary URI. The vulnerability stems from a file upload feature in which Parse Server retrieves the file data from a URI that is provided in the request. A request to the provided URI is executed, but the response is not stored in Parse Server's file storage as the server crashes upon receiving the response. This issue is fixed in versions 7.5.4 and 8.4.0-alpha.1.	7.5	More Details
CVE-2025-64347	Apollo Router Core is a configurable Rust graph router written to run a federated supergraph using Apollo Federation 2. Versions 1.61.12-rc.0 and below and 2.8.1-rc.0 allow unauthorized access to protected data through schema elements with access control directives (@authenticated, @requiresScopes, and @policy) that were renamed via @link imports. Router did not enforce renamed access control directives on schema elements (e.g. fields and types), allowing queries to bypass those element-level access controls. This issue is fixed in versions 1.61.12 and 2.8.1.	7.5	More Details
CVE-2025-12139	The File Manager for Google Drive – Integrate Google Drive with WordPress plugin for WordPress is vulnerable to sensitive information exposure in all versions up to, and including, 1.5.3 via the "get_localize_data" function. This makes it possible for unauthenticated attackers to extract sensitive data including Google OAuth credentials (client_id and client_secret) and Google account email addresses.	7.5	More Details

CVE-2025-60704	Missing cryptographic step in Windows Kerberos allows an unauthorized attacker to elevate privileges over a network.	7.5	More Details
CVE-2025-59171	Due to insufficient sanitization, an attacker can upload a specially crafted configuration file to traverse directories and achieve remote code execution with system-level permissions.	7.5	More Details
CVE-2025-64458	An issue was discovered in 5.1 before 5.1.14, 4.2 before 4.2.26, and 5.2 before 5.2.8. NFKC normalization in Python is slow on Windows. As a consequence, `django.http.HttpResponseRedirect`, `django.http.HttpResponsePermanentRedirect`, and the shortcut `django.shortcuts.redirect` were subject to a potential denial-of-service attack via certain inputs with a very large number of Unicode characters. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Seokchan Yoon for reporting this issue.	7.5	More Details
CVE-2025-60202	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Kyle Phillips Favorites favorites allows PHP Local File Inclusion.This issue affects Favorites: from n/a through <= 2.3.6.	7.5	More Details
CVE-2025-60191	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Premmerce Premmerce Wishlist for WooCommerce premmerce-woocommerce-wishlist allows PHP Local File Inclusion.This issue affects Premmerce Wishlist for WooCommerce: from n/a through <= 1.1.10.	7.5	More Details
CVE-2025-46784	A denial of service vulnerability exists in the lasso_node_init_from_message_with_format functionality of Entr'ouvert Lasso 2.5.1. A specially crafted SAML response can lead to a memory depletion, resulting in denial of service. An attacker can send a malformed SAML response to trigger this vulnerability.	7.5	More Details
CVE-2025-60200	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThimPress LearnPress Export Import learnpress-import-export allows PHP Local File Inclusion.This issue affects LearnPress Export Import: from n/a through <= 4.0.9.	7.5	More Details
CVE-2025-60203	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Josh Kohlbach Store Exporter woocommerce-exporter allows PHP Local File Inclusion.This issue affects Store Exporter: from n/a through <= 2.7.6.	7.5	More Details
CVE-2025-46705	A denial of service vulnerability exists in the g_assert_not_reached functionality of Entr'ouvert Lasso 2.5.1 and 2.8.2. A specially crafted SAML assertion response can lead to a denial of service. An attacker can send a malformed SAML response to trigger this vulnerability.	7.5	More Details
CVE-2025-60196	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Clearblue Clearblue® Ovulation Calculator clearblue-ovulation-calculator allows PHP Local File Inclusion.This issue affects Clearblue® Ovulation Calculator: from n/a through <= 1.2.4.	7.5	More Details
CVE-2025-60194	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Premmerce Premmerce Product Search for WooCommerce premmerce-search allows PHP Local File Inclusion.This issue affects Premmerce Product Search for WooCommerce: from n/a through <= 2.2.4.	7.5	More Details
CVE-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP		

2025-60193	Remote File Inclusion') vulnerability in Premmerce Premmerce User Roles premmerce-user-roles allows PHP Local File Inclusion.This issue affects Premmerce User Roles: from n/a through <= 1.0.13.	7.5	More Details
CVE-2025-60192	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Premmerce Premmerce Wholesale Pricing for WooCommerce premmerce-woocommerce-wholesale-pricing allows PHP Local File Inclusion.This issue affects Premmerce Wholesale Pricing for WooCommerce: from n/a through <= 1.1.10.	7.5	More Details
CVE-2025-60074	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Processby Lazy Load Optimizer lazy-load-optimizer allows PHP Local File Inclusion.This issue affects Lazy Load Optimizer: from n/a through <= 1.4.7.	7.5	More Details
CVE-2025-63248	DWSurvey 6.14.0 is vulnerable to Incorrect Access Control. When deleting a questionnaire, replacing the questionnaire ID with the ID of another questionnaire can enable the deletion of other questionnaires.	7.5	More Details
CVE-2025-60240	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Alexander AnyComment anycomment allows PHP Local File Inclusion.This issue affects AnyComment: from n/a through <= 0.3.6.	7.5	More Details
CVE-2025-60241	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Premmerce Premmerce premmerce allows PHP Local File Inclusion.This issue affects Premmerce: from n/a through <= 1.3.19.	7.5	More Details
CVE-2025-60204	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Josh Kohlbach WooCommerce Store Toolkit woocommerce-store-toolkit allows PHP Local File Inclusion.This issue affects WooCommerce Store Toolkit: from n/a through <= 2.4.3.	7.5	More Details
CVE-2025-46404	A denial of service vulnerability exists in the lasso_provider_verify_saml_signature functionality of Entr'ouvert Lasso 2.5.1. A specially crafted SAML response can lead to a denial of service. An attacker can send a malformed SAML response to trigger this vulnerability.	7.5	More Details
CVE-2025-60201	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in aguilatechnologies WP Customer Area customer-area allows PHP Local File Inclusion.This issue affects WP Customer Area: from n/a through <= 8.2.7.	7.5	More Details
CVE-2025-35963	Insufficient control flow management for some Intel(R) PROSet/Wireless WiFi Software for Windows before version 23.160 within Ring 2: Device Drivers may allow a denial of service. Unprivileged software adversary with an unauthenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via adjacent access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (high) impacts.	7.4	More Details
CVE-2025-33029	Out-of-bounds write for some Intel(R) PROSet/Wireless WiFi Software for Windows before version 23.160 within Ring 2: Device Drivers may allow a denial of service. Unprivileged software adversary with an unauthenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via adjacent access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity	7.4	More Details

	(none) and availability (high) impacts.		
CVE-2025-62066	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in fuelthemes Revolution revolution.This issue affects Revolution: from n/a through < 2.5.8.	7.4	More Details
CVE-2025-36186	IBM Db2 12.1.0 through 12.1.3 for Linux, UNIX and Windows (includes Db2 Connect Server) under specific configurations could allow a local user to execute malicious code that escalate their privileges to root due to execution of unnecessary privileges operated at a higher than minimum level.	7.4	More Details
CVE-2025-35967	Out-of-bounds read for some Intel(R) PROSet/Wireless WiFi Software for Windows before version 23.160 within Ring 2: Device Drivers may allow a denial of service. Unprivileged software adversary with an unauthenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via adjacent access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (high) impacts.	7.4	More Details
CVE-2025-64688	In JetBrains YouTrack before 2025.3.104432 missing VCS URL validation allowed delegation to unauthorized repositories from the Junie widget	7.4	More Details
CVE-2025-41731	A vulnerability was identified in the password generation algorithm when accessing the debug-interface. An unauthenticated local attacker with knowledge of the password generation timeframe might be able to brute force the password in a timely manner and thus gain root access to the device if the debug interface is still enabled.	7.4	More Details
CVE-2025-12790	A flaw was found in Rubygem MQTT. By default, the package used to not have hostname validation, resulting in possible Man-in-the-Middle (MITM) attack.	7.4	More Details
CVE-2025-62075	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Ido Kobelkowsky Simple Payment simple-payment.This issue affects Simple Payment: from n/a through <= 2.4.6.	7.3	More Details
CVE-2025-12938	A vulnerability was identified in projectworlds Online Admission System 1.0. Affected by this vulnerability is an unknown functionality of the file /process_login.php. The manipulation of the argument keywords leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2024-25621	containerd is an open-source container runtime. Versions 0.1.0 through 1.7.28, 2.0.0-beta.0 through 2.0.6, 2.1.0-beta.0 through 2.1.4 and 2.2.0-beta.0 through 2.2.0-rc.1 have an overly broad default permission vulnerability. Directory paths `/var/lib/containerd`, `/run/containerd/io.containerd.grpc.v1.cri` and `/run/containerd/io.containerd.sandbox.controller.v1.shim` were all created with incorrect permissions. This issue is fixed in versions 1.7.29, 2.0.7, 2.1.5 and 2.2.0. Workarounds include updating system administrator permissions so the host can manually chmod the directories to not have group or world accessible permissions, or to run containerd in rootless mode.	7.3	More Details
CVE-2025-43990	Dell Command Monitor (DCM), versions prior to 10.12.3.28, contains an Execution with Unnecessary Privileges vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	7.3	More Details

CVE-2025-59504	Heap-based buffer overflow in Azure Monitor Agent allows an unauthorized attacker to execute code locally.	7.3	More Details
CVE-2025-10161	Improper Restriction of Excessive Authentication Attempts, Client-Side Enforcement of Server-Side Security, Reliance on Untrusted Inputs in a Security Decision vulnerability in Turkguven Software Technologies Inc. Perfektive allows Brute Force, Authentication Bypass, Functionality Bypass.This issue affects Perfektive: before Version: 12574 Build: 2701.	7.3	More Details
CVE-2025-7430	Zohocorp ManageEngine Exchange Reporter Plus versions 5723 and below are vulnerable to the Stored XSS Vulnerability in the Folder Message Count and Size report.	7.3	More Details
CVE-2025-12925	A security flaw has been discovered in rymcu forest up to de53ce79db9faa2efc4e79ce1077a302c42a1224. Impacted is the function getAll/addDic/getAllDic/deleteDic of the file src/main/java/com/rymcu/forest/lucene/api/UserDicController.java. The manipulation results in missing authorization. The attack may be launched remotely. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases.	7.3	More Details
CVE-2025-7633	Zohocorp ManageEngine Exchange Reporter Plus versions 5723 and below are vulnerable to the Stored XSS Vulnerability in the Custom report.	7.3	More Details
CVE-2025-12929	A flaw has been found in SourceCodester Survey Application System 1.0. This impacts the function save_user/update_user of the file /LoginRegistration.php. Executing manipulation of the argument fullname can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used. Other parameters might be affected as well.	7.3	More Details
CVE-2025-12928	A vulnerability was detected in code-projects Online Job Search Engine 1.0. This affects an unknown function of the file /login.php. Performing manipulation of the argument username/phone results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-7632	Zohocorp ManageEngine Exchange Reporter Plus versions 5723 and below are vulnerable to the Stored XSS Vulnerability in the Public Folders report.	7.3	More Details
CVE-2025-60541	A Server-Side Request Forgery (SSRF) in the /api/proxy/ component of linshenkx prompt-optimizer v1.3.0 to v1.4.2 allows attackers to scan internal resources via a crafted request.	7.3	More Details
CVE-2025-46430	Dell Display and Peripheral Manager, versions prior to 2.1.2.12, contains an Execution with Unnecessary Privileges vulnerability in the Installer. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	7.3	More Details
CVE-2025-64496	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Versions 0.6.224 and prior contain a code injection vulnerability in the Direct Connections feature that allows malicious external model servers to execute arbitrary JavaScript in victim browsers via Server-Sent Event (SSE) execute events. This leads to authentication token theft, complete account takeover, and when chained with the Functions API, enables remote code execution on the backend server. The attack requires the victim to enable Direct Connections (disabled by default) and add the attacker's malicious model URL, achievable through social engineering of the admin and subsequent users. This issue is fixed in version 0.6.35.	7.3	More Details

CVE-2025-7429	Zohocorp ManageEngine Exchange Reporter Plus versions 5723 and below are vulnerable to the Stored XSS Vulnerability in the Mails Deleted or Moved report.	7.3	More Details
CVE-2025-11967	The Mail Mint plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the process_contact_attribute_import function in all versions up to, and including, 1.18.10. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2025-12867	EIP Plus developed by Hundred Plus has an Arbitrary File Uplaod vulnerability, allowing privileged remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	7.2	More Details
CVE-2025-63417	A Stored Cross-Site Scripting (XSS) vulnerability in the chat functionality of the SelfBest platform 2023.3 allows authenticated attackers to inject arbitrary web scripts or HTML via the chat message input field. This malicious content is stored and then executed in the context of other users' browsers when they view the malicious message, potentially leading to session hijacking, account takeover, or other client-side attacks.	7.2	More Details
CVE-2025-12099	The Academy LMS – WordPress LMS Plugin for Complete eLearning Solution plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.3.8 via deserialization of untrusted input in the 'import_all_courses' function. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	7.2	More Details
CVE-2025-40815	A vulnerability has been identified in LOGO! 12/24RCE (6ED1052-1MD08-0BA2) (All versions), LOGO! 12/24RCEo (6ED1052-2MD08-0BA2) (All versions), LOGO! 230RCE (6ED1052-1FB08-0BA2) (All versions), LOGO! 230RCEo (6ED1052-2FB08-0BA2) (All versions), LOGO! 24CE (6ED1052-1CC08-0BA2) (All versions), LOGO! 24CEo (6ED1052-2CC08-0BA2) (All versions), LOGO! 24RCE (6ED1052-1HB08-0BA2) (All versions), LOGO! 24RCEo (6ED1052-2HB08-0BA2) (All versions), SIPLUS LOGO! 12/24RCE (6AG1052-1MD08-7BA2) (All versions), SIPLUS LOGO! 12/24RCEo (6AG1052-2MD08-7BA2) (All versions), SIPLUS LOGO! 230RCE (6AG1052-1FB08-7BA2) (All versions), SIPLUS LOGO! 230RCEo (6AG1052-2FB08-7BA2) (All versions), SIPLUS LOGO! 24CE (6AG1052-1CC08-7BA2) (All versions), SIPLUS LOGO! 24CEo (6AG1052-2CC08-7BA2) (All versions), SIPLUS LOGO! 24RCE (6AG1052-1HB08-7BA2) (All versions), SIPLUS LOGO! 24RCEo (6AG1052-2HB08-7BA2) (All versions). Affected devices do not properly validate the structure of TCP packets in several methods. This could allow an attacker to cause buffer overflows, get control over the instruction counter and run custom code.	7.2	More Details
CVE-2025-12399	The Alex Reservations: Smart Restaurant Booking plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the /wp-json/srr/v1/app/upload/file REST endpoint in all versions up to, and including, 2.2.3. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2025-53573	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jegtheme Epic Review epic-review allows Reflected XSS.This issue affects Epic Review: from n/a through <= 1.0.2.	7.1	More Details

CVE-2025-11206	Heap buffer overflow in Video in Google Chrome prior to 141.0.7390.54 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	7.1	More Details
CVE-2025-61830	Adobe Pass versions 3.7.3 and earlier are affected by an Incorrect Authorization vulnerability. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized read and write access. Exploitation of this issue requires user interaction in that a victim must install a malicious SDK.	7.1	More Details
CVE-2025-54721	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThimPress Resca resca allows Reflected XSS.This issue affects Resca: from n/a through <= 3.0.2.	7.1	More Details
CVE-2025-10918	Insecure default permissions in the agent of Ivanti Endpoint Manager before version 2024 SU4 allows a local authenticated attacker to write arbitrary files anywhere on disk	7.1	More Details
CVE-2025-54722	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ex-Themes WooTour woo-tour allows Reflected XSS.This issue affects WooTour: from n/a through <= 3.6.3.	7.1	More Details
CVE-2025-54718	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Yogi - Health Beauty & Yoga noo-yogi allows Reflected XSS.This issue affects Yogi - Health Beauty & Yoga: from n/a through <= 2.9.2.	7.1	More Details
CVE-2025-61084	MDaemon Mail Server 23.5.2 validates SPF, DKIM, and DMARC using the email enclosed in angle brackets (<>) in the From: header of SMTP DATA. An attacker can craft a From: header with multiple invisible Unicode thin spaces to display a spoofed sender while passing validation, allowing email spoofing even when anti-spoofing protections are in place.	7.1	More Details
CVE-2025-60726	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	7.1	More Details
CVE-2025-62202	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	7.1	More Details
CVE-2025-63711	A Cross-Site Request Forgery (CSRF) vulnerability in the SourceCodester Client Database Management System 1.0 allows an attacker to cause an authenticated administrative user to perform user deletion actions without their consent. The application's user deletion endpoint (e.g., superadmin_user_delete.php) accepts POST requests containing a user_id parameter and does not enforce request origin or anti-CSRF tokens. Because the endpoint lacks proper authentication/authorization checks and CSRF protections, a remote attacker can craft a malicious page that triggers deletion when visited by an authenticated admin, resulting in arbitrary removal of user accounts.	7.1	More Details
CVE-2025-64167	Combodo iTop is a web based IT service management tool. Versions prior to 2.7.13 and 3.2.2 are vulnerable to a cross-site scripting attack (leading to JS execution) when editing the URL parameter. Versions 2.7.13 and 3.2.2 don't use export.php, which was deprecated. They use export-v2.php instead.	7.1	More Details
CVE-2025-54737	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Jobmonster noo-jobmonster allows Reflected XSS.This issue affects Jobmonster: from n/a through <= 4.7.8.	7.1	More Details
CVE-2025-	Missing Authorization vulnerability in bPlugins Info Cards info-cards allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Info	7.1	More

54711	Cards: from n/a through <= 1.0.11.		Details
CVE-2025-21079	Improper input validation in Samsung Members prior to version 5.5.01.3 allows remote attackers to connect arbitrary URL and launch arbitrary activity with Samsung Members privilege. User interaction is required for triggering this vulnerability.	7.1	More Details
CVE-2025-53585	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme WeMusic noo-wemusic allows Reflected XSS.This issue affects WeMusic: from n/a through <= 1.9.1.	7.1	More Details
CVE-2025-63589	A reflected XSS vulnerability exists in CMSimple_XH 1.8's index.php router when attacker-controlled path segments are not sanitized or encoded before being inserted into the generated HTML (navigation links, breadcrumbs, search form action, footer links). An attacker-controlled string placed in the URL path is reflected into multiple HTML elements, allowing execution of arbitrary JavaScript in victims' browsers visiting a crafted URL.	7.1	More Details
CVE-2025-63588	An unauthenticated reflected cross-site scripting vulnerability in the query handling of CMSimpleXH allows remote attackers to inject and execute arbitrary JavaScript in a victim's browser via a crafted request (e.g., a maliciously crafted POST login). Successful exploitation may lead to theft of session cookies, credential disclosure, or other client-side impacts.	7.1	More Details
CVE-2025-62074	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Amauri WPMobile.App wpappninja.This issue affects WPMobile.App: from n/a through <= 11.71.	7.1	More Details
CVE-2025-62036	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uxper Togo togo.This issue affects Togo: from n/a through < 1.0.4.	7.1	More Details
CVE-2025-62059	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force SureRank surerank.This issue affects SureRank: from n/a through <= 1.3.2.	7.1	More Details
CVE-2025-62057	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in favethemes Houzez Theme - Functionality houzez-theme-functionality.This issue affects Houzez Theme - Functionality: from n/a through < 4.2.0.	7.1	More Details
CVE-2025-64232	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in icopydoc Import from YML import-from-yml allows Reflected XSS.This issue affects Import from YML: from n/a through <= 3.1.17.	7.1	More Details
CVE-2025-62076	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ido Kobelkowsky Simple Payment simple-payment.This issue affects Simple Payment: from n/a through <= 2.4.6.	7.1	More Details
CVE-2025-62040	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in YOP YOP Poll yop-poll.This issue affects YOP Poll: from n/a through <= 6.5.37.	7.1	More Details
CVE-2025-62041	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem (Elementor) thegem-elementor.This issue affects TheGem (Elementor): from n/a through <= 5.10.5.1.	7.1	More Details
CVE-2025-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in appscreo Easy Social Share Buttons easy-social-share-buttons3	7.1	More

64198	allows Reflected XSS.This issue affects Easy Social Share Buttons: from n/a through < 10.7.1.		Details
CVE-2025-62031	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Composer td-composer.This issue affects tagDiv Composer: from n/a through <= 5.4.1.	7.1	More Details
CVE-2025-64224	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand Conference Theme Custom Post Type grandconference-custom-post allows Reflected XSS.This issue affects Grand Conference Theme Custom Post Type: from n/a through < 2.6.4.	7.1	More Details
CVE-2025-64196	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pluggabl Booster for WooCommerce woocommerce-jetpack allows Reflected XSS.This issue affects Booster for WooCommerce: from n/a through <= 7.2.5.	7.1	More Details
CVE-2025-37735	Improper preservation of permissions in Elastic Defend on Windows hosts can lead to arbitrary files on the system being deleted by the Defend service running as SYSTEM. In some cases, this could result in local privilege escalation.	7.0	More Details
CVE-2025-59508	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Speech allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-60719	Untrusted pointer dereference in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-59507	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Speech allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-59506	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows DirectX allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-60716	Use after free in Windows DirectX allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-60717	Use after free in Windows Broadcast DVR User Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-62219	Double free in Microsoft Wireless Provisioning System allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-62218	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Wireless Provisioning System allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-62217	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-62215	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.0	More Details

CVE-2025-62213	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-59515	Use after free in Windows Broadcast DVR User Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-42895	Due to insufficient validation of connection property values, the SAP HANA JDBC Client allows a high-privilege locally authenticated user to supply crafted parameters that lead to unauthorized code loading, resulting in low impact on confidentiality and integrity and high impact on availability of the application.	6.9	More Details
CVE-2025-52662	A vulnerability in Nuxt DevTools has been fixed in version **2.6.4***. This issue may have allowed Nuxt auth token extraction via XSS under certain configurations. All users are encouraged to upgrade. More details: https://vercel.com/changelog/cve-2025-52662-xss-on-nuxt-devtools	6.9	More Details
CVE-2025-59392	On Elspec G5 devices through 1.2.2.19, a person with physical access to the device can reset the Admin password by inserting a USB drive (containing a publicly documented reset string) into a USB port.	6.8	More Details
CVE-2025-21073	Insecure default configuration in USB connection mode prior to SMR Nov-2025 Release 1 allows privileged physical attackers to access user data. User interaction is required for triggering this vulnerability.	6.8	More Details
CVE-2025-42894	Due to a Path Traversal vulnerability in SAP Business Connector, an attacker authenticated as an administrator with adjacent access could read, write, overwrite, and delete arbitrary files on the host system. Successful exploitation could enable the attacker to execute arbitrary operating system commands on the server, resulting in a complete compromise of the confidentiality, integrity, and availability of the affected system.	6.8	More Details
CVE-2025-62449	Improper limitation of a pathname to a restricted directory ('path traversal') in Visual Studio Code CoPilot Chat Extension allows an authorized attacker to bypass a security feature locally.	6.8	More Details
CVE-2025-5718	The ACAP Application framework could allow privilege escalation through a symlink attack. This vulnerability can only be exploited if the Axis device is configured to allow the installation of unsigned ACAP applications, and if an attacker convinces the victim to install a malicious ACAP application.	6.8	More Details
CVE-2025-42892	Due to an OS Command Injection vulnerability in SAP Business Connector, an authenticated attacker with administrative access and adjacent network access could upload specially crafted content to the server. If processed by the application, this content enables execution of arbitrary operating system commands. Successful exploitation could lead to full compromise of the system's confidentiality, integrity, and availability.	6.8	More Details
CVE-2025-56232	GOG Galaxy 2.0.0.2 suffers from Missing SSL Certificate Validation. An attacker who controls the local network, DNS, or a proxy can perform a man-in-the-middle (MitM) attack to intercept update requests and replace installer or update packages with malicious files.	6.8	More Details
CVE-2025-27246	Incorrect default permissions for the Intel(R) Processor Identification Utility before version 8.0.43 within Ring 3: User Applications may allow an escalation of privilege. System software adversary with an authenticated user combined with a high complexity attack may enable local code execution. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability	6.7	More Details

	may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.		
CVE-2025-30506	Uncontrolled search path for some Intel Driver and Support Assistant before version 25.2 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable local code execution. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-30182	Uncontrolled search path for some Intel(R) Distribution for Python software installers before version 2025.2.0 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-47179	Improper access control in Microsoft Configuration Manager allows an authorized attacker to elevate privileges locally.	6.7	More Details
CVE-2025-4645	An ACAP configuration file lacked sufficient input validation, which could allow for arbitrary code execution. This vulnerability can only be exploited if the Axis device is configured to allow the installation of unsigned ACAP applications, and if an attacker convinces the victim to install a malicious ACAP application.	6.7	More Details
CVE-2025-3125	An arbitrary file upload vulnerability exists in multiple WSO2 products due to improper input validation in the CarbonAppUploader admin service endpoint. An authenticated attacker with appropriate privileges can upload a malicious file to a user-controlled location on the server, potentially leading to remote code execution (RCE). This functionality is restricted by default to admin users; therefore, successful exploitation requires valid credentials with administrative permissions.	6.7	More Details
CVE-2025-25059	Uncontrolled search path for some Intel(R) One Boot Flash Update (Intel(R) OFU) software before version 14.1.31 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-32038	Uncontrolled search path for some FPGA Support Package for the Intel oneAPI DPC++C++ Compiler software before version 2025.0.1 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none)	6.7	More Details

	impacts.		
CVE-2025-32001	Uncontrolled search path for the Intel(R) Processor Identification Utility before version 8.0.43 within Ring 3: User Applications may allow an escalation of privilege. System software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-31647	Uncontrolled search path for some Intel(R) Graphics Software before version 25.22.1502.2 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-31931	Uncontrolled search path for the Instrumentation and Tracing Technology API (ITT API) software before version 3.25.4 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-27711	Incorrect default permissions for some Intel(R) One Boot Flash Update (Intel(R) OFU) software before version 14.1.31 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-24842	Uncontrolled search path for the Intel(R) System Support Utility before version 4.1.0 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with a privileged user combined with a high complexity attack may enable local code execution. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires passive user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-24918	Improper link resolution before file access ('link following') for some Intel(R) Server Configuration Utility software and Intel(R) Server Firmware Update Utility software before version 16.0.12. within Ring 3: User Applications may allow an escalation of privilege. System software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential	6.7	More Details

	vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.		
CVE-2025-24327	Insecure inherited permissions for some Intel(R) Rapid Storage Technology Application before version 20.0.1021 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable local code execution. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-35972	Uncontrolled search path for the Intel MPI Library before version 2021.16 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-20050	Uncontrolled search path for some Intel(R) CIP software before version WIN_DCA_2.4.0.11001 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable local code execution. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-46366	Dell CloudLink, versions prior to 8.1.1, contain a vulnerability where a privileged user may exploit and gain parallel privilege escalation or access to the database to obtain confidential information.	6.7	More Details
CVE-2025-46424	Dell CloudLink, versions prior to 8.2, contain use of a Cryptographic Primitive with a Risky Implementation vulnerability. A high privileged attacker could potentially exploit this vulnerability leading to Denial of service.	6.7	More Details
CVE-2025-20065	Uncontrolled search path for some Display Virtualization for Windows OS software before version 1797 within Ring 2: Device Drivers may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-20614	External control of file name or path for some Intel(R) CIP software before version WIN_DCA_2.4.0.11001 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with a privileged user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (low) and availability	6.7	More Details

	(none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.		
CVE-2025-22391	Improper access control for some SigTest before version 6.1.10 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-24491	Uncontrolled search path for some Intel(R) Killer(TM) Performance Suite software before version killer 4.0 40.25.509.1465 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-6298	ACAP applications can gain elevated privileges due to improper input validation, potentially leading to privilege escalation. This vulnerability can only be exploited if the Axis device is configured to allow the installation of unsigned ACAP applications, and if an attacker convinces the victim to install a malicious ACAP application.	6.7	More Details
CVE-2025-62214	Improper neutralization of special elements used in a command ('command injection') in Visual Studio allows an authorized attacker to execute code locally.	6.7	More Details
CVE-2025-22397	Dell Integrated Dell Remote Access Controller 9, 14G versions prior to 7.00.00.181, 15G and 16G versions 6.10.80.00 through 7.20.10.50 and Dell Integrated Dell Remote Access Controller 10, 17G versions prior to 1.20.25.00, contain an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	6.7	More Details
CVE-2025-31645	Uncontrolled search path for some System Event Log Viewer Utility software for all versions within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-32449	Unquoted search path for some PRI Driver software before version 03.03.1002 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details

CVE-2025-8108	An ACAP configuration file has improper permissions and lacks input validation, which could potentially lead to privilege escalation. This vulnerability can only be exploited if the Axis device is configured to allow the installation of unsigned ACAP applications, and if an attacker convinces the victim to install a malicious ACAP application.	6.7	More Details
CVE-2025-6779	An ACAP configuration file has improper permissions, which could allow command injection and potentially lead to privilege escalation. This vulnerability can only be exploited if the Axis device is configured to allow the installation of unsigned ACAP applications, and if an attacker convinces the victim to install a malicious ACAP application.	6.7	More Details
CVE-2025-31940	Incorrect default permissions for some Intel(R) Thread Director Visualizer software before version 1.1.1 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-30518	Incorrect default permissions for some Intel(R) PresentMon before version 2.3.1 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-32732	Buffer overflow for some Intel(R) QAT Windows software before version 2.6.0. within Ring 3: User Applications may allow a denial of service. System software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (low), integrity (low) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.6	More Details
CVE-2025-5452	A malicious ACAP application can gain access to admin-level service account credentials used by legitimate ACAP applications, leading to potential privilege escalation of the malicious ACAP application. This vulnerability can only be exploited if the Axis device is configured to allow the installation of unsigned ACAP applications, and if an attacker convinces the victim to install a malicious ACAP application.	6.6	More Details
CVE-2025-12890	Improper handling of malformed Connection Request with the interval set to be 1 (which supposed to be illegal) and the chM 0x7CFFFFFFF triggers a crash. The peripheral will not be connectable after it.	6.5	More Details
CVE-2024-47118	IBM Db2 10.5.0 through 10.5.11, 11.1.0 through 11.1.4.7, 11.5.0 through 11.5.9, and 12.1.0 through 12.1.3 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.	6.5	More Details
	Untrusted pointer dereference for some Intel QuickAssist Technology software		

CVE-2025-32446	before version 2.6.0 within Ring 3: User Applications may allow an escalation of privilege. System software adversary with an authenticated user combined with a low complexity attack may enable data manipulation. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (high) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.5	More Details
CVE-2025-33202	NVIDIA Triton Inference Server for Linux and Windows contains a vulnerability where an attacker could cause a stack overflow by sending extra-large payloads. A successful exploit of this vulnerability might lead to denial of service.	6.5	More Details
CVE-2025-36006	IBM Db2 10.5.0 through 10.5.11, 11.1.0 through 11.1.4.7, 11.5.0 through 11.5.9, and 12.1.0 through 12.1.3 for Linux, UNIX and Windows (includes Db2 Connect Server) could allow an authenticated user to cause a denial due to the improper release of resources after use.	6.5	More Details
CVE-2025-26402	Protection mechanism failure for some Intel(R) NPU Drivers within Ring 3: User Applications may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.5	More Details
CVE-2025-36008	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.3 for Linux, UNIX and Windows (includes Db2 Connect Server) could allow an authenticated user to cause a denial of service due to improper allocation of resources.	6.5	More Details
CVE-2025-62037	Missing Authorization vulnerability in uxper Togo togo.This issue affects Togo: from n/a through < 1.0.4.	6.5	More Details
CVE-2025-9227	Zohocorp ManageEngine OpManager versions 128609 and below are vulnerable to Stored XSS Vulnerability in the SNMP trap processor.	6.5	More Details
CVE-2025-60247	Missing Authorization vulnerability in Bux Bux Woocommerce bux-woocommerce allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Bux Woocommerce: from n/a through <= 1.2.3.	6.5	More Details
CVE-2025-62011	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem thegem.This issue affects TheGem: from n/a through <= 5.10.5.	6.5	More Details
CVE-2025-62012	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem (Elementor) thegem-elementor.This issue affects TheGem (Elementor): from n/a through <= 5.10.5.	6.5	More Details
CVE-2025-62030	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Composer td-composer.This issue affects tagDiv Composer: from n/a through <= 5.4.1.	6.5	More Details
CVE-2025-62032	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Cloud Library td-cloud-library allows DOM-Based XSS.This issue affects tagDiv Cloud Library: from n/a through < 3.9.2.	6.5	More Details
CVE-	Missing Authorization vulnerability in uxper Togo togo.This issue affects Togo: from		More

2025-62033	n/a through < 1.0.4.	6.5	Details
CVE-2025-12092	The CYAN Backup plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'delete' functionality in all versions up to, and including, 2.5.4. This makes it possible for authenticated attackers, with Administrator-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).	6.5	More Details
CVE-2025-40817	A vulnerability has been identified in LOGO! 12/24RCE (6ED1052-1MD08-0BA2) (All versions), LOGO! 12/24RCEo (6ED1052-2MD08-0BA2) (All versions), LOGO! 230RCE (6ED1052-1FB08-0BA2) (All versions), LOGO! 230RCEo (6ED1052-2FB08-0BA2) (All versions), LOGO! 24CE (6ED1052-1CC08-0BA2) (All versions), LOGO! 24CEo (6ED1052-2CC08-0BA2) (All versions), LOGO! 24RCE (6ED1052-1HB08-0BA2) (All versions), LOGO! 24RCEo (6ED1052-2HB08-0BA2) (All versions), SIPLUS LOGO! 12/24RCE (6AG1052-1MD08-7BA2) (All versions), SIPLUS LOGO! 12/24RCEo (6AG1052-2MD08-7BA2) (All versions), SIPLUS LOGO! 230RCE (6AG1052-1FB08-7BA2) (All versions), SIPLUS LOGO! 230RCEo (6AG1052-2FB08-7BA2) (All versions), SIPLUS LOGO! 24CE (6AG1052-1CC08-7BA2) (All versions), SIPLUS LOGO! 24CEo (6AG1052-2CC08-7BA2) (All versions), SIPLUS LOGO! 24RCE (6AG1052-1HB08-7BA2) (All versions), SIPLUS LOGO! 24RCEo (6AG1052-2HB08-7BA2) (All versions). Affected devices do not conduct certain validations when interacting with them. This could allow an unauthenticated remote attacker to change time of the device, which means the device could behave differently.	6.5	More Details
CVE-2025-24519	Buffer overflow for some Intel(R) QAT Windows software before version 2.6.0. within Ring 3: User Applications may allow an escalation of privilege. System software adversary with an authenticated user combined with a low complexity attack may enable data manipulation. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (high) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.5	More Details
CVE-2025-62038	Insertion of Sensitive Information Into Sent Data vulnerability in Sovlix MeetingHub meetinghub allows Retrieve Embedded Sensitive Data.This issue affects MeetingHub: from n/a through <= 1.23.9.	6.5	More Details
CVE-2025-62051	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AndonDesign UDesign Core u-design-core.This issue affects UDesign Core: from n/a through <= 4.14.1.	6.5	More Details
CVE-2025-24834	Protection mechanism failure for some Intel(R) CIP software before version WIN_DCA_2.4.0.11001 within Ring 3: User Applications may allow an information disclosure. Unprivileged software adversary with an unauthenticated user combined with a low complexity attack may enable data exposure. This result may potentially occur via adjacent access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.5	More Details
CVE-2025-7663	The Ovatheme Events Manager plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on several functions in the /class-ovaem-ajax.php file in all versions up to, and including, 1.8.6. This makes it possible for unauthenticated attackers to delete ticket files, download tickets, and more.	6.5	More Details

CVE-2025-12000	The WPFunnels plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the wpfnl_delete_log() function in all versions up to, and including, 3.6.2. This makes it possible for authenticated attackers, with Administrator-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).	6.5	More Details
CVE-2025-64493	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. In versions 8.6.0 through 8.9.0, there is an authenticated, blind (time-based) SQL-injection inside the appMetadata-operation of the GraphQL-API. This allows extraction of arbitrary data from the database, and does not require administrative access. This issue is fixed in version 8.9.1.	6.5	More Details
CVE-2025-24863	Improper privilege management for some Intel(R) CIP software before version WIN_DCA_2.4.0.11001 within Ring 3: User Applications may allow an information disclosure. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable data exposure. This result may potentially occur via network access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.5	More Details
CVE-2025-62044	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem Theme Elements (for WPBakery) thegem-elements.This issue affects TheGem Theme Elements (for WPBakery): from n/a through <= 5.10.5.1.	6.5	More Details
CVE-2025-27710	Untrusted pointer dereference for some Intel(R) QAT Windows software before version 2.6.0. within Ring 3: User Applications may allow an information disclosure. System software adversary with an authenticated user combined with a low complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.5	More Details
CVE-2025-64433	KubeVirt is a virtual machine management add-on for Kubernetes. Prior to 1.5.3 and 1.6.1, a vulnerability was discovered that allows a VM to read arbitrary files from the virt-launcher pod's file system. This issue stems from improper symlink handling when mounting PVC disks into a VM. Specifically, if a malicious user has full or partial control over the contents of a PVC, they can create a symbolic link that points to a file within the virt-launcher pod's file system. Since libvirt can treat regular files as block devices, any file on the pod's file system that is symlinked in this way can be mounted into the VM and subsequently read. Although a security mechanism exists where VMs are executed as an unprivileged user with UID 107 inside the virt-launcher container, limiting the scope of accessible resources, this restriction is bypassed due to a second vulnerability. The latter causes the ownership of any file intended for mounting to be changed to the unprivileged user with UID 107 prior to mounting. As a result, an attacker can gain access to and read arbitrary files located within the virt-launcher pod's file system or on a mounted PVC from within the guest VM. This vulnerability is fixed in 1.5.3 and 1.6.1.	6.5	More Details
CVE-2025-62046	Missing Authorization vulnerability in CodexThemes TheGem Demo Import (for WPBakery) thegem-importer.This issue affects TheGem Demo Import (for WPBakery): from n/a through <= 5.10.5.	6.5	More Details
CVE-	Missing Authorization vulnerability in Stylemix Cost Calculator Builder cost-		

2025-62049	calculator-builder.This issue affects Cost Calculator Builder: from n/a through <= 3.5.32.	6.5	More Details
CVE-2025-62914	Missing Authorization vulnerability in anibalwainstein Effect Maker effect-maker allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Effect Maker: from n/a through <= 1.2.1.	6.5	More Details
CVE-2025-20376	A vulnerability in the web UI of Cisco Unified CCX could allow an authenticated, remote attacker to upload and execute arbitrary files. This vulnerability is due to an insufficient input validation associated to file upload mechanisms. An attacker could exploit this vulnerability by uploading a malicious file to the web UI and executing it. A successful exploit could allow the attacker to execute arbitrary commands on the underlying system and elevate privileges to root. To exploit this vulnerability, the attacker must have valid administrative credentials.	6.5	More Details
CVE-2025-60784	A vulnerability in the XiaozhangBang Voluntary Like System V8.8 allows remote attackers to manipulate the zhekou parameter in the /topfirst.php Pay module, enabling unauthorized discounts. By sending a crafted HTTP POST request with zhekou set to an abnormally low value, an attacker can purchase votes at a reduced cost. Furthermore, by modifying the zid parameter, attackers can influence purchases made by other users, amplifying the impact. This issue stems from insufficient server-side validation of these parameters, potentially leading to economic loss and unfair manipulation of vote counts.	6.5	More Details
CVE-2025-60708	Untrusted pointer dereference in Storvsp.sys Driver allows an authorized attacker to deny service locally.	6.5	More Details
CVE-2025-10713	An XML External Entity (XXE) vulnerability exists in multiple WSO2 products due to improper configuration of the XML parser. The application parses user-supplied XML without applying sufficient restrictions, allowing resolution of external entities. A successful attack could enable a remote, unauthenticated attacker to read sensitive files from the server's filesystem or perform denial-of-service (DoS) attacks that render affected services unavailable.	6.5	More Details
CVE-2025-42884	SAP NetWeaver Enterprise Portal allows an unauthenticated attacker to inject JNDI environment properties or pass a URL used during JNDI lookup operations, enabling access to an unintended JNDI provider.&#xFFFD;This could further lead to disclosure or modification of information about the server. There is no impact on availability.	6.5	More Details
CVE-2025-62206	Exposure of sensitive information to an unauthorized actor in Microsoft Dynamics 365 (on-premises) allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2025-55341	Cross Site Scripting vulnerability in Quipux 4.0.1 through e1774ac allows anexos/anexos_nuevo.php asocImgRad.	6.5	More Details
CVE-2025-12636	The Ubia camera ecosystem fails to adequately secure API credentials, potentially enabling an attacker to connect to backend services. The attacker would then be able to gain unauthorized access to available cameras, enabling the viewing of live feeds or modification of settings.	6.5	More Details
CVE-2025-12010	The Authors List plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.0.6.1 via the via arbitrary method call from Authors_List_Shortcode class. This makes it possible for authenticated attackers, with Contributor-level access and above, to call methods such as get_meta to extract sensitive user data including password hashes, email addresses, usernames, and activation keys via specially crafted shortcode	6.5	More Details

	attributes		
CVE-2025-63585	OSSN (Open Source Social Network) 8.6 is vulnerable to SQL Injection in /action/rtcomments/status via the timestamp parameter.	6.5	More Details
CVE-2025-12808	Improper access control in Devolutions allows a View-only user to retrieve sensitive third-level nested fields, such as password lists custom values, resulting in password disclosure. This issue affects the following versions : * Devolutions Server 2025.3.2.0 through 2025.3.5.0 * Devolutions Server 2025.2.15.0 and earlier	6.5	More Details
CVE-2025-4522	The IDonate – Blood Donation, Request And Donor Management System plugin for WordPress is vulnerable to Insecure Direct Object Reference via the admin_post_donor_delete() function in versions 2.0.0 to 2.1.9. By supplying an arbitrary user_id parameter value to the wp_delete_user() function, authenticated attackers, with Subscriber-level access and above could delete arbitrary user accounts, including those of administrators.	6.5	More Details
CVE-2025-64114	ClipBucket v5 is an open source video sharing platform. Versions 5.5.2 - #151 and below allow authenticated administrators with plugin management privileges to execute arbitrary SQL commands against the database through its ClipBucket Custom Fields plugin. The vulnerabilities require the Custom Fields plugin to be installed and accessible, and can only be exploited by users with administrative access to the plugin interface. This issue is fixed in version 5.5.2 - #.	6.5	More Details
CVE-2025-60722	Improper limitation of a pathname to a restricted directory ('path traversal') in OneDrive for Android allows an authorized attacker to elevate privileges over a network.	6.5	More Details
CVE-2025-20375	A vulnerability in the web UI of Cisco Unified CCX could allow an authenticated, remote attacker to upload and execute arbitrary files. This vulnerability is due to an insufficient input validation associated to specific UI features. An attacker could exploit this vulnerability by uploading a crafted file to the web UI. A successful exploit could allow the attacker to upload arbitrary files to a vulnerable system and execute them, gaining access to the underlying operating system. To exploit this vulnerability, the attacker must have valid administrative credentials.	6.5	More Details
CVE-2025-11828	The Magazine Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'headerHtmlTag' attribute in the bnm-blocks/featured-posts-1 block in all versions up to, and including, 1.2.3. This is due to insufficient input sanitization and output escaping when using user-supplied values as HTML tag names. 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-2025-11873	The WP BBCode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'url' shortcode in all versions up to, and including, 1.8.1 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-2025-12754	The Geopost plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'height' parameter of the 'geopost' shortcode in all versions up to, and including, 1.2. This is 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
	The Live Photos on WordPress plugin for WordPress is vulnerable to Stored Cross-		

CVE-2025-12651	Site Scripting via the 'video_src', 'img_src', and 'class' parameters in the livephotos_photo shortcode in all versions up to, and including, 0.1. This is 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 when a user accesses an injected page.	6.4	More Details
CVE-2025-11856	The Eventbee Ticketing Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'eventbeeticketwidget' shortcode in all versions up to, and including, 1.0. This is due to the plugin not properly sanitizing user input and output of several parameters. 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-2025-11917	The WPeMatico RSS Feed Fetcher plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.8.11 via the wpematico_test_feed() 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-2025-11129	The Include Fussball.de Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'api' and 'type' parameters in all versions up to, and including, 4.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-64302	Insufficient input sanitization in the dashboard label or path can allow an attacker to trigger a device error causing information disclosure or data manipulation.	6.4	More Details
CVE-2025-12388	The B Carousel Block – Responsive Image and Content Carousel plugin for WordPress is vulnerable to Server-Side Request Forgery in versions up to, and including, 1.1.5. This is due to the plugin not validating user-supplied URLs before passing them to the wp_remote_request() 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-2025-5454	An ACAP configuration file lacked sufficient input validation, which could allow a path traversal attack leading to potential privilege escalation. This vulnerability can only be exploited if the Axis device is configured to allow the installation of unsigned ACAP applications, and if an attacker convinces the victim to install a malicious ACAP application.	6.4	More Details
CVE-2025-11987	The Visual Link Preview plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's visual-link-preview shortcode in versions up to, and including, 2.2.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11745	The Ad Inserter – Ad Manager & AdSense Ads plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom field through the plugin's 'adinserter' shortcode in all versions up to, and including, 2.8.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an	6.4	More Details

	injected page.		
CVE-2025-11882	The Simple Donate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's simpledonate shortcode in versions less than, or equal to, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11162	The Spectra Gutenberg Blocks – Website Builder for the Block Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Custom CSS in all versions up to, and including, 2.19.14 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-2025-11820	The Graphina – Elementor Charts and Graphs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple chart widgets in all versions up to, and including, 3.1.8 due to insufficient input sanitization and output escaping on data 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. The vulnerability affects multiple chart widgets including Area Chart, Line Chart, Column Chart, Donut Chart, Heatmap Chart, Radar Chart, Polar Chart, Pie Chart, Radial Chart, and Advance Data Table widgets.	6.4	More Details
CVE-2025-12753	The Chart Expert plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pmzez_chart' shortcode in all versions up to, and including, 1.0. This is due to insufficient input sanitization and output escaping on user supplied shortcode attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12583	The Simple Downloads List plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wp_ajax_neofix_sdl_edit' AJAX endpoint along with many others in all versions up to, and including, 1.4.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to alter many of the plugin's settings/downloads and inject malicious web scripts.	6.4	More Details
CVE-2025-11869	The Precise Columns plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `wrap_id` shortcode attribute in all versions up to, and including, 1.0. This is due to the plugin not properly sanitizing user input or escaping output when inserting the wrapper ID into the generated HTML. 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-2025-12112	The Insert Headers and Footers Code – HT Script plugin for WordPress is vulnerable to Stored Cross-Site Scripting via adding scripts in all versions up to, and including, 1.1.6 due to insufficient capability checks. 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-2025-11863	The My Geo Posts Free plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mygeo_city' shortcode in all versions up to, and including, 1.2. This is due to the plugin not properly sanitizing user input or escaping output of the 'default' shortcode attribute. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE-2025-12915	A vulnerability was found in 70mai X200 up to 20251019. This issue affects some unknown processing of the component Init Script Handler. The manipulation results in file inclusion. The attack requires a local approach. A high complexity level is associated with this attack. The exploitability is assessed as difficult. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.4	More Details
CVE-2025-12662	The Coon Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'height' parameter in the 'map' shortcode in all versions up to, and including, 1.0. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11859	The Paypal Donation Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'paypal' shortcode in all versions up to, and including, 0.1. This is due to the plugin not properly sanitizing user input and output of the 'title' and 'text' parameters. 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-2025-12837	The aThemes Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Call To Action widget in versions up to, and including, 1.1.5 due to insufficient input sanitization and output escaping on user-supplied values. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12658	The Preload Current Images plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'complete' parameter in the 'preload_progress_bar' shortcode in all versions up to, and including, 1.3. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9055	The VAPIX Edge storage API that allowed a privilege escalation, enabling a VAPIX administrator-privileged user to gain Linux Root privileges. This flaw can only be exploited after authenticating with an administrator-privileged service account.	6.4	More Details
CVE-2025-12643	The Saphali LiqPay for donate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'saphali_liqpay' shortcode in all versions up to, and including, 1.0.2. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12652	The Ungapped Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'prefillvalues' parameter in the ungapped-form shortcode in all versions up to, and including, 1. This is 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 when a user accesses an injected page.	6.4	More Details
CVE-2025-11805	The Skip to Timestamp plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'skipto' shortcode in all versions up to, and including, 1.4.4. This is due to insufficient input sanitization and output escaping on the 'time' attribute. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user	6.4	More Details

	accesses an injected page.		
CVE-2025-11829	The Five9 Live Chat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'toolbar' attribute of the [five9-chat] shortcode in all versions up to, and including, 1.1.2. This is 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-2025-12663	The Jeba Cute forkit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'text' parameter in the 'jeba_forkit' shortcode in all versions up to, and including, 1.0. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12671	The WP-Iconics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters of the 'wp_iconics' shortcode in all versions up to, and including, 0.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11860	The Twitter Feed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ottwitter_feed' shortcode in all versions up to, and including, 1.3.1. This is due to the plugin not properly sanitizing user input and output of the 'width' and 'height' parameters. 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-2025-35968	Protection mechanism failure in the UEFI firmware for the Slim Bootloader within firmware may allow an escalation of privilege. Startup code and smm adversary with a privileged user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.4	More Details
CVE-2025-12711	The Share to Google Classroom plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the share_to_google shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12672	The Flickr Show plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'div_height' parameter of the 'flickrshow' shortcode in all versions up to, and including, 1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12644	The Nonaki – Drag and Drop Email Template builder and Newsletter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'nonaki' shortcode in all versions up to, and including, 1.0.11. This is due to insufficient input sanitization and output escaping on user supplied custom field values that are retrieved and rendered by the shortcode. This makes it possible for authenticated attackers, with	6.4	More Details

	contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-11821	The Woocommerce – Products By Custom Tax plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'woo_products_custom_tax' shortcode in all versions up to, and including, 2.2. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-11822	The WP Bootstrap Tabs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'bootstrap_tab' shortcode in all versions up to, and including, 1.0.4. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12668	The WP Count Down Timer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple parameters of the 'wp_countdown_timer' shortcode in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12667	The GitHub Gist Shortcode Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter of the 'gist' shortcode in all versions up to, and including, 0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-12922	A vulnerability was found in OpenClinica Community Edition up to 3.12.2/3.13. This affects an unknown part of the file /ImportCRFData?action=confirm of the component CRF Data Import. Performing manipulation of the argument xml_file results in path traversal. The attack can be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-12930	A vulnerability has been found in SourceCodester Food Ordering System 1.0. Affected is an unknown function of the file /view-ticket.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-12862	A vulnerability was identified in projectworlds Online Notes Sharing Platform 1.0. Affected by this issue is some unknown functionality of the file /dashboard/userprofile.php. Such manipulation of the argument image leads to unrestricted upload. The attack may be performed from remote. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-24848	Protection mechanism failure for some Intel(R) CIP software before version WIN_DCA_2.4.0.11001 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with a privileged user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires passive user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.3	More Details

CVE-2025-11216	Inappropriate implementation in Storage in Google Chrome on Mac prior to 141.0.7390.54 allowed a remote attacker to perform domain spoofing via a crafted video file. (Chromium security severity: Low)	6.3	More Details
CVE-2025-43079	The Qualys Cloud Agent included a bundled uninstall script (qagent_uninstall.sh), specific to Linux supported versions that invoked multiple system commands without using absolute paths and without sanitizing the $PATH environment. If the uninstall script is executed with elevated privileges (e.g., via sudo) in an environment where $PATH has been manipulated, an attacker with root/sudo privileges could cause malicious executables to be run in place of the intended system binaries. This behavior can be leveraged for local privilege escalation and arbitrary command execution under elevated privileges.	6.3	More Details
CVE-2025-11208	Inappropriate implementation in Media in Google Chrome prior to 141.0.7390.54 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.3	More Details
CVE-2025-6027	The Ace User Management WordPress plugin through 2.0.3 does not properly validate that a password reset token is associated with the user who requested it, allowing any authenticated users, such as subscriber to reset the password of arbitrary accounts, including administrators.	6.3	More Details
CVE-2025-11212	Inappropriate implementation in Media in Google Chrome on Windows prior to 141.0.7390.54 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform domain spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.3	More Details
CVE-2025-12939	A security flaw has been discovered in SourceCodester Interview Management System up to 1.0. Affected by this issue is some unknown functionality of the file /addCandidate.php. The manipulation of the argument candName results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	6.3	More Details
CVE-2025-33012	IBM Db2 10.5.0 through 10.5.11, 11.1.0 through 11.1.4.7, 11.5.0 through 11.5.9, and 12.1.0 through 12.1.3 for Linux could allow an authenticated user to regain access after account lockout due to password use after expiration date.	6.3	More Details
CVE-2025-12931	A vulnerability was found in SourceCodester Food Ordering System 1.0. Affected by this vulnerability is an unknown functionality of the file /routers/edit-orders.php. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-10567	The FunnelKit WordPress plugin before 3.12.0.1 does not sanitize user input before echoing it back in some of its checkout-related AJAX actions, allowing attackers to conduct reflected XSS attacks against logged-in users.	6.3	More Details
CVE-2025-12916	A vulnerability was determined in Sangfor Operation and Maintenance Security Management System 3.0. Impacted is an unknown function of the file /fort/portal_login of the component Frontend. This manipulation of the argument loginUrl causes command injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 3.0.11 and 3.0.12 is recommended to address this issue. It is advisable to upgrade the affected component.	6.3	More Details
CVE-2025-12926	A weakness has been identified in SourceCodester Farm Management System 1.0. The affected element is an unknown function of the file /review.php. This manipulation of the argument pid causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	6.3	More Details

CVE-2025-60723	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows DirectX allows an authorized attacker to deny service over a network.	6.3	More Details
CVE-2025-11213	Inappropriate implementation in Omnibox in Google Chrome on Android prior to 141.0.7390.54 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform domain spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.3	More Details
CVE-2025-12933	A vulnerability was identified in SourceCodester Baby Care System 1.0. This affects an unknown part of the file /updatewelcome.php?id=siteoptions&action=welcome. Such manipulation of the argument roleid leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-36185	IBM Db2 12.1.0 through 12.1.2 for Linux, UNIX and Windows (includes Db2 Connect Server) could allow a local user to cause a denial of service due to improper neutralization of special elements in data query logic.	6.2	More Details
CVE-2025-12910	Inappropriate implementation in Passkeys in Google Chrome prior to 140.0.7339.80 allowed a local attacker to obtain potentially sensitive information via debug logs. (Chromium security severity: Low)	6.2	More Details
CVE-2025-12829	An uninitialized stack read issue exists in Amazon Ion-C versions <v1.1.4 that may allow a threat actor to craft data and serialize it to Ion text in such a way that sensitive data in memory could be exposed through UTF-8 escape sequences. To mitigate this issue, users should upgrade to version v1.1.4.	6.2	More Details
CVE-2025-12064	The WP2Social Auto Publish plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via PostMessage in all versions up to, and including, 2.4.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-49904	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in magepeopleteam Booking and Rental Manager booking-and-rental-manager-for-woocommerce allows Reflected XSS.This issue affects Booking and Rental Manager: from n/a through <= 2.5.3.	6.1	More Details
CVE-2025-53574	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ptibogxiv Doliconnect doliconnect allows Reflected XSS.This issue affects Doliconnect: from n/a through <= 9.3.2.	6.1	More Details
CVE-2025-12589	The WP-Walla plugin for WordPress is vulnerable to Cross-Site Request Forgery to Stored Cross-Site Scripting in all versions up to, and including, 0.5.3.5. This is due to missing nonce verification on the settings page and insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-12193	The Mang Board WP plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'mp' parameter in all versions up to, and including, 2.3.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-	Due to a Reflected Cross-Site Scripting (XSS) vulnerability in SAP Business Connector, an unauthenticated attacker could generate a malicious link and make it publicly accessible. If an authenticated victim accesses this link, the injected input		More

2025-42886	is processed during web page generation, resulting in the execution of malicious content in the victim's browser context. This could allow the attacker to access or modify information within the victim's browser scope, impacting confidentiality and integrity, while availability remains unaffected	6.1	Details
CVE-2025-12590	The YSlider plugin for WordPress is vulnerable to Cross-Site Request Forgery to Stored Cross-Site Scripting in all versions up to, and including, 1.1. This is due to missing nonce verification on the content configuration page and insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages via a forged request granted they can trick an administrator into performing an action such as clicking on a link. The injected scripts will execute whenever a user accesses an injected page.	6.1	More Details
CVE-2025-49398	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Easy Appointments Easy Appointments easy-appointments allows Code Injection.This issue affects Easy Appointments: from n/a through <= 3.12.14.	6.1	More Details
CVE-2025-49909	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Bookmark & Follow penci-bookmark-follow allows Reflected XSS.This issue affects Penci Bookmark & Follow: from n/a through < 2.4.	6.1	More Details
CVE-2025-11960	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Aryom Software High Technology Systems Inc. KVKNET allows Reflected XSS.This issue affects KVKNET: before 2.1.8.	6.1	More Details
CVE-2025-53239	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bnovotny User Registration Aide user-registration-aide allows Reflected XSS.This issue affects User Registration Aide: from n/a through <= 1.5.3.8.	6.1	More Details
CVE-2025-42893	Due to an Open Redirect vulnerability in SAP Business Connector, an unauthenticated attacker could craft a malicious URL that, if accessed by a victim, redirects them to an attacker-controlled site displayed within an embedded frame. Successful exploitation could allow the attacker to steal sensitive information and perform unauthorized actions, impacting the confidentiality and integrity of web client data. There is no impact to system availability resulting from this vulnerability.	6.1	More Details
CVE-2025-63785	A DOM-based Cross-Site Scripting (XSS) vulnerability exists in the text editor feature of the Onlook web application 0.2.32. This vulnerability occurs because user-supplied input is not properly sanitized before being directly injected into the DOM via innerHTML when editing a text element. An attacker can exploit this to inject malicious HTML and script code, which is then executed within the context of the preview iframe, allowing for the execution of arbitrary scripts in the user's session.	6.1	More Details
CVE-2025-36054	IBM Business Automation Workflow containers 24.0.0 through 24.0.0-IF006, 24.0.1 through 24.0.1-IF004, 25.0.0 through 25.0.0-IF001 and IBM Business Automation Workflow traditional with Process Federation Server 24.0.0 through 24.0.1 and 25.0.0 are vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.1	More Details
CVE-2025-52764	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in marielav flexoslider flexoslider allows Reflected XSS.This issue affects flexoslider: from n/a through <= 1.0004.	6.1	More Details
CVE-2025-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PluginsCafe Range Slider Addon for Gravity Forms range-slider-	6.1	More

49905	addon-for-gravity-forms allows Reflected XSS.This issue affects Range Slider Addon for Gravity Forms: from n/a through <= 1.1.6.		Details
CVE-2025-42924	SAP S/4HANA landscape SAP E-Recruiting BSP allows an unauthenticated attacker to craft malicious links, when clicked the victim could be redirected to the page controlled by the attacker. This has low impact on confidentiality and integrity of the application with no impact on availability.	6.1	More Details
CVE-2025-63418	A DOM-based Cross-Site Scripting (XSS) vulnerability in the SelfBest platform 2023.3 allows attackers to execute arbitrary JavaScript in the context of a logged-in user's session by injecting payloads via the browser's developer console. The vulnerability arises from the application's client-side code being susceptible to direct DOM manipulation without adequate sanitization or a Content Security Policy (CSP), potentially leading to account takeover and data theft.	6.1	More Details
CVE-2025-5770	A reflected cross-site scripting (XSS) vulnerability exists in the authentication endpoints of multiple WSO2 products due to a lack of output encoding. A malicious actor can inject arbitrary JavaScript payloads into the authentication endpoint, which are reflected back in the response, enabling browser-based attacks. Exploitation may result in redirection to malicious websites, UI manipulation, or unauthorized data access from the victim’s browser. However, session-related cookies are protected with the httpOnly flag, which mitigates session hijacking via this vector.	6.1	More Details
CVE-2025-53286	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jhainey Milevis Dropify wc-dropi-integration allows Reflected XSS.This issue affects Dropify: from n/a through <= 4.6.9.	6.1	More Details
CVE-2025-12789	A flaw was found in Red Hat Single Sign-On. This issue is an Open Redirect vulnerability that occurs during the logout process. The redirect_uri parameter associated with the openid-connect logout protocol does not properly validate the provided URL.	6.1	More Details
CVE-2025-12580	The SMS for WordPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'paged' parameter in all versions up to, and including, 1.1.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-12471	The Hubbub Lite – Fast, free social sharing and follow buttons plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'dpsp_list_attention_search' parameter in all versions up to, and including, 1.36.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-10955	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Netcad Software Inc. Netigma allows XSS Through HTTP Query Strings.This issue affects Netigma: from 6.3.5 before 6.3.5 V8.	6.1	More Details
CVE-2025-31146	Time-of-check time-of-use race condition for some Intel Ethernet Adapter Complete Driver Pack software before version 1.5.1.0 within Ring 3: User Applications may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via adjacent access when attack requirements are not present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.1	More Details

CVE-2025-12021	The WP-OAuth plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'error_description' parameter in all versions up to, and including, 0.4.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-64491	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Versions 7.14.7 and below allow unauthenticated reflected Cross-Site Scripting (XSS). Successful exploitation could lead to full account takeover, for example by altering the login form to send credentials to an attacker-controlled server. As a reflected XSS issue, exploitation requires the victim to open a crafted malicious link, which can be delivered via phishing, social media, or other communication channels. This issue is fixed in version 7.14.8.	6.1	More Details
CVE-2025-53349	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Laborator Kalium kalium allows Reflected XSS.This issue affects Kalium: from n/a through <= 3.18.3.	6.1	More Details
CVE-2025-6571	A 3rd-party component exposed its password in process arguments, allowing for low-privileged users to access it.	6.0	More Details
CVE-2025-26405	Improper control of dynamically-managed code resources for some Intel(R) NPU Drivers within Ring 3: User Applications may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires passive user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	5.9	More Details
CVE-2025-12436	Policy bypass in Extensions in Google Chrome prior to 142.0.7444.59 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension. (Chromium security severity: Medium)	5.9	More Details
CVE-2025-43723	Dell PowerScale OneFS, versions prior to 9.10.1.3 and versions 9.11.0.0 through 9.12.0.0, contains a use of a broken or risky cryptographic algorithm vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	5.9	More Details
CVE-2025-42885	Due to missing authentication, SAP HANA 2.0 (hdbrss) allows an unauthenticated attacker to call a remote-enabled function that will enable them to view information. As a result, it has a low impact on the confidentiality but no impact on the integrity and availability of the system.	5.8	More Details
CVE-2025-27712	Improper neutralization for some Intel(R) Neural Compressor software before version v3.4 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (low), integrity (low) and availability (low) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	5.7	More Details
CVE-			

2025-21071	Out-of-bounds write in handling opcode in fingerprint trustlet prior to SMR Nov-2025 Release 1 allows local privileged attackers to write out-of-bounds memory.	5.7	More Details
CVE-2025-31937	Out-of-bounds read for some Intel(R) QAT Windows software before version 2.6.0. within Ring 3: User Applications may allow a denial of service. System software adversary with an authenticated user combined with a high complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	5.6	More Details
CVE-2025-8871	The Everest Forms (Pro) plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.9.7 via deserialization of untrusted input in the mime_content_type() function. This makes it possible for unauthenticated attackers to inject a PHP Object. This vulnerability may be exploited by unauthenticated attackers when a form is present on the site with a non-required signature form field along with an image upload field. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present. This vulnerability is only exploitable in PHP versions prior to 8.	5.6	More Details
CVE-2025-24512	Improper input validation for some Intel(R) PROSet/Wireless WiFi Software for Windows before version 23.160 within Ring 2: Device Drivers may allow a denial of service. Authorized adversary with an authenticated user combined with a high complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are present with special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (low) impacts.	5.6	More Details
CVE-2025-61844	Format Plugins versions 1.1.1 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-61843	Format Plugins versions 1.1.1 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-12439	Inappropriate implementation in App-Bound Encryption in Google Chrome on Windows prior to 142.0.7444.59 allowed a local attacker to obtain potentially sensitive information from process memory via a malicious file. (Chromium security severity: Medium)	5.5	More Details
CVE-2025-62209	Insertion of sensitive information into log file in Windows License Manager allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-60706	Out-of-bounds read in Windows Hyper-V allows an authorized attacker to disclose information locally.	5.5	More Details

CVE-2025-12748	A flaw was discovered in libvirt in the XML file processing. More specifically, the parsing of user provided XML files was performed before the ACL checks. A malicious user with limited permissions could exploit this flaw by submitting a specially crafted XML file, causing libvirt to allocate too much memory on the host. The excessive memory consumption could lead to a libvirt process crash on the host, resulting in a denial-of-service condition.	5.5	More Details
CVE-2025-12632	The RandomQuotr plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2025-59513	Out-of-bounds read in Windows Bluetooth RFCOM Protocol Driver allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-60753	An issue was discovered in libarchive bsdtar before version 3.8.1 in function apply_substitution in file tar/subst.c when processing crafted -s substitution rules. This can cause unbounded memory allocation and lead to denial of service (Out-of-Memory crash).	5.5	More Details
CVE-2025-59510	Improper link resolution before file access ('link following') in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to deny service locally.	5.5	More Details
CVE-2025-59509	Insertion of sensitive information into sent data in Windows Speech allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2025-61845	Format Plugins versions 1.1.1 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-61842	Format Plugins versions 1.1.1 and earlier are affected by a Use After Free vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-42888	SAP GUI for Windows may allow a highly privileged user on the affected client PC to locally access sensitive information stored in process memory during runtime.This vulnerability has a high impact on confidentiality, with no impact on integrity and availability.	5.5	More Details
CVE-2025-26694	Null pointer dereference for some Intel(R) QAT Windows software before version 2.6.0. within Ring 3: User Applications may allow a denial of service. System software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	5.5	More Details
CVE-2025-62208	Insertion of sensitive information into log file in Windows License Manager allows an authorized attacker to disclose information locally.	5.5	More Details

CVE-2025-40760	A vulnerability has been identified in Altair Grid Engine (All versions < V2026.0.0). Affected products do not properly handle error messages and discloses sensitive password hash information when processing user authentication requests. This could allow a local attacker to extract password hashes for privileged accounts, which can then be subjected to offline brute-force attacks.	5.5	More Details
CVE-2025-21076	Improper handling of insufficient permissions or privileges in Samsung Account prior to version 15.5.00.18 allows local attackers to access data in Samsung Account. User interaction is required for triggering this vulnerability.	5.5	More Details
CVE-2025-59240	Exposure of sensitive information to an unauthorized actor in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	5.5	More Details
CVE-2025-27249	Uncontrolled resource consumption for some Gaudi software before version 1.21.0 within Ring 3: User Applications may allow a denial of service. System software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	5.5	More Details
CVE-2025-61840	Format Plugins versions 1.1.1 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-61841	Format Plugins versions 1.1.1 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to access sensitive memory information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-53245	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Afzal Multani WP Logo Changer am-login-logo allows Stored XSS.This issue affects WP Logo Changer: from n/a through <= 1.2.	5.4	More Details
CVE-2025-42889	SAP Starter Solution allows an authenticated attacker to execute crafted database queries, thereby exposing the back-end database. As a result, this vulnerability has a low impact on the application's confidentiality and integrity but no impact on its availability.	5.4	More Details
CVE-2025-53324	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodeYatri Gutenify gutenify allows Stored XSS.This issue affects Gutenify: from n/a through <= 1.5.7.	5.4	More Details
CVE-2025-12126	The The Total Book Project plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.0 via several functions due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Contributor-level access and above, to perform several actions like moving/deleting/creating chapters in books that do not belong to them.	5.4	More Details
CVE-2025-64687	In JetBrains YouTrack before 2025.3.104432 improper access control allowed modify MCP tool logic	5.4	More Details
	The Slippy Slider – Responsive Touch Navigation Slider plugin for WordPress is		

CVE-2025-11874	vulnerable to Stored Cross-Site Scripting via the plugin's 'slippy-slider' shortcode in all versions up to, and including, 2.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2025-12435	Incorrect security UI in Omnibox in Google Chrome on Android prior to 142.0.7444.59 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-2025-64690	In JetBrains YouTrack before 2025.3.104432 insecure Junie configuration could lead to data exposure and unauthorized changes	5.4	More Details
CVE-2025-12880	The Progress Bar Blocks for Gutenberg plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	5.4	More Details
CVE-2025-31029	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bingu replyMail replymail allows Stored XSS.This issue affects replyMail: from n/a through <= 1.2.0.	5.4	More Details
CVE-2025-31954	HCL iAutomate v6.5.1 and v6.5.2 is susceptible to a sensitive information disclosure. An HTTP GET method is used to process a request and includes sensitive information in the query string of that request. An attacker could potentially access information or resources they were not intended to see.	5.4	More Details
CVE-2025-61261	A reflected cross-site scripting (XSS) vulnerability in CKeditor v46.1.0 & Angular v18.0.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload.	5.4	More Details
CVE-2025-12905	Inappropriate implementation in Downloads in Google Chrome on Windows prior to 140.0.7339.80 allowed a remote attacker to bypass Mark of the Web via a crafted HTML page. (Chromium security severity: Low)	5.4	More Details
CVE-2025-20304	Multiple vulnerabilities in the web-based management interface of Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to conduct a reflected XSS attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker must have at least a low-privileged account on the affected device.	5.4	More Details
CVE-2025-64177	ThinkDashboard is a self-hosted bookmark dashboard built with Go and vanilla JavaScript. In versions 0.6.7 and below, there is a stored Cross-Site Scripting (XSS) vulnerability in the dashboard, which can exploited when a user clicks on a malicious bookmark, made vulnerable by the lack of scheme filtering. This is fixed in version 0.6.8.	5.4	More Details
CVE-2025-	Multiple vulnerabilities in the web-based management interface of Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to conduct a reflected XSS attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit	5.4	More Details

20303	could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker must have at least a low-privileged account on the affected device.		
CVE-2025-12908	Insufficient validation of untrusted input in Downloads in Google Chrome on Android prior to 140.0.7339.80 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	5.4	More Details
CVE-2025-11210	Side-channel information leakage in Tab in Google Chrome prior to 141.0.7390.54 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-2024-12125	A flaw was found in the 3scale developer portal. This issue can allow account creation or updates passed through hidden or read-only fields, the contents of which may be altered. This flaw allows an attacker to access or modify restricted information.	5.4	More Details
CVE-2025-12906	Inappropriate implementation in Permissions in Google Chrome prior to 140.0.7339.80 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	5.4	More Details
CVE-2025-33110	IBM OpenPages 9.1, and 9.0 with Watson is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site.	5.4	More Details
CVE-2025-36135	IBM Sterling B2B Integrator 6.0.0.0 through 6.1.2.7_1, 6.2.0.0 through 6.2.0.5, and 6.2.1.0 and IBM Sterling File Gateway 6.0.0.0 through 6.1.2.7_1, 6.2.0.0 through 6.2.0.5, and 6.2.1.0 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2025-58337	An attacker with a valid read-only account can bypass Doris MCP Server’s read-only mode due to improper access control, allowing modifications that should have been prevented by read-only restrictions. Impact: Bypasses read-only mode; attackers with read-only access may perform unauthorized modifications. Recommended action for operators: Upgrade to version 0.6.0 as soon as possible (this release contains the fix).	5.4	More Details
CVE-2025-49390	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in christophrado Cookie Notice & Consent cookie-notice-consent allows Stored XSS.This issue affects Cookie Notice & Consent: from n/a through <= 1.6.4.	5.4	More Details
CVE-2025-57244	OpenKM Community Edition 6.3.12 is vulnerable to stored cross-site scripting (XSS) in the user account creation interface. The Name field accepts script tags and the Email field is vulnerable when the POST request is modified to include encoded script tags, by passing frontend validation.	5.4	More Details
CVE-2025-62017	Missing Authorization vulnerability in hogash Kallyas kallyas.This issue affects Kallyas: from n/a through <= 4.22.0.	5.4	More Details
CVE-2025-10259	Improper Validation of Specified Quantity in Input vulnerability in TCP Communication Function on Mitsubishi Electric Corporation MELSEC iQ-F Series CPU module allows a remote attacker to disconnect the connection by sending specially crafted TCP packets to cause a denial-of-service (DoS) condition on the products. There is no impact on connections other than the attacked one.	5.3	More Details
	Due to information disclosure vulnerability in anonymous API provided by SAP		

CVE-2025-42897	Business One (SLD), an attacker with normal user access could gain access to unauthorized information. As a result, it has a low impact on the confidentiality of the application but no impact on the integrity and availability.	5.3	More Details
CVE-2025-62018	Missing Authorization vulnerability in hogash Kallyas kallyas.This issue affects Kallyas: from n/a through <= 4.22.0.	5.3	More Details
CVE-2025-33150	IBM Cognos Analytics Certified Containers 12.1.0 could disclose package parameter information due to the presence of hidden pages.	5.3	More Details
CVE-2025-12676	The KiotViet Sync plugin for WordPress is vulnerable to authorizarion bypass in all versions up to, and including, 1.8.5. This is due to the plugin using a hardcoded password for authentication in the QueryControllerAdmin::authenticated function. This makes it possible for unauthenticated attackers to create and sync products.	5.3	More Details
CVE-2025-64323	kgateway is a Cloud-Native API and AI Gateway. Versions 2.0.4 and below and 2.1.0-agw-cel-rbac through 2.1.0-rc.2 lack authentication, allowing any client with unrestricted network access to the xDS port to retrieve potentially sensitive configuration data including certificate data, backend service information, routing rules, and cluster metadata. This issue is solved in versions 2.0.5 and 2.1.0.	5.3	More Details
CVE-2025-11999	The Add Multiple Marker plugin for WordPress is vulnerable to unauthorized modification of data to due to a missing capability check on the addmultiplemarker_reset_map() and amm_save_map_api() functions in all versions up to, and including, 1.2. This makes it possible for unauthenticated attackers to update the map API and reset maps.	5.3	More Details
CVE-2025-12192	The Events Calendar plugin for WordPress is vulnerable to information disclosure in versions up to, and including, 6.15.9. The sysinfo REST endpoint compares the provided key to the stored opt-in key using a loose comparison, allowing unauthenticated attackers to send a boolean value and obtain the full system report whenever "Yes, automatically share my system information with The Events Calendar support team" setting is enabled.	5.3	More Details
CVE-2025-11997	The Document Pro Elementor – Documentation & Knowledge Base plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.0.9. This is due to the plugin exposing sensitive Algolia API keys through the frontend JavaScript code via wp_localize_script without proper access restrictions. This makes it possible for unauthenticated attackers to view sensitive API keys in the page source, which could be leveraged to make unauthorized API calls to the configured Algolia search service.	5.3	More Details
CVE-2025-11532	The Wisly plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.0.0 due to missing validation on the 'wishlist_id' user controlled key. This makes it possible for unauthenticated attackers to remove and add items to other user's wishlists.	5.3	More Details
CVE-2025-11271	The Easy Digital Downloads plugin for WordPress is vulnerable to Order Manipulation in all versions up to, and including, 3.5.2 due to an order verification bypass. The verification is unconditionally skipped when the POST body includes verification_override=1. Because this value is attacker-supplied, an unauthenticated actor can submit a forged IPN and have it treated as verified, even on production sites and with verification otherwise enabled. A valid PayPal transaction id is needed, restricting order manipulation to orders placed by the attacker. This, in turn, requires them to have a customer account.	5.3	More Details
	The Crypto plugin for WordPress is vulnerable to unauthorized manipulation of data		

CVE-2025-11988	in all versions up to, and including, 2.22. This is due to the plugin registering an unauthenticated AJAX action (wp_ajax_nopriv_crypto_connect_ajax_process) that allows calling the crypto_delete_json method with only a publicly-available nonce check. This makes it possible for unauthenticated attackers to delete specific JSON files matching the pattern *_pending.json within the wp-content/uploads/yak/ directory, causing data loss and denial of service for plugin workflows that rely on these artifacts.	5.3	More Details
CVE-2025-11996	The Find Unused Images plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the fui_delete_image() and fui_delete_all_images() functiosn in all versions up to, and including, 1.0.7. This makes it possible for unauthenticated attackers to delete all of a site's attachments.	5.3	More Details
CVE-2025-42919	Due to an Information Disclosure vulnerability in SAP NetWeaver Application Server Java, internal metadata files could be accessed via manipulated URLs. An unauthenticated attacker could exploit this vulnerability by inserting arbitrary path components in the request, allowing unauthorized access to sensitive application metadata. This results in a partial compromise of the confidentiality of the information without affecting the integrity or availability of the application server.	5.3	More Details
CVE-2025-46365	Dell CloudLink, versions prior 8.1.1, contain a Command Injection vulnerability which can be exploited by an Authenticated attacker to cause Command Injection on an affected Dell CloudLink.	5.3	More Details
CVE-2025-11835	The Paid Membership Subscriptions – Effortless Memberships, Recurring Payments & Content Restriction plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability and validation check on the PMS_AJAX_Checkout_Handler::process_payment() function in all versions up to, and including, 2.16.4. This makes it possible for unauthenticated attackers to trigger stored auto-renew charges for arbitrary members.	5.3	More Details
CVE-2025-59716	ownCloud Guests before 0.12.5 allows unauthenticated user enumeration via the /apps/guests/register/{email}/{token} endpoint. Because of insufficient validation of the supplied token in showPasswordForm, the server responds differently when an e-mail address corresponds to a valid pending guest user rather than a non-existent user.	5.3	More Details
CVE-2025-64327	ThinkDashboard is a self-hosted bookmark dashboard built with Go and vanilla JavaScript. Versions 0.6.7 and below contain a Blind Server-Side Request Forgery (SSRF) vulnerability, in its `/api/ping?url= endpoint`. This allows an attacker to make arbitrary requests to internal or external hosts. This can include discovering ports open on the local machine, hosts on the local network, and ports open on the hosts on the internal network. This issue is fixed in version 0.6.8.	5.3	More Details
CVE-2025-12745	A weakness has been identified in QuickJS up to eb2c89087def1829ed99630cb14b549d7a98408c. This affects the function js_array_buffer_slice of the file quickjs.c. This manipulation causes buffer over-read. The attack is restricted to local execution. The exploit has been made available to the public and could be exploited. This product adopts a rolling release strategy to maintain continuous delivery Patch name: c6fe5a98fd3ef3b7064e6e0145dfebfe12449fea. To fix this issue, it is recommended to deploy a patch.	5.3	More Details
CVE-2025-64176	ThinkDashboard is a self-hosted bookmark dashboard built with Go and vanilla JavaScript. In versions 0.6.7 and below, an attacker can upload any file they wish to the /data directory of the web application via the backup import feature. When importing a backup, an attacker can first choose a .zip file to bypass the client-side file-type verification. This could lead to stored XSS, or be used for other nefarious purposes such as malware distribution. This issue is fixed in version 0.6.8.	5.3	More Details

CVE-2025-11891	The Shelf Planner plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.7.0 through publicly exposed log files. This makes it possible for unauthenticated attackers to view potentially sensitive information contained in the exposed log files.	5.3	More Details
CVE-2025-12677	The KiotViet Sync plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.8.5 via the register_api_route() function in kiotvietsync/includes/public_actions/WebHookAction.php. This makes it possible for unauthenticated attackers to extract the webhook token value when configured.	5.3	More Details
CVE-2025-11894	The Shelf Planner plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several REST API endpoints in all versions up to, and including, 2.7.0. This makes it possible for unauthenticated attackers to modify several of the plugin's settings like the ServerKey and LicenseKey.	5.3	More Details
CVE-2025-11986	The Crypto plugin for WordPress is vulnerable to Information exposure in all versions up to, and including, 2.22. This is due to the plugin registering an unauthenticated AJAX action (wp_ajax_nopriv_crypto_connect_ajax_process) that allows calling the register and savenft methods with only a publicly-available nonce check and no wallet signature verification. This makes it possible for unauthenticated attackers to set a site-wide global authentication state via a single transient, bypassing all access controls for ALL visitors to the site. The impact is complete bypass of [crypto-block] shortcode restrictions and page-level access controls, affecting all site visitors for one hour, plus the ability to inject arbitrary data into the plugin's custom_users table.	5.3	More Details
CVE-2025-64179	lakeFS is an open-source tool that transforms object storage into a Git-like repositories. In versions 1.69.0 and below, missing authentication in the /api/v1/usage-report/summary endpoint allows anyone to retrieve aggregate API usage counts. While no sensitive data is disclosed, the endpoint may reveal information about service activity or uptime. This issue is fixed in version 1.71.0 . To workaround the vulnerability, use a load-balancer or application level firewall in order to block the request route /api/v1/usage-report/summary.	5.3	More Details
CVE-2025-12440	Inappropriate implementation in Autofill in Google Chrome prior to 142.0.7444.59 allowed a remote attacker who convinced a user to engage in specific UI gestures to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	5.3	More Details
CVE-2025-55342	Quipux 4.0.1 through e1774ac allows enumeration of usernames, and accessing the Ecuadorean identification number for all registered users via the Administracion/usuarios/cambiar_password_olvido_validar.php txt_login parameter.	5.3	More Details
CVE-2025-12468	The FunnelKit Automations – Email Marketing Automation and CRM for WordPress & WooCommerce plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.6.4.1 via the '/wc-coupons/' REST API endpoint. This is due to the endpoint being marked as a public API (`public_api = true`), which results in the endpoint being registered with `permission_callback => '__return_true'`, bypassing all authentication and capability checks. This makes it possible for unauthenticated attackers to extract sensitive data including all WooCommerce coupon codes, coupon IDs, and expiration status.	5.3	More Details
CVE-2025-33185	NVIDIA AIStore contains a vulnerability in AuthN where an unauthenticated user may cause information disclosure. A successful exploit of this vulnerability may lead to information disclosure.	5.3	More Details
CVE-	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 8.6.0		

2025-12560	via the getFullContent() 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.	5.3	More Details
CVE-2025-2534	IBM Db2 11.1.0 through 11.1.4.7, 11.5.0 through 11.5.9, and 12.1.0 through 12.1.3 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.	5.3	More Details
CVE-2025-10873	The ElementInvader Addons for Elementor WordPress plugin before 1.4.1 allows unauthenticated user to send arbitrary e-mails to arbitrary addresses due to missing authorization on the elementinvader_addons_for_elementor_forms_send_form action.	5.3	More Details
CVE-2025-64683	In JetBrains Hub before 2025.3.104432 information disclosure was possible via the Users API	5.3	More Details
CVE-2025-12788	The Hydra Booking — Appointment Scheduling & Booking Calendar plugin for WordPress is vulnerable to missing payment verification to unauthenticated payment bypass in all versions up to, and including, 1.1.27. This is due to the plugin accepting client-controlled payment confirmation data in the tfhb_meeting_paypal_payment_confirmation_callback function without server-side verification with PayPal's API. This makes it possible for unauthenticated attackers to bypass payment requirements and confirm bookings as paid without any actual payment transaction occurring.	5.3	More Details
CVE-2025-12787	The Hydra Booking — Appointment Scheduling & Booking Calendar plugin for WordPress is vulnerable to unauthorized booking cancellation in all versions up to, and including, 1.1.27. This is due to the plugin's "tfhb_meeting_form_submit_callback" function using insufficiently random values to generate booking cancellation tokens, combined with a globally shared nonce. This makes it possible for unauthenticated attackers to cancel arbitrary bookings via brute force attacks against the tfhb_meeting_form_cencel AJAX endpoint.	5.3	More Details
CVE-2025-12098	The Academy LMS – WordPress LMS Plugin for Complete eLearning Solution plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.3.8 via the 'enqueue_social_login_script' function. This makes it possible for unauthenticated attackers to extract sensitive data including the Facebook App Secret if Facebook Social Login is enabled.	5.3	More Details
CVE-2025-11072	The MelAbu WP Download Counter Button WordPress plugin through 1.8.6.7 does not validate the path of files to be downloaded, which could allow unauthenticated attacker to read/download arbitrary files.	5.3	More Details
CVE-2025-7700	A flaw was found in FFmpeg’s ALS audio decoder, where it does not properly check for memory allocation failures. This can cause the application to crash when processing certain malformed audio files. While it does not lead to data theft or system control, it can be used to disrupt services and cause a denial of service.	5.3	More Details
CVE-2025-12875	A weakness has been identified in mruby 3.4.0. This vulnerability affects the function ary_fill_exec of the file mrbgems/mruby-array-ext/src/array.c. Executing manipulation of the argument start/length can lead to out-of-bounds write. The attack needs to be launched locally. The exploit has been made available to the public and could be exploited. This patch is called 93619f06dd378db6766666b30c08978311c7ec94. It is best practice to apply a patch to resolve this issue.	5.3	More Details
	The Flexible Refund and Return Order for WooCommerce plugin for WordPress is		

CVE-2025-12621	vulnerable to unauthorized modification of data due to a misconfigured capability check on the 'create_refund' function in all versions up to, and including, 1.0.42. This makes it possible for authenticated attackers, with Contributor-level access and above, to update the status of refund requests, including approving and refusing refunds.	5.3	More Details
CVE-2025-58243	Missing Authorization vulnerability in Jthemes imEvent imevent allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects imEvent: from n/a through <= 3.4.0.	5.3	More Details
CVE-2025-12353	The WPFunnels – The Easiest Funnel Builder For WordPress And WooCommerce To Collect Leads And Increase Sales plugin for WordPress is vulnerable to unauthorized user registration in all versions up to, and including, 3.6.2. This is due to the plugin relying on a user controlled value 'optin_allow_registration' to determine if user registration is allowed, instead of the site-specific setting. This makes it possible for unauthenticated attackers to register new user accounts, even when user registration is disabled.	5.3	More Details
CVE-2025-12177	The Download Manager plugin for WordPress is vulnerable to unauthorized access due to a hardcoded Cron key used in the deleteExpired() and clearTempDataCPCron() functions in all versions up to, and including, 3.3.30. This makes it possible for unauthenticated attackers to trigger these cron jobs leading to deletion of expired posts and clearing cache.	5.3	More Details
CVE-2025-12042	The Course Booking System plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check in the csv-export.php file in all versions up to, and including, 6.1.5. This makes it possible for unauthenticated attackers to directly access the file and obtain an export of all booking data.	5.3	More Details
CVE-2025-12909	Insufficient policy enforcement in Devtools in Google Chrome prior to 140.0.7339.80 allowed a remote attacker to leak cross-origin data via Devtools. (Chromium security severity: Low)	5.3	More Details
CVE-2025-64435	KubeVirt is a virtual machine management add-on for Kubernetes. Prior to 1.7.0-beta.0, a logic flaw in the virt-controller allows an attacker to disrupt the control over a running VMI by creating a pod with the same labels as the legitimate virt-launcher pod associated with the VMI. This can mislead the virt-controller into associating the fake pod with the VMI, resulting in incorrect status updates and potentially causing a DoS (Denial-of-Service). This vulnerability is fixed in 1.7.0-beta.0.	5.3	More Details
CVE-2025-10853	A reflected cross-site scripting (XSS) vulnerability exists in the management console of multiple WSO2 products due to improper output encoding. By tampering with specific parameters, a malicious actor can inject arbitrary JavaScript into the response, leading to reflected XSS. Successful exploitation could result in UI manipulation, redirection to malicious websites, or data theft from the browser. However, session-related sensitive cookies are protected with the httpOnly flag, which mitigates the risk of session hijacking.	5.2	More Details
CVE-2025-31719	In TEE EcDSA algorithm, there is a possible memory consistency issue. This could lead to generated incorrect signature results with low probability.	5.1	More Details
CVE-2025-36136	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.3 for Linux, UNIX and Windows (includes DB2 Connect Server) could allow a local user to cause a denial of service due to the database monitor script incorrectly detecting that the instance is still starting under specific conditions.	5.1	More Details
	Langfuse is an open source large language model engineering platform. Starting in		

CVE-2025-64504	version 2.70.0 and prior to versions 2.95.11 and 3.124.1, in certain project membership APIs, the server trusted a user-controlled orgId and used it in authorization checks. As a result, any authenticated user on the same Langfuse instance could enumerate names and email addresses of users in another organization if they knew the target organization’s ID. Disclosure is limited to names and email addresses of members/invitees. No customer data such as traces, prompts, or evaluations is exposed or accessible. For Langfuse Cloud, the maintainers ran a thorough investigation of access logs of the last 30 days and could not find any evidence that this vulnerability was exploited. For most self-hosting deployments, the attack surface is significantly reduced given an SSO provider is configured and email/password sign-up is disabled. In these cases, only users who authenticate via the Enterprise SSO IdP (e.g. Okta) would be able to exploit this vulnerability to access the member list, i.e. internal users getting access to a list of other internal users. In order to exploit the vulnerability, the actor must have a valid Langfuse user account within the same instance, know the target orgId, and use the request made to the API that powers the frontend membership tables, including their project/user authentication token, while changing the orgId to the target organization. Langfuse Cloud (EU, US, HIPAA) were affected until fix deployment on November 1, 2025. The maintainers reviewed the Langfuse Cloud access logs from the past 30 days and found no evidence that this vulnerability was exploited. Self-Hosted versions which contain patches include v2.95.11 for major version 2 and v3.124.1 for major version 3. There are no known workarounds. Upgrading is required to fully mitigate this issue.	5.0	More Details
CVE-2025-62453	Improper validation of generative ai output in GitHub Copilot and Visual Studio Code allows an authorized attacker to bypass a security feature locally.	5.0	More Details
CVE-2025-64437	KubeVirt is a virtual machine management add-on for Kubernetes. In versions before 1.5.3 and 1.6.1, the virt-handler does not verify whether the launcher-sock is a symlink or a regular file. This oversight can be exploited, for example, to change the ownership of arbitrary files on the host node to the unprivileged user with UID 107 (the same user used by virt-launcher) thus, compromising the CIA (Confidentiality, Integrity and Availability) of data on the host. To successfully exploit this vulnerability, an attacker should be in control of the file system of the virt-launcher pod. This vulnerability is fixed in 1.5.3 and 1.6.1.	5.0	More Details
CVE-2025-11972	The Tag, Category, and Taxonomy Manager – AI Autotagger with OpenAI plugin for WordPress is vulnerable to SQL Injection via the 'post_types' parameter in all versions up to, and including, 3.40.0 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 Editor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2025-20374	A vulnerability in the web UI of Cisco Unified CCX could allow an authenticated, remote attacker to perform a directory traversal and access arbitrary resources. This vulnerability is due to an insufficient input validation associated to specific UI features. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to arbitrary files on the underlying operating system. To exploit this vulnerability, the attacker must have valid administrative credentials.	4.9	More Details
CVE-2025-11980	The Quick Featured Images plugin for WordPress is vulnerable to SQL Injection via the 'delete_orphaned' function in all versions up to, and including, 13.7.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Editor-level access and above, to append additional SQL queries into	4.9	More Details

	already existing queries that can be used to extract sensitive information from the database, granted they can convince an author-level user or higher to add a malicious custom field value.		
CVE-2025-10683	The Easy Email Subscription plugin for WordPress is vulnerable to SQL Injection via the 'uid' parameter in all versions up to, and including, 1.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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-2025-12020	The Double the Donation – A workplace giving tool to help your fundraising efforts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.9	More Details
CVE-2025-60187	Unrestricted Upload of File with Dangerous Type vulnerability in Vito Peleg Atarim atarim-visual-collaboration allows Using Malicious Files.This issue affects Atarim: from n/a through <= 4.2.	4.8	More Details
CVE-2025-20289	Multiple vulnerabilities in the web-based management interface of Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to conduct a reflected XSS attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker must have at least a low-privileged account on the affected device.	4.8	More Details
CVE-2025-12873	A security flaw has been discovered in Campcodes School File Management 1.0. This affects an unknown part of the file /admin/update_user.php. Performing manipulation of the argument user_id results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	4.7	More Details
CVE-2025-12856	A weakness has been identified in code-projects Responsive Hotel Site 1.0. Impacted is an unknown function of the file /admin/reservation.php. This manipulation of the argument email causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	4.7	More Details
CVE-2025-12914	A vulnerability has been found in aaPanel BaoTa up to 11.1.0. This vulnerability affects unknown code of the file /database?action=GetDatabaseAccess of the component Backend. The manipulation of the argument Name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-12927	A security vulnerability has been detected in DedeBIZ up to 6.3.2. The impacted element is an unknown function of the file /admin/archives_add.php. Such manipulation of the argument flags[] leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	4.7	More Details
CVE-	A vulnerability was determined in SourceCodester Baby Care System 1.0. Affected by this issue is some unknown functionality of the file /admin.php?id=inbox. This		More

2025-12932	manipulation of the argument msgid causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	4.7	Details
CVE-2025-64432	KubeVirt is a virtual machine management add-on for Kubernetes. Versions 1.5.3 and below, and 1.6.0 contained a flawed implementation of the Kubernetes aggregation layer's authentication flow which could enable bypass of RBAC controls. It was discovered that the virt-api component fails to correctly authenticate the client when receiving API requests over mTLS. In particular, it fails to validate the CN (Common Name) field in the received client TLS certificates against the set of allowed values defined in the extension-apiserver-authentication configmap. Failre to validate certain fields in the client TLS certificate may allow an attacker to bypass existing RBAC controls by directly communicating with the aggregated API server, impersonating the Kubernetes API server and its aggregator component. This issue is fixed in versions 1.5.3 and 1.6.1.	4.7	More Details
CVE-2025-12861	A vulnerability was determined in DedeBIZ up to 6.3.2. Affected by this vulnerability is an unknown functionality of the file /admin/spec_add.php. This manipulation of the argument flags[] causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2025-12860	A vulnerability was found in DedeBIZ up to 6.3.2. Affected is an unknown function of the file /admin/freelist_main.php. The manipulation of the argument orderby results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	4.7	More Details
CVE-2025-12913	A flaw has been found in code-projects Responsive Hotel Site 1.0. This affects an unknown part of the file /admin/roomdel.php. Executing 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.	4.7	More Details
CVE-2025-12859	A vulnerability has been found in DedeBIZ up to 6.3.2. This impacts an unknown function of the file /admin/templets_one_edit.php. The manipulation of the argument ids leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2025-12855	A security flaw has been discovered in code-projects Responsive Hotel Site 1.0. This issue affects some unknown processing of the file /admin/newsletterdel.php. The manipulation of the argument eid results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	4.7	More Details
CVE-2025-12853	A vulnerability was determined in SourceCodester Best House Rental Management System 1.0. This affects the function delete_house of the file /admin_class.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2025-12857	A security vulnerability has been detected in code-projects Responsive Hotel Site 1.0. The affected element is an unknown function of the file /admin/roombook.php. Such manipulation of the argument rid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	4.7	More Details
CVE-2025-64434	KubeVirt is a virtual machine management add-on for Kubernetes. Prior to 1.5.3 and 1.6.1, due to the peer verification logic in virt-handler (via verifyPeerCert), an attacker who compromises a virt-handler instance, could exploit these shared credentials to impersonate virt-api and execute privileged operations against other virt-handler instances potentially compromising the integrity and availability of the VM managed by it. This vulnerability is fixed in 1.5.3 and 1.6.1.	4.7	More Details
	A vulnerability has been identified in Spectrum Power 4 (All versions < V4.70 SP12		

CVE-2024-32014	Update 2). The affected application is vulnerable to alter the local database which contains the application credentials. This allows an attacker to gain administrative application privileges.	4.7	More Details
CVE-2025-64494	Soft Serve is a self-hostable Git server for the command line. In versions prior to 0.10.0, there are several places where the user can insert data (e.g. names) and ANSI escape sequences are not being removed, which can then be used, for example, to show fake alerts. In the same token, git messages, when printed, are also not being sanitized. This issue is fixed in version 0.10.0.	4.6	More Details
CVE-2025-43418	This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 18.7.2 and iPadOS 18.7.2. An attacker with physical access to a locked device may be able to view sensitive user information.	4.6	More Details
CVE-2025-36131	IBM Db2 11.1.0 through 11.1.4.7, 11.5.0 through 11.5.9, and 12.1.0 through 12.1.3 for Linux, UNIX and Windows (includes Db2 Connect Server) clpplus command exposes user credentials to the terminal which could be obtained by a third party with physical access to the system.	4.6	More Details
CVE-2025-24516	Improper access control for some Intel(R) CIP software before version WIN_DCA_2.4.0.11001 within Ring 3: User Applications may allow an information disclosure. Unprivileged software adversary with a privileged user combined with a low complexity attack may enable data exposure. This result may potentially occur via adjacent access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	4.5	More Details
CVE-2025-24847	Improper input validation for some Intel(R) CIP software before version WIN_DCA_2.4.0.11001 within Ring 3: User Applications may allow an information disclosure. Unprivileged software adversary with a privileged user combined with a low complexity attack may enable data exposure. This result may potentially occur via network access when attack requirements are present without special internal knowledge and requires passive user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	4.5	More Details
CVE-2025-12125	The HTML Forms – Simple WordPress Forms Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.5.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-20056	Improper input validation for some Intel VTune Profiler before version 2025.1 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable data manipulation. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (low) and availability (low) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	4.4	More Details
	Time-of-check time-of-use race condition for some ACAT before version 3.13 within		

CVE-2025-27725	Ring 3: User Applications may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	4.4	More Details
CVE-2025-12019	The Featured Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via image metadata in all versions up to, and including, 2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-12896	Improper resource management in firmware of some Solidigm DC Products may allow an attacker with local or physical access to gain un-authorized access to a locked storage device.	4.4	More Details
CVE-2025-12902	Improper resource management in firmware of some Solidigm DC Products may allow an attacker with local or physical access to gain un-authorized access to a locked Storage Device or create a Denial of Service.	4.4	More Details
CVE-2025-10905	Collision in MiniFilter driver in Avast Software Avast Free Antivirus before 25.9 on Windows allows a local attacker with administrative privileges to disable real-time protection and self-defense mechanisms.	4.4	More Details
CVE-2025-12631	The Squirrels Auto Inventory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-12538	The Fleet Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.5.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2025-12582	The Features plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'features_revert_option AJAX endpoint in all versions up to, and including, 0.0.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to revert options.	4.3	More Details
CVE-2025-20305	A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability exists because certain files lack proper data protection mechanisms. An attacker with read-only Administrator privileges could exploit this vulnerability by performing actions where the results should only be viewable to a high-privileged user. A successful exploit could allow the attacker to view passwords that are normally not visible to read-only administrators.	4.3	More Details
	The FunnelKit Automations – Email Marketing Automation and CRM for WordPress & WooCommerce plugin for WordPress is vulnerable to Missing Authorization in all		

CVE-2025-12469	versions up to, and including, 3.6.4.1. This is due to the plugin not properly verifying that a user is authorized to perform administrative actions in the `bwfan_test_email` AJAX handler. The nonce used for verification is publicly exposed to all visitors (including unauthenticated users) via the frontend JavaScript localization, and the `check_nonce()` function accepts low-privilege authenticated users who possess this nonce. This makes it possible for authenticated attackers, with Subscriber-level access and above, to send arbitrary emails from the site with attacker-controlled subject and body content.	4.3	More Details
CVE-2025-20377	A vulnerability in the API subsystem of Cisco Unified Intelligence Center could allow an authenticated, remote attacker to obtain sensitive information from an affected system. This vulnerability is due to improper validation of requests to certain API endpoints. An attacker could exploit this vulnerability by sending a valid request to a specific API endpoint within the affected system. A successful exploit could allow a low-privileged user to view sensitive information on the affected system that should be restricted. To exploit this vulnerability, the attacker must have valid user credentials on the affected system.	4.3	More Details
CVE-2025-11886	The CTL Arcade Lite plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incorrect nonce validation on the 'ctl_arcade_lite_page_manage_games' page. This makes it possible for unauthenticated attackers to deactivate and activate arbitrary plugins via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-60728	Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to disclose information over a network.	4.3	More Details
CVE-2025-10691	The Easy Email Subscription plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3. This is due to missing or incorrect nonce validation on the show_editsub_page() function. This makes it possible for unauthenticated attackers to delete arbitrary subscribers via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-12132	The WP Custom Admin Login Page Logo plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4.8.4. This is due to missing or incorrect nonce validation on the wpclpl_save functionality. This makes it possible for unauthenticated attackers to modify the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-12526	The Private Google Calendars plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'pgc_remove' action in all versions up to, and including, 20250811. This makes it possible for authenticated attackers, with Subscriber-level access and above, to reset the plugin's settings.	4.3	More Details
CVE-2025-12588	The USB Qr Code Scanner For Woocommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing nonce validation on the settings page. This makes it possible for unauthenticated attackers to update the plugin's settings via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-12563	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to limited file upload due to an incorrect capability check on theuploadVideo() function in all versions up to, and including, 8.6.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to	4.3	More Details

	upload mp4 files to the 'wp-content/uploads/<YYYY>/<MM>/' directory.		
CVE-2025-12360	The Better Find and Replace – AI-Powered Suggestions plugin for WordPress is vulnerable to unauthorized API usage due to a missing capability check on the rtafar_ajax() function in all versions up to, and including, 1.7.7. This makes it possible for authenticated attackers, with Subscriber-level access, to trigger OpenAI API key usage resulting in quota consumption potentially incurring cost.	4.3	More Details
CVE-2025-11268	The Strong Testimonials plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 3.2.16. This is due to the software allowing users to submit a testimonial in which a value is not properly validated or sanitized prior to being passed to a do_shortcode call. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes if an administrator previews or publishes a crafted testimonial.	4.3	More Details
CVE-2025-12665	The Ninja Countdown | Fastest Countdown Builder plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'ninja_countdown_admin_ajax' AJAX endpoint in all versions up to, and including, 1.5.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary countdowns.	4.3	More Details
CVE-2025-9524	The VAPIX API port.cgi did not have sufficient input validation, which may result in process crashes and impact usability. This vulnerability can only be exploited after authenticating with a viewer- operator- or administrator-privileged service account.	4.3	More Details
CVE-2025-12953	The Classified Listing – AI-Powered Classified ads & Business Directory Plugin plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the "rtcl_ajax_add_listing_type", "rtcl_ajax_update_listing_type", and "rtcl_ajax_delete_listing_type" function in all versions up to, and including, 5.2.0. This makes it possible for authenticated attackers, with subscriber level access and above, to add, update, or delete listing types.	4.3	More Details
CVE-2025-12443	Out of bounds read in WebXR in Google Chrome prior to 142.0.7444.59 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2025-21075	Out-of-bounds write in libimagecodec.quram.so prior to SMR Nov-2025 Release 1 allows remote attackers to access out-of-bounds memory.	4.3	More Details
CVE-2025-64684	In JetBrains YouTrack before 2025.3.104432 information disclosure was possible via the feedback form	4.3	More Details
CVE-2025-12924	A vulnerability was identified in rymcu forest up to de53ce79db9faa2efc4e79ce1077a302c42a1224. This issue affects the function GlobalResult of the file src/main/java/com/rymcu/forest/web/api/bank/BankController.java. The manipulation leads to missing authorization. The attack may be initiated remotely. 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.	4.3	More Details
CVE-2025-12433	Inappropriate implementation in V8 in Google Chrome prior to 142.0.7444.59 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2025-12441	Out of bounds read in V8 in Google Chrome prior to 142.0.7444.59 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details

CVE-2025-11748	The Groups plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.7.0 via the 'group_id' parameter of the group_join function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to register for groups other than ones set in the shortcode.	4.3	More Details
CVE-2025-12725	Out of bounds read in WebGPU in Google Chrome on Android prior to 142.0.7444.137 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2025-12167	The Contact Form 7 AWeber Extension plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wp_ajax_aweber_logreset' AJAX endpoint in all versions up to, and including, 0.1.42. This makes it possible for authenticated attackers, with Subscriber-level access and above, to reset the AWeber logs.	4.3	More Details
CVE-2025-12498	The EventPrime – Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to unauthorized booking note creation due to a missing capability check on the 'booking_add_notes' function in all versions up to, and including, 4.2.0.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to add a note to the backend view of any booking.	4.3	More Details
CVE-2025-11448	The Gallery Plugin for WordPress – Envira Photo Gallery plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the '/envira-convert/v1/bulk-convert' REST API endpoint in all versions up to, and including, 1.11.0. This makes it possible for authenticated attackers, with contributor-level access and above, to convert galleries to Envira galleries.	4.3	More Details
CVE-2025-12917	A vulnerability was identified in TOZED ZLT T10 T10PLUS_3.04.15. The affected element is an unknown function of the file /reqproc/proc_post of the component Reboot Handler. Such manipulation leads to denial of service. Access to the local network is required for this attack to succeed. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-11215	Off by one error in V8 in Google Chrome prior to 141.0.7390.54 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2025-48878	Combodo iTop is a web based IT service management tool. In versions on the 3.x branch prior to 3.2.2, an insecure direct object reference allows a user (e.g. with Service desk agent profile) to create a ModuleInstallation object when they shouldn't be able to do so. Version 3.2.2 fixes the issue.	4.3	More Details
CVE-2025-12911	Inappropriate implementation in Permissions in Google Chrome prior to 140.0.7339.80 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2025-12921	A vulnerability has been found in OpenClinica Community Edition up to 3.12.2/3.13. Affected by this issue is some unknown functionality of the file /ImportCRFData?action=confirm of the component CRF Data Import. Such manipulation of the argument xml_file leads to xml injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-42899	SAP S4CORE (Manage journal entries) does not perform necessary authorization checks for an authenticated user resulting in escalation of privileges. This has low impact on confidentiality of the application with no impact on integrity and availability of the application.	4.3	More Details

CVE-2025-21074	Out-of-bounds read in libimagecodec.quram.so prior to SMR Nov-2025 Release 1 allows remote attackers to access out-of-bounds memory.	4.3	More Details
CVE-2025-12675	The KiotViet Sync plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the saveConfig() function in all versions up to, and including, 1.8.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugin's config.	4.3	More Details
CVE-2025-12527	The Page & Post Notes plugin for WordPress is vulnerable to unauthorized modification of notes due to a missing capability check on the 'yydev_notes_save_dashboard_data' function in all versions up to, and including, 1.3.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify notes.	4.3	More Details
CVE-2025-10966	curl's code for managing SSH connections when SFTP was done using the wolfSSH powered backend was flawed and missed host verification mechanisms. This prevents curl from detecting MITM attackers and more.	4.3	More Details
CVE-2025-12815	An ownership verification issue in the Virtual Desktop preview page in the Research and Engineering Studio (RES) on AWS before version 2025.09 may allow an authenticated remote user to view another user's active desktop session metadata, including periodical desktop preview screenshots. To mitigate this issue, users should upgrade to version 2025.09 or above.	4.3	More Details
CVE-2025-62028	Missing Authorization vulnerability in ThemeNectar Salient salient.This issue affects Salient: from n/a through < 17.4.0.	4.3	More Details
CVE-2025-11373	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 arbitrary file uploads due to a missing capability checks in the "depicter-media-upload" AJAX route in all versions up to, and including, 4.0.4. This makes it possible for authenticated attackers, with Contributor-level access and above, to upload limited files on the affected site's server.	4.3	More Details
CVE-2025-62950	Cross-Site Request Forgery (CSRF) vulnerability in Wasiliy Strecker / ContestGallery developer Contest Gallery contest-gallery allows Cross Site Request Forgery.This issue affects Contest Gallery: from n/a through <= 28.0.0.	4.3	More Details
CVE-2025-42882	Due to a missing authorization check in SAP NetWeaver Application Server for ABAP, an authenticated attacker with basic privileges could execute a specific function module in ABAP to retrieve restricted technical information from the system. This disclosure of environment details of the system could further assist this attacker to plan subsequent attacks. As a result, this vulnerability has a low impact on confidentiality, with no impact on the integrity or availability of the application.	4.3	More Details
CVE-2025-12444	Incorrect security UI in Fullscreen UI in Google Chrome prior to 142.0.7444.59 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.2	More Details
CVE-2025-12446	Incorrect security UI in SplitView in Google Chrome prior to 142.0.7444.59 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted domain name. (Chromium security severity: Low)	4.2	More Details
CVE-2025-52602	HCL BigFix Query is affected by a sensitive information disclosure in the WebUI Query application. An HTTP GET endpoint request returns discoverable responses that may disclose: group names, active user names (or IDs). An attacker can use that information to target individuals with phishing or other social-engineering	4.2	More Details

	attacks.		
CVE-2025-12729	Inappropriate implementation in Omnibox in Google Chrome on Android prior to 142.0.7444.137 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.2	More Details
CVE-2025-12728	Inappropriate implementation in Omnibox in Google Chrome on Android prior to 142.0.7444.137 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.2	More Details
CVE-2025-12434	Race in Storage in Google Chrome on Windows prior to 142.0.7444.59 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.2	More Details
CVE-2025-12447	Incorrect security UI in Omnibox in Google Chrome on Android prior to 142.0.7444.59 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.2	More Details
CVE-2025-63420	CrushFTP11 before 11.3.7_57 is vulnerable to stored HTML injection in the CrushFTP Admin Panel (Reports / "Who Created Folder"), enabling persistent HTML execution in admin sessions.	4.1	More Details
CVE-2025-22288	Path Traversal: '.../...//' vulnerability in WPMU DEV - Your All-in-One WordPress Platform Smush Image Compression and Optimization wp-smushit allows Path Traversal.This issue affects Smush Image Compression and Optimization: from n/a through <= 3.17.0.	4.1	More Details
CVE-2025-12520	The WP Airbnb Review Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 4.2 due to insufficient URL validation that allows users to pull in a malicious HTML file. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.0	More Details
CVE-2025-30509	Improper input validation for some Intel QuickAssist Technology software before version 2.6.0 within Ring 3: User Applications may allow an escalation of privilege. System software adversary with an authenticated user combined with a low complexity attack may enable data manipulation. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (low) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	3.8	More Details
CVE-2025-20622	Sensitive information uncleared in resource before release for reuse for some Intel(R) NPU Drivers for Windows before version 32.0.100.4023 within Ring 3: User Applications may allow an information disclosure. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (low), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	3.8	More Details
	A vulnerability was detected in EverShop up to 2.0.1. Affected is an unknown		

CVE-2025-12919	function of the file /src/modules/oms/graphql/types/Order/Order.resolvers.js of the component Order Handler. The manipulation of the argument uuid results in improper control of resource identifiers. The attack may be performed from remote. This attack is characterized by high complexity. The exploitability is told to be difficult. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2025-48985	A vulnerability in Vercel’s AI SDK has been fixed in versions 5.0.52, 5.1.0-beta.9, and 6.0.0-beta. This issue may have allowed users to bypass filetype whitelists when uploading files. All users are encouraged to upgrade. More details: https://vercel.com/changelog/cve-2025-48985-input-validation-bypass-on-ai-sdk	3.7	More Details
CVE-2025-12854	A vulnerability was identified in newbee-mall-plus up to 2.4.1. This vulnerability affects the function executeSeckill of the file /seckillExecution/. The manipulation of the argument userid leads to authorization bypass. It is possible to initiate the attack remotely. The attack is considered to have high complexity. It is stated that the exploitability is difficult. The exploit is publicly available and might be used.	3.7	More Details
CVE-2025-62780	changedetection.io is a free open source web page change detection tool. A Stored Cross Site Scripting is present in changedetection.io Watch update API in versions prior to 0.50.34 due to insufficient security checks. Two scenarios are possible. In the first, an attacker can insert a new watch with an arbitrary URL which really points to a web page. Once the HTML content is retrieved, the attacker updates the URL with a JavaScript payload. In the second, an attacker substitutes the URL in an existing watch with a new URL that is in reality a JavaScript payload. When the user clicks on *Preview* and then on the malicious link, the JavaScript malicious code is executed. Version 0.50.34 fixes the issue.	3.5	More Details
CVE-2025-25216	Improper input validation in some firmware for some Intel(R) Graphics Drivers and Intel LTS kernels within Ring 1: Device Drivers may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are present with special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (low) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	3.3	More Details
CVE-2025-21077	Improper input validation in Samsung Email prior to version 6.2.06.0 allows local attackers to launch arbitrary activity with Samsung Email privilege.	3.3	More Details
CVE-2025-32088	Improper conditions check for some Intel(R) QAT Windows software before version 2.6.0. within Ring 3: User Applications may allow a denial of service. System software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (low) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	3.3	More Details
CVE-2025-31948	Improper input validation for some Intel(R) oneAPI Math Kernel Library before version 2025.2 within Ring 3: User Applications may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (low) of the vulnerable	3.3	More Details

	system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.		
CVE-2025-8998	It was possible to upload files with a specific name to a temporary directory, which may result in process crashes and impact usability. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account.	3.1	More Details
CVE-2025-64686	In JetBrains YouTrack before 2025.3.104432 missing user principal cleanup led to reuse of incorrect authorization context	3.1	More Details
CVE-2025-11219	Use after free in V8 in Google Chrome prior to 141.0.7390.54 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Low)	3.1	More Details
CVE-2025-12918	A security flaw has been discovered in yungifez Skuul School Management System up to 2.6.5. The impacted element is an unknown function of the file /dashboard/fees/fee-invoices/ of the component View Fee Invoice. Performing manipulation of the argument invoice_id results in improper control of resource identifiers. Remote exploitation of the attack is possible. The attack is considered to have high complexity. The exploitability is regarded as difficult. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2025-64681	In JetBrains Hub before 2025.3.104992 a race condition allowed bypass of the user limit via invitations	2.7	More Details
CVE-2025-64682	In JetBrains Hub before 2025.3.104432 a race condition allowed bypass of the Agent-user limit	2.7	More Details
CVE-2025-12923	A vulnerability was determined in liweiyi ChestnutCMS up to 1.5.8. This vulnerability affects the function resourceDownload of the file /dev-api/common/download. Executing manipulation of the argument path can lead to path traversal. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	2.7	More Details
CVE-2025-42883	Migration Workbench (DX Workbench) in SAP NetWeaver Application Server for ABAP fails to trigger a malware scan when an attacker with administrative privileges uploads files to the application server. An attacker could leverage this and upload a malicious file into the system. This results in a low impact on the integrity of the application.	2.7	More Details
CVE-2025-64773	In JetBrains YouTrack before 2025.3.104432 a race condition allowed bypass of helpdesk Agent limit	2.7	More Details
CVE-2025-64326	Weblate is a web based localization tool. In versions 5.14 and below, Weblate leaks the IP address of the project member inviting the user to the project in the audit log. The audit log includes IP addresses from admin-triggered actions, which can be viewed by invited users. This issue is fixed in version 5.14.1.	2.6	More Details
CVE-2025-12920	A flaw has been found in qianfox FoxCMS up to 1.2.16. Affected by this vulnerability is the function add/edit of the file app/admin/controller/Product.php. This manipulation of the argument Title causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
	Improper access control for some Intel(R) CIP software before version		

CVE-2025-24314	WIN_DCA_2.4.0.11001 within Ring 3: User Applications may allow an information disclosure. Unprivileged software adversary with a privileged user combined with a high complexity attack may enable data exposure. This result may potentially occur via network access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (low), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	2.2	More Details
CVE-2025-24862	Unrestricted upload of file with dangerous type for some Intel(R) CIP software before version WIN_DCA_2.4.0.11001 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with a privileged user combined with a high complexity attack may enable data manipulation. This result may potentially occur via network access when attack requirements are present with special internal knowledge and requires passive user interaction. The potential vulnerability may impact the confidentiality (none), integrity (low) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	2.0	More Details
CVE-2025-32037	Improper access control for some Intel(R) PresentMon before version 2.3.1 within Ring 3: User Applications may allow a denial of service. Network adversary with a privileged user combined with a high complexity attack may enable denial of service. This result may potentially occur via adjacent access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (low) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	2.0	More Details
CVE-2025-24307	Improper privilege management for some Intel(R) CIP software before version WIN_DCA_2.4.0.11001 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable data manipulation. This result may potentially occur via network access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (low) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	2.0	More Details
CVE-2025-64481	Datasette is an open source multi-tool for exploring and publishing data. In versions 0.65.1 and below and 1.0a0 through 1.0a19, deployed instances of Datasette include an open redirect vulnerability. Hits to the path //example.com/foo/bar/ (the trailing slash is required) will redirect the user to https://example.com/foo/bar. This problem has been patched in both Datasette 0.65.2 and 1.0a21. To workaround this issue, if Datasette is running behind a proxy, that proxy could be configured to replace // with / in incoming request URLs.	0.0	More Details
CVE-2025-53409	An allocation of resources without limits or throttling vulnerability has been reported to affect File Station 5. 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 version: File Station 5 5.5.6.5018 and later	N/A	More Details
CVE-2025-63713	Cross-Site Scripting (XSS) vulnerability in SourceCodester "MatchMaster" 1.0 allows remote attackers to inject arbitrary web script or HTML via crafted input in the custom test creation feature. The vulnerability exists because the application fails to properly sanitize user-supplied input in test titles and matching pair items before rendering them in the DOM during test execution.	N/A	More Details

CVE-2025-53410	An allocation of resources without limits or throttling vulnerability has been reported to affect File Station 5. 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 version: File Station 5 5.5.6.5018 and later	N/A	More Details
CVE-2025-52425	An SQL injection vulnerability has been reported to affect QuMagie. A remote attacker can exploit the vulnerability to execute unauthorized code or commands. We have already fixed the vulnerability in the following versions: QuMagie 2.7.0 and later	N/A	More Details
CVE-2025-61994	Cross-site scripting vulnerability exists in GROWI prior to v7.2.10. If a malicious user creates a page containing crafted contents, an arbitrary script may be executed on the web browser of a victim user who accesses the page.	N/A	More Details
CVE-2025-63718	A SQL injection vulnerability exists in the SourceCodester PQMS (Patient Queue Management System) 1.0 in the api_patient_schedule.php endpoint. The appointmentID parameter is not properly sanitized, allowing attackers to execute arbitrary SQL commands.	N/A	More Details
CVE-2025-47207	A NULL pointer dereference vulnerability has been reported to affect several product 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 version: File Station 5 5.5.6.5018 and later	N/A	More Details
CVE-2025-63716	The SourceCodester Leads Manager Tool v1.0 is vulnerable to Cross-Site Request Forgery (CSRF) attacks that allow unauthorized state-changing operations. The application lacks CSRF protection mechanisms such as anti-CSRF tokens or same-origin verification for critical endpoints.	N/A	More Details
CVE-2025-34299	Monsta FTP versions 2.11 and earlier contain a vulnerability that allows unauthenticated arbitrary file uploads. This flaw enables attackers to execute arbitrary code by uploading a specially crafted file from a malicious (S)FTP server.	N/A	More Details
CVE-2025-53408	A NULL pointer dereference vulnerability has been reported to affect File Station 5. 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 version: File Station 5 5.5.6.5018 and later	N/A	More Details
CVE-2025-64480	Rejected reason: Not used	N/A	More Details
CVE-2025-64449	Rejected reason: Not used	N/A	More Details
CVE-2025-63714	Cross-Site Scripting (XSS) vulnerability in SourceCodester User Account Generator 1.0 allows remote attackers to execute arbitrary JavaScript code in the context of the user's browser session via crafted input in the Username Prefix field. The vulnerability exists due to improper sanitization of user-supplied input when rendering generated account data to the DOM, allowing persistent injection of malicious HTML elements that execute when clicked by users.	N/A	More Details
CVE-2025-52865	A NULL pointer dereference vulnerability has been reported to affect File Station 5. 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 version: File Station 5 5.5.6.5018 and later	N/A	More Details

CVE-2025-53411	An allocation of resources without limits or throttling vulnerability has been reported to affect File Station 5. 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 version: File Station 5 5.5.6.5018 and later	N/A	More Details
CVE-2025-58469	A cross-site request forgery (CSRF) vulnerability has been reported to affect QuLog Center. The remote attackers can then exploit the vulnerability to gain privileges or hijack user identities. We have already fixed the vulnerability in the following version: QuLog Center 1.8.2.927 (2025/09/17) and later	N/A	More Details
CVE-2025-57697	AstrBot Project v3.5.22 has an arbitrary file read vulnerability in function _encode_image_bs64. Since the _encode_image_bs64 function defined in entities.py opens the image specified by the user in the request body and returns the image content as a base64-encoded string without checking the legitimacy of the image path, attackers can construct a series of malicious URLs to read any specified file, resulting in sensitive data leakage.	N/A	More Details
CVE-2025-64448	Rejected reason: Not used	N/A	More Details
CVE-2025-58464	A relative path traversal vulnerability has been reported to affect QuMagie. If a remote attacker, 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 version: QuMagie 2.7.3 and later	N/A	More Details
CVE-2025-58463	A relative path traversal vulnerability has been reported to affect Download Station. 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: Download Station 5.10.0.305 (2025/09/16) and later Download Station 5.10.0.304 (2025/09/08) and later	N/A	More Details
CVE-2025-63686	There is an arbitrary file download vulnerability in GuoMinJim PersonManage thru commit 5a02b1ab208feacf3a34fc123c9381162afbaa95 (2020-11-23) in the document query function under the Download Center menu in the PersonManage system.	N/A	More Details
CVE-2025-57712	A path traversal vulnerability has been reported to affect Qsync Central. If a remote 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 version: Qsync Central 5.0.0.3 (2025/08/28) and later	N/A	More Details
CVE-2025-9338	A improper restriction of operations within the bounds of a memory buffer exists in AsIO3.sys driver. This vulnerability can be triggered by manually executing a specially crafted process, potentially leading to local privilage escalation. For additional information, please refer to the 'Security Update for Armoury Crate App' section of the ASUS Security Advisory.	N/A	More Details
CVE-2025-64478	Rejected reason: Not used	N/A	More Details
CVE-2025-57706	A cross-site scripting (XSS) vulnerability has been reported to affect File Station 5. If a remote attacker gains a user account, they can then exploit the vulnerability to bypass security mechanisms or read application data. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5018 and later	N/A	More Details

CVE-2025-63687	An issue was discovered in rymcu forest thru commit f782e85 (2025-09-04) in function doBefore in file src/main/java/com/rymcu/forest/core/service/security/AuthorshipAspect.java, allowing authorized attackers to delete arbitrary users posts.	N/A	More Details
CVE-2025-63783	A Broken Object Level Authorization (BOLA) vulnerability was discovered in the tRPC project mutation APIs (update, delete, add/remove tag) of the Onlook web application 0.2.32. The vulnerability exists because the API fails to verify the ownership or membership of the currently authenticated user for the requested project ID. An authenticated attacker can send a malicious request containing another user's project ID to unlawfully modify, delete, or manipulate tags on that project, which can severely compromise data integrity and availability.	N/A	More Details
CVE-2025-54168	A cross-site scripting (XSS) vulnerability has been reported to affect QuLog Center. If a remote attacker gains an administrator account, they can then exploit the vulnerability to bypass security mechanisms or read application data. We have already fixed the vulnerability in the following version: QuLog Center 1.8.2.923 (2025/08/27) and later	N/A	More Details
CVE-2025-3222	Improper Authentication vulnerability in GE Vernova Smallworld on Windows, Linux allows Authentication Abuse.This issue affects Smallworld: 5.3.3 and prior versions for Linux, and 5.3.4. and prior versions for Windows.	N/A	More Details
CVE-2025-54167	A cross-site scripting (XSS) vulnerability has been reported to affect Notification Center. If a remote attacker gains an administrator account, they can then exploit the vulnerability to bypass security mechanisms or read application data. We have already fixed the vulnerability in the following versions: Notification Center 2.1.0.3443 and later Notification Center 1.9.2.3163 and later Notification Center 3.0.0.3466 and later	N/A	More Details
CVE-2025-53413	An allocation of resources without limits or throttling vulnerability has been reported to affect File Station 5. 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 version: File Station 5 5.5.6.5018 and later	N/A	More Details
CVE-2025-57698	AstrBot Project v3.5.22 contains a directory traversal vulnerability. The handler function install_plugin_upload of the interface '/plugin/install-upload' parses the filename from the request body provided by the user, and directly uses the filename to assign to file_path without checking the validity of the filename. The variable file_path is then passed as a parameter to the function `file.save`, so that the file in the request body can be saved to any location in the file system through directory traversal.	N/A	More Details
CVE-2025-63784	An Open Redirect vulnerability exists in the OAuth callback handler in file onlook/apps/web/client/src/app/auth/callback/route.ts in Onlook web application 0.2.32. The vulnerability occurs because the application trusts the X-Forwarded-Host header value without proper validation when constructing a redirect URL. A remote attacker can send a manipulated X-Forwarded-Host header to redirect an authenticated user to an arbitrary external website under their control, which can be exploited for phishing attacks.	N/A	More Details
CVE-2025-7719	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in GE Vernova Smallworld on Windows, Linux allows File Manipulation.This issue affects Smallworld: 5.3.5. and previous versions.	N/A	More Details
CVE-	A cross-site scripting (XSS) vulnerability has been reported to affect Download Station. If a remote attacker gains a user account, they can then exploit the vulnerability to bypass security mechanisms or read application data. We have		More

2025-58465	already fixed the vulnerability in the following versions: Download Station 5.10.0.305 (2025/09/16) and later Download Station 5.10.0.304 (2025/09/08) and later	N/A	Details
CVE-2025-53412	A NULL pointer dereference vulnerability has been reported to affect File Station 5. 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 version: File Station 5 5.5.6.5018 and later	N/A	More Details
CVE-2025-12858	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-64479	Rejected reason: Not used	N/A	More Details
CVE-2025-64455	Rejected reason: Not used	N/A	More Details
CVE-2025-10870	SQL injection vulnerability in DIAL's CentrosNet v2.64. Allows an attacker to retrieve, create, update, and delete databases by sending POST and GET requests with the 'ultralogin' parameter in '/centrosnet/ultralogin.php'.	N/A	More Details
CVE-2022-50594	Advantech iView versions prior to v5.7.04 build 6425 contain a vulnerability within the SNMP management tool that allows for remote attackers to bypass authentication checks and reach a SQL injection vulnerability within the ‘data’ parameter to the ‘NetworkServlet’ endpoint. Successful exploitation allows for the exfiltration of user data, included clear text passwords.	N/A	More Details
CVE-2025-34246	Advantech WebAccess/VPN versions prior to 1.1.5 contain a SQL injection vulnerability in AjaxPrevalidationController.ajaxAction() that allows an authenticated low-privileged observer user to inject SQL via datatable search parameters, leading to disclosure of database information.	N/A	More Details
CVE-2025-34245	Advantech WebAccess/VPN versions prior to 1.1.5 contain a SQL injection vulnerability in AjaxStandaloneVpnClientsController.ajaxAction() that allows an authenticated low-privileged observer user to inject SQL via datatable search parameters, leading to disclosure of database information.	N/A	More Details
CVE-2025-34244	Advantech WebAccess/VPN versions prior to 1.1.5 contain a SQL injection vulnerability in AjaxFwRulesController.ajaxDeviceFwRulesAction() that allows an authenticated low-privileged observer user to inject SQL via datatable search parameters, leading to disclosure of database information.	N/A	More Details
CVE-2025-34243	Advantech WebAccess/VPN versions prior to 1.1.5 contain a SQL injection vulnerability in AjaxFwRulesController.ajaxNetworkFwRulesAction() that allows an authenticated low-privileged observer user to inject SQL via datatable search parameters, leading to disclosure of database information.	N/A	More Details
CVE-2025-34242	Advantech WebAccess/VPN versions prior to 1.1.5 contain a SQL injection vulnerability in AjaxNetworkController.ajaxAction() that allows an authenticated low-privileged observer user to inject SQL via datatable search parameters, leading to disclosure of database information.	N/A	More Details
CVE-2025-34241	Advantech WebAccess/VPN versions prior to 1.1.5 contain a SQL injection vulnerability in AjaxDeviceController.ajaxDeviceAction() that allows an authenticated low-privileged observer user to inject SQL via datatable search parameters, leading to disclosure of database information.	N/A	More Details

CVE-2025-34240	Advantech WebAccess/VPN versions prior to 1.1.5 contain a SQL injection vulnerability in AppManagementController.appUpgradeAction() that allows an authenticated low-privileged observer user to inject SQL via datatable search parameters, leading to disclosure of database information.	N/A	More Details
CVE-2025-34239	Advantech WebAccess/VPN versions prior to 1.1.5 contain a command injection vulnerability in AppManagementController.appUpgradeAction() that allows an authenticated system administrator to execute arbitrary commands as the web server user (www-data) by supplying a crafted uploaded filename.	N/A	More Details
CVE-2025-34238	Advantech WebAccess/VPN versions prior to 1.1.5 contain an absolute path traversal via AjaxStandaloneVpnClientsController.ajaxDownloadRoadWarriorConfigFileAction() that allows an authenticated network administrator to cause the application to read and return the contents of arbitrary files the web user (www-data) can access.	N/A	More Details
CVE-2025-34237	Advantech WebAccess/VPN versions prior to 1.1.5 contain a stored cross-site scripting (XSS) vulnerability via StandaloneVpnClientsController.addStandaloneVpnClientAction(). Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2025-34236	Advantech WebAccess/VPN versions prior to 1.1.5 contain a stored cross-site scripting (XSS) vulnerability via NetworksController.addNetworkAction(). Insufficient validation or escaping of user-supplied input may allow an attacker to inject and execute arbitrary script in the context of a victim's browser.	N/A	More Details
CVE-2025-12490	Netgate pfSense CE Suricata Path Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to create arbitrary files on affected installations of Netgate pfSense. Authentication is required to exploit this vulnerability. The specific flaw exists within the Suricata package. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to create files in the context of root. Was ZDI-CAN-28085.	N/A	More Details
CVE-2022-50596	D-Link DIR-1260 Wi-Fi router firmware versions up to and including v1.20B05 contain a command injection vulnerability within the web management interface that allows for unauthenticated attackers to execute arbitrary commands on the device with root privileges. The flaw specifically exists within the SetDest/Dest/Target arguments to the GetDeviceSettings form. The management interface is accessible over HTTP and HTTPS on the local and Wi-Fi networks and optionally from the Internet.	N/A	More Details
CVE-2022-50595	Advantech iView versions prior to v5.7.04 build 6425 contain a vulnerability within the SNMP management tool that allows for remote attackers to bypass authentication checks and reach a SQL injection vulnerability within the ‘ztp_search_value’ parameter to the ‘NetworkServlet’ endpoint. Successful exploitation allows for remote code execution with administrator privileges.	N/A	More Details
CVE-2022-50593	Advantech iView versions prior to v5.7.04 build 6425 contain a vulnerability within the SNMP management tool that allows for remote attackers to bypass authentication checks and reach a SQL injection vulnerability within the ‘search_term’ parameter to the ‘NetworkServlet’ endpoint. Successful exploitation allows for remote code execution with administrator privileges.	N/A	More Details
	runc is a CLI tool for spawning and running containers according to the OCI specification. Versions 1.0.0-rc3 through 1.2.7, 1.3.0-rc.1 through 1.3.2, and 1.4.0-rc.1 through 1.4.0-rc.2, due to insufficient checks when bind-mounting `/dev/pts/$n` to `/dev/console` inside the container, an attacker can trick runc into bind-mounting		

CVE-2025-52565	paths which would normally be made read-only or be masked onto a path that the attacker can write to. This attack is very similar in concept and application to CVE-2025-31133, except that it attacks a similar vulnerability in a different target (namely, the bind-mount of `/dev/pts/$n` to `/dev/console` as configured for all containers that allocate a console). This happens after `pivot_root(2)`, so this cannot be used to write to host files directly -- however, as with CVE-2025-31133, this can load to denial of service of the host or a container breakout by providing the attacker with a writable copy of `/proc/sysrq-trigger` or `/proc/sys/kernel/core_pattern` (respectively). This issue is fixed in versions 1.2.8, 1.3.3 and 1.4.0-rc.3.	N/A	More Details
CVE-2022-50592	Advantech iView versions prior to v5.7.04 build 6425 contain a vulnerability within the SNMP management tool that allows for remote attackers to bypass authentication checks and reach a SQL injection vulnerability within the ‘getInventoryReportData’ parameter to the ‘NetworkServlet’ endpoint. Successful exploitation allows for remote code execution with administrator privileges.	N/A	More Details
CVE-2022-50591	Advantech iView versions prior to v5.7.04 build 6425 contain a vulnerability within the SNMP management tool that allows for remote attackers to bypass authentication checks and reach a SQL injection vulnerability within the ‘ztp_config_id’ parameter to the ‘NetworkServlet’ endpoint. Successful exploitation allows for the exfiltration of user data, included clear text passwords.	N/A	More Details
CVE-2022-50590	SuiteCRM versions prior to 7.12.6 contain a type confusion vulnerability within the processing of the ‘module’ parameter within the ‘deleteAttachment’ functionality. Successful exploitation allows remote unauthenticated attackers to alter database objects including changing the email address of the administrator.	N/A	More Details
CVE-2022-50589	SuiteCRM versions prior to 7.12.6 contain a SQL injection vulnerability within the processing of the ‘uid’ parameter within the ‘export’ functionality. Successful exploitation allows remote unauthenticated attackers to ultimately execute arbitrary code.	N/A	More Details
CVE-2025-31133	runc is a CLI tool for spawning and running containers according to the OCI specification. In versions 1.2.7 and below, 1.3.0-rc.1 through 1.3.1, 1.4.0-rc.1 and 1.4.0-rc.2 files, runc would not perform sufficient verification that the source of the bind-mount (i.e., the container's /dev/null) was actually a real /dev/null inode when using the container's /dev/null to mask. This exposes two methods of attack: an arbitrary mount gadget, leading to host information disclosure, host denial of service, container escape, or a bypassing of maskedPaths. This issue is fixed in versions 1.2.8, 1.3.3 and 1.4.0-rc.3.	N/A	More Details
CVE-2025-60188	Insertion of Sensitive Information Into Sent Data vulnerability in Vito Peleg Atarim atarim-visual-collaboration allows Retrieve Embedded Sensitive Data.This issue affects Atarim: from n/a through <= 4.2.	N/A	More Details
CVE-2025-3717	When using the Grafana Snowflake Datasource Plugin, if Oauth passthrough is enabled on the datasource, and multiple users are using the same datasource at the same time on a single Grafana instance, it could result in the wrong user identifier being used, and information for which the viewer is not authorized being returned. This issue affects Grafana Snowflake Datasource Plugin: from 1.5.0 before 1.14.1.	N/A	More Details
CVE-2025-60189	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in PoloPag PoloPag – Pix Automático para Woocommerce wc-polo-payments allows PHP Local File Inclusion.This issue affects PoloPag – Pix Automático para Woocommerce: from n/a through <= 2.0.9.	N/A	More Details

CVE-2025-59396	Rejected reason: Not a security vulnerability	N/A	More Details
CVE-2025-60207	Unrestricted Upload of File with Dangerous Type vulnerability in Addify Custom User Registration Fields for WooCommerce user-registration-plugin-for-woocommerce allows Upload a Web Shell to a Web Server.This issue affects Custom User Registration Fields for WooCommerce: from n/a through <= 2.1.2.	N/A	More Details
CVE-2025-41116	When using the Grafana Databricks Datasource Plugin, if Oauth passthrough is enabled on the datasource, and multiple users are using the same datasource at the same time on a single Grafana instance, it could result in the wrong user identifier being used, and information for which the viewer is not authorized being returned. This issue affects Grafana Databricks Datasource Plugin: from 1.12.1 before 1.12.0	N/A	More Details
CVE-2025-60235	Unrestricted Upload of File with Dangerous Type vulnerability in Plugify Helpdesk Support Ticket System for WooCommerce support-ticket-system-for-woocommerce allows Using Malicious Files.This issue affects Helpdesk Support Ticket System for WooCommerce: from n/a through <= 2.1.0.	N/A	More Details
CVE-2025-60245	Deserialization of Untrusted Data vulnerability in WP User Manager WP User Manager wp-user-manager allows Object Injection.This issue affects WP User Manager: from n/a through <= 2.9.12.	N/A	More Details
CVE-2025-60244	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in RealMag777 TableOn posts-table-filterable allows Code Injection.This issue affects TableOn: from n/a through <= 1.0.4.2.	N/A	More Details
CVE-2025-34247	Advantech WebAccess/VPN versions prior to 1.1.5 contain a SQL injection vulnerability in NetworksController.addNetworkAction() that allows an authenticated low-privileged observer user to inject SQL via datatable search parameters, leading to disclosure of database information.	N/A	More Details
CVE-2025-12486	Heimdall Data Database Proxy Cross-Site Scripting Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Heimdall Data Database Proxy. Minimal user interaction is required to exploit this vulnerability. The specific flaw exists within the handling of the database event logs. The issue results from the lack of proper validation of user-supplied data, which can lead to the injection of arbitrary script. An attacker can leverage this vulnerability to interact with the application in the context of the target user. Was ZDI-CAN-24755.	N/A	More Details
CVE-2025-64477	Rejected reason: Not used	N/A	More Details
CVE-2025-64187	OctoPrint provides a web interface for controlling consumer 3D printers. Versions 1.11.3 and below are affected by a vulnerability that allows injection of arbitrary HTML and JavaScript into Action Command notifications and prompts popups generated by the printer. An attacker who successfully convinces a victim to print a specially crafted file could exploit this issue to disrupt ongoing prints, extract information (including sensitive configuration settings, if the targeted user has the necessary permissions for that), or perform other actions on behalf of the targeted user within the OctoPrint instance. This issue is fixed in version 1.11.4.	N/A	More Details
CVE-2025-46413	Use of password hash with insufficient computational effort issue exists in BUFFALO Wi-Fi router 'WSR-1800AX4 series'. When WPS is enabled, PIN code and/or Wi-Fi password may be obtained by an attacker.	N/A	More Details

CVE-2025-64476	Rejected reason: Not used	N/A	More Details
CVE-2025-64475	Rejected reason: Not used	N/A	More Details
CVE-2025-64474	Rejected reason: Not used	N/A	More Details
CVE-2025-64473	Rejected reason: Not used	N/A	More Details
CVE-2025-64472	Rejected reason: Not used	N/A	More Details
CVE-2025-64346	archives is a Go library for extracting archives (tar, zip, etc.). Version 1.0.0 does not prevent a malicious user to feed a specially crafted archive to the library causing RCE, modification of files or other malignancies in the context of whatever the user is running this library as, through the program that imports it. Severity depends on user permissions, environment and how arbitrary archives are passed. This issue is fixed in version 1.0.1.	N/A	More Details
CVE-2025-58996	Unrestricted Upload of File with Dangerous Type vulnerability in Helmut Wandl Advanced Settings advanced-settings allows Upload a Web Shell to a Web Server.This issue affects Advanced Settings: from n/a through <= 3.1.1.	N/A	More Details
CVE-2025-64339	ClipBucket v5 is an open source video sharing platform. In versions 5.5.2-#146 and below, the Manage Playlists feature is vulnerable to stored Cross-site Scripting (XSS),specifically in the Playlist Name field. An authenticated low-privileged user can create a playlist with a malicious name containing HTML/JavaScript code, which is rendered unescaped on playlist detail and listing pages. This results in arbitrary JavaScript execution in every viewer’s browser, including administrators. This issue is fixed in version 5.5.2-#147.	N/A	More Details
CVE-2025-64171	MARIN3R is a lightweight, CRD based envoy control plane for kubernetes. In versions 0.13.3 and below, there is a cross-namespace secret access vulnerability in the project's DiscoveryServiceCertificate which allows users to bypass RBAC and access secrets in unauthorized namespaces. This issue is fixed in version 0.13.4.	N/A	More Details
CVE-2025-58995	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Creatives_Planet Leblix leblix allows PHP Local File Inclusion.This issue affects Leblix: from n/a through <= 2.4.	N/A	More Details
CVE-2025-64336	ClipBucket v5 is an open source video sharing platform. In versions 5.5.2-#146 and below, the Manage Photos feature is vulnerable to stored Cross-site Scripting (XSS). An authenticated regular user can upload a photo with a malicious Photo Title containing HTML/JavaScript code. While the payload does not execute in the user-facing photo gallery or detail pages, it is rendered unsafely in the Admin → Manage Photos section, resulting in JavaScript execution in the administrator’s browser. This issue is fixed in version 5.5.2-#147.	N/A	More Details
CVE-2025-64329	containerd is an open-source container runtime. Versions 1.7.28 and below, 2.0.0-beta.0 through 2.0.6, 2.1.0-beta.0 through 2.1.4, and 2.2.0-beta.0 through 2.2.0-rc.1 contain a bug in the CRI Attach implementation where a user can exhaust memory on the host due to goroutine leaks. This issue is fixed in versions 1.7.29,	N/A	More Details

	2.0.7, 2.1.5 and 2.2.0. To workaround this vulnerability, users can set up an admission controller to control accesses to pods/attach resources.		
CVE-2025-64328	FreePBX Endpoint Manager is a module for managing telephony endpoints in FreePBX systems. In versions 17.0.2.36 and above before 17.0.3, the filestore module within the Administrative interface is vulnerable to a post-authentication command injection by an authenticated known user via the testconnection -> check_ssh_connect() function. An attacker can leverage this vulnerability to obtain remote access to the system as an asterisk user. This issue is fixed in version 17.0.3.	N/A	More Details
CVE-2025-58998	Deserialization of Untrusted Data vulnerability in Cristián Lávaque s2Member s2member allows Object Injection.This issue affects s2Member: from n/a through <= 250701.	N/A	More Details
CVE-2025-12487	oobabooga text-generation-webui trust_remote_code Reliance on Untrusted Inputs Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of oobabooga text-generation-webui. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the trust_remote_code parameter provided to the join endpoint. The issue results from the lack of proper validation of a user-supplied argument before using it to load a model. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-26681.	N/A	More Details
CVE-2025-11546	CLUSTERPRO X for Linux 4.0, 4.1, 4.2, 5.0, 5.1 and 5.2 and EXPRESSCLUSTER X for Linux 4.0, 4.1, 4.2, 5.0, 5.1 and 5.2, CLUSTERPRO X SingleServerSafe for Linux 4.0, 4.1, 4.2, 5.0, 5.1 and 5.2, EXPRESSCLUSTER X SingleServerSafe for Linux 4.0, 4.1, 4.2, 5.0, 5.1 and 5.2 allows an attacker sends specially crafted network packets to the product, arbitrary OS commands may be executed without authentication.	N/A	More Details
CVE-2025-59556	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup GoStore gostore allows Reflected XSS.This issue affects GoStore: from n/a through < 1.6.4.	N/A	More Details
CVE-2025-62225	Optical Disc Archive Software provided by Sony Corporation registers a Windows service with an unquoted file path. A user with the write permission on the root directory of the system drive may execute arbitrary code with SYSTEM privilege.	N/A	More Details
CVE-2025-11460	Use after free in Storage in Google Chrome prior to 141.0.7390.65 allowed a remote attacker to execute arbitrary code via a crafted video file. (Chromium security severity: High)	N/A	More Details
CVE-2025-60073	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Processby Responsive Sidebar responsive-sidebar allows PHP Local File Inclusion.This issue affects Responsive Sidebar: from n/a through <= 1.2.2.	N/A	More Details
CVE-2025-64178	Jellysweep is a cleanup tool for the Jellyfin media server. In versions 0.12.1 and below, /api/images/cache, used to download media posters from the server, accepted a URL parameter that was directly passed to the cache package, which downloaded the poster from this URL. This URL parameter can be used to make the Jellysweep server download arbitrary content. The API endpoint can only be used by authenticated users. This issue is fixed in version 0.13.0.	N/A	More Details
CVE-2025-11211	Out of bounds read in Media in Google Chrome prior to 141.0.7390.54 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	N/A	More Details
CVE-	Inappropriate implementation in Omnibox in Google Chrome on Android prior to		

2025-11209	141.0.7390.54 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	N/A	More Details
CVE-2025-11207	Side-channel information leakage in Storage in Google Chrome prior to 141.0.7390.54 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: Medium)	N/A	More Details
CVE-2025-64151	Multiple Roboticsware products provided by Roboticsware PTE. LTD. register Windows services with unquoted file paths. A user with the write permission on the root directory of the system drive may execute arbitrary code with SYSTEM privilege.	N/A	More Details
CVE-2025-64174	Magento-lts is a long-term support alternative to Magento Community Edition (CE). Versions 20.15.0 and below are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin with direct database access or the admin notification feed source to inject malicious scripts into vulnerable fields. Unescaped translation strings and URLs are printed into contexts inside app/code/core/Mage/Adminhtml/Block/Notification/Grid/Renderer/Actions.php. A malicious translation or polluted data can inject script. This issue is fixed in version 20.16.0.	N/A	More Details
CVE-2025-52881	runc is a CLI tool for spawning and running containers according to the OCI specification. In versions 1.2.7, 1.3.2 and 1.4.0-rc.2, an attacker can trick runc into misdirecting writes to /proc to other procfs files through the use of a racing container with shared mounts (we have also verified this attack is possible to exploit using a standard Dockerfile with docker buildx build as that also permits triggering parallel execution of containers with custom shared mounts configured). This redirect could be through symbolic links in a tmpfs or theoretically other methods such as regular bind-mounts. While similar, the mitigation applied for the related CVE, CVE-2019-19921, was fairly limited and effectively only caused runc to verify that when LSM labels are written they are actually procfs files. This issue is fixed in versions 1.2.8, 1.3.3, and 1.4.0-rc.3.	N/A	More Details
CVE-2025-12489	evernote-mcp-server openBrowser Command Injection Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of evernote-mcp-server. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the openBrowser function. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-27913.	N/A	More Details
CVE-2025-12488	oobabooga text-generation-webui trust_remote_code Reliance on Untrusted Inputs Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of oobabooga text-generation-webui. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the trust_remote_code parameter provided to the load endpoint. The issue results from the lack of proper validation of a user-supplied argument before using it to load a model. An attacker can leverage this vulnerability to execute code in the context of the service account. . Was ZDI-CAN-26680.	N/A	More Details
CVE-2025-64338	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
	KubeVirt is a virtual machine management add-on for Kubernetes. In 1.5.0 and earlier, the permissions granted to the virt-handler service account, such as the		

CVE-2025-64436	ability to update VMI and patch nodes, could be abused to force a VMI migration to an attacker-controlled node. This vulnerability could otherwise allow an attacker to mark all nodes as unschedulable, potentially forcing the migration or creation of privileged pods onto a compromised node.	N/A	More Details
CVE-2025-58994	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in designervily Greenify greenify allows PHP Local File Inclusion.This issue affects Greenify: from n/a through <= 2.2.	N/A	More Details
CVE-2025-63152	Tenda AX3 V16.03.12.10_CN was discovered to contain a stack overflow in the wpapsk_crypto parameter of the wlSetExternParameter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-11307	The WP Go Maps (formerly WP Google Maps) WordPress plugin before 9.0.48 does not sanitize user input provided via an AJAX action, allowing unauthenticated users to store XSS payloads which are later retrieved from another AJAX call and output unescaped.	N/A	More Details
CVE-2025-11855	The age-restriction WordPress plugin through 3.0.2 does not have authorisation in the age_restrictionRemoteSupportRequest function, allowing any authenticated users, such as subscriber to create an admin user with a hardcoded username and arbitrary password.	N/A	More Details
CVE-2025-47286	Combodo iTop is a web based IT service management tool. In versions prior to 2.7.13 and 3.2.2, an administrator can, by editing the configuration of the iTop instance, execute code on the server. Versions 2.7.13 and 3.2.2 escape and check the config parameter before executing a command based on it.	N/A	More Details
CVE-2025-63835	A stack-based buffer overflow vulnerability was discovered in Tenda AC18 v15.03.05.05_multi. The vulnerability exists in the guestSsid parameter of the /goform/WifiGuestSet interface. Remote attackers can exploit this vulnerability by sending oversized data to the guestSsid parameter, leading to denial of service (device crash) or potential remote code execution.	N/A	More Details
CVE-2025-63834	A stored cross-site scripting (XSS) vulnerability was discovered in Tenda AC18 v15.03.05.05_multi. The vulnerability exists in the ssid parameter of the wireless settings. Remote attackers can inject malicious payloads that execute when any user visits the router's homepage.	N/A	More Details
CVE-2025-63497	The patient prescription viewing functionality in his_doc_view_single_patient.php of rickxy Hospital Management System version 1.0 contains an SQL injection vulnerability. The pat_number GET parameter is directly concatenated into SQL queries without proper sanitization, allowing authenticated attackers (doctor role) to execute arbitrary SQL queries.	N/A	More Details
CVE-2025-63457	Tenda AX-1803 v1.0.0.1 was discovered to contain a stack overflow via the wanMTU parameter in the sub_4F55C function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-63456	Tenda AX-1803 v1.0.0.1 was discovered to contain a stack overflow via the time parameter in the SetSysTimeCfg function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-63147	Tenda AX3 V16.03.12.10_CN was discovered to contain a stack overflow in the deviceId parameter of the saveParentControlInfo function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-63154	TOTOLink A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow in the addEffect parameter of the urldecode function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	N/A	More Details

CVE-2025-63153	TOTOLink A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow in the ssid parameter of the urldecode function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-5317	An improper access restriction to a folder in Bitdefender Endpoint Security Tools for Mac (BEST) before 7.20.52.200087 allows local users with administrative privileges to bypass the configured uninstall password protection. An unauthorized user with sudo privileges can manually remove the application directory (/Applications/Endpoint Security for Mac.app/) and the related directories within /Library/Bitdefender/AVP without needing the uninstall password.	N/A	More Details
CVE-2025-8768	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2025-12020. Reason: This candidate is a reservation duplicate of CVE-2025-12020. Notes: All CVE users should reference CVE-2025-12020 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-63288	In Open5GS 2.7.6, AMF crashes when receiving an abnormal NGSetupRequest message, resulting in denial of service.	N/A	More Details
CVE-2025-63712	Cross-Site Request Forgery (CSRF) in SourceCodester Product Expiry Management System. The User Management module (delete-user.php) allows remote attackers to delete arbitrary user accounts via forged cross-origin GET requests because the endpoint relies solely on session cookies and lacks CSRF protection.	N/A	More Details
CVE-2017-20210	Photo Station 5.4.1 & 5.2.7 include the security fix for the vulnerability related to the XMR mining programs identified by internal research.	N/A	More Details
CVE-2025-63710	The send_message.php endpoint in SourceCodester Simple Public Chat Room 1.0 is vulnerable to Cross-Site Request Forgery (CSRF). The application does not implement any CSRF-protection mechanisms such as tokens, nonces, or same-site cookie restrictions. An attacker can create a malicious HTML page that, when visited by an authenticated user, will automatically submit a forged POST request to the vulnerable endpoint. This request will be executed with the victim's privileges, allowing the attacker to perform unauthorized actions on their behalf, such as sending arbitrary messages in any chat room.	N/A	More Details
CVE-2025-63709	A Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Simple To-Do List System 1.0 in the "Add Tasks" text input. An authenticated user can submit HTML/JavaScript that is not correctly sanitized or encoded on output. The injected script is stored and later rendered in the browser of any user who views the task, allowing execution of arbitrary script in the context of the victim's browser.	N/A	More Details
CVE-2025-64453	Rejected reason: Not used	N/A	More Details
CVE-2025-64457	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority while details are being clarified. A corrected record will be published once verification is complete.	N/A	More Details
CVE-2025-41101	HTML injection vulnerability found in Fairsketch's RISE CRM Framework v3.8.1, which consist of an HTML code injection due to lack of proper validation of user inputs by sending a POST request in parameter 'title' in'/projects/save'.	N/A	More Details
CVE-2025-	HTML injection vulnerability found in Fairsketch's RISE CRM Framework v3.8.1, which consist of an HTML code injection due to lack of proper validation of user	N/A	More Details

41102	inputs by sending a POST request in parameter 'title' in '/events/save'.		
CVE-2025-41001	Cross Site Scripting (XSS) vulnerability stored in SOPlanning v1.53.02, which consist of a stored XSS due to a lack of proper validation of user input by sending a POST request using the 'LOGOUT_REDIRECT' parameter in '/soplanning/www/process/options.php'. This vulnerability could allow a remote user to send a specially crafted query to an authenticated user and steal their cookie session details.	N/A	More Details
CVE-2025-41103	HTML injection vulnerability found in Fairsketch's RISE CRM Framework v3.8.1, which consist of an HTML code injection due to lack of proper validation of user inputs by sending a POST request in parameter 'reply_message' in '/messages/reply'.	N/A	More Details
CVE-2025-41104	HTML injection vulnerability found in Fairsketch's RISE CRM Framework v3.8.1, which consist of an HTML code injection due to lack of proper validation of user inputs by sending a POST request in parameter 'custom_field_1' in '/estimate_requests/save_estimate_request'.	N/A	More Details
CVE-2025-41105	HTML injection vulnerability found in Fairsketch's RISE CRM Framework v3.8.1, which consist of an HTML code injection due to lack of proper validation of user inputs by sending a POST request in parameter 'title' in '/tickets/save'.	N/A	More Details
CVE-2025-11237	The Make Email Customizer for WooCommerce WordPress plugin through 1.0.6 lacks proper authorization checks and option validation in its AJAX actions, allowing any authenticated user, such as a Subscriber, to update arbitrary WordPress options.	N/A	More Details
CVE-2025-12428	Type Confusion in V8 in Google Chrome prior to 142.0.7444.59 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2025-11084	A security issue exists within DataMosaix™ Private Cloud, allowing attackers to bypass MFA during setup and obtain a valid login-token cookie without knowing the users password. This vulnerability occurs when MFA is enabled but not completed within a 7-day period.	N/A	More Details
CVE-2025-64181	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. In versions 3.3.0 through 3.3.5 and 3.4.0 through 3.4.2, while fuzzing `openexr_exrcheck_fuzzer`, Valgrind reports a conditional branch depending on uninitialized data inside `generic_unpack`. This indicates a use of uninitialized memory. The issue can result in undefined behavior and/or a potential crash/denial of service. Versions 3.3.6 and 3.4.3 fix the issue.	N/A	More Details
CVE-2025-64529	SpiceDB is an open source database system for creating and managing security-critical application permissions. In versions prior to 1.45.2, users who use the exclusion operator somewhere in their authorization schema; have configured their SpiceDB server such that `--write-relationships-max-updates-per-call` is bigger than 6500; and issue calls to WriteRelationships with a large enough number of updates that cause the payload to be bigger than what their datastore allows; will receive a successful response from their `WriteRelationships` call, when in reality that call failed, and receive incorrect permission check results, if those relationships had to be read to resolve the relation involving the exclusion. Version 1.45.2 contains a patch for the issue. As a workaround, set `--write-relationships-max-updates-per-call` to `1000`.	N/A	More Details
CVE-2025-63678	An authenticated arbitrary file upload vulnerability in the /uploads/ endpoint of CMS Made Simple Foundation File Manager v2.2.22 allows attackers with Administrator privileges to execute arbitrary code via uploading a crafted PHP file.	N/A	More Details

CVE-2025-12542	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-11892	An improper neutralization of input vulnerability was identified in GitHub Enterprise Server that allows DOM-based cross-site scripting via Issues search label filter that could lead to privilege escalation and unauthorized workflow triggers. Successful exploitation requires an attacker to have access to the target GitHub Enterprise Server instance and to entice a user, while operating in sudo mode, to click on a crafted malicious link to perform actions that require elevated privileges. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.18.1, 3.17.7, 3.16.10, 3.15.14, 3.14.19.	N/A	More Details
CVE-2025-11578	A privilege escalation vulnerability was identified in GitHub Enterprise Server that allowed an authenticated Enterprise admin to gain root SSH access to the appliance by exploiting a symlink escape in pre-receive hook environments. By crafting a malicious repository and environment, an attacker could replace system binaries during hook cleanup and execute a payload that adds their own SSH key to the root user's authorized keys—thereby granting themselves root SSH access to the server. To exploit this vulnerability, the attacker needed to have enterprise admin privileges. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.19, and was fixed in versions 3.14.19, 3.15.14, 3.16.10, 3.17.7 and 3.18.1. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	More Details
CVE-2021-4462	Employee Records System version 1.0 contains an unrestricted file upload vulnerability that allows a remote unauthenticated attacker to upload arbitrary files via the uploadID.php endpoint; uploaded files can be executed because the application does not perform proper server-side validation.	N/A	More Details
CVE-2018-25124	PacsOne Server version 6.6.2 (prior versions are likely affected) contains a directory traversal vulnerability within the web-based DICOM viewer component. Successful exploitation allows a remote unauthenticated attacker to read arbitrary files via the 'nocache.php' endpoint with a crafted 'path' parameter. Exploitation evidence was observed by the Shadowserver Foundation on 2025-02-07 UTC.	N/A	More Details
CVE-2025-64513	Milvus is an open-source vector database built for generative AI applications. An unauthenticated attacker can exploit a vulnerability in versions prior to 2.4.24, 2.5.21, and 2.6.5 to bypass all authentication mechanisms in the Milvus Proxy component, gaining full administrative access to the Milvus cluster. This grants the attacker the ability to read, modify, or delete data, and to perform privileged administrative operations such as database or collection management. This issue has been fixed in Milvus 2.4.24, 2.5.21, and 2.6.5. If immediate upgrade is not possible, a temporary mitigation can be applied by removing the sourceID header from all incoming requests at the gateway, API gateway, or load balancer level before they reach the Milvus Proxy. This prevents attackers from exploiting the authentication bypass behavior.	N/A	More Details
CVE-2025-64507	Incus is a system container and virtual machine manager. An issue in versions prior to 6.0.6 and 6.19.0 affects any Incus user in an environment where an unprivileged user may have root access to a container with an attached custom storage volume that has the `security.shifted` property set to `true` as well as access to the host as an unprivileged user. The most common case for this would be systems using `incus-user` with the less privileged `incus` group to provide unprivileged users with an isolated restricted access to Incus. Such users may be able to create a custom storage volume with the necessary property (depending on kernel and filesystem support) and can then write a setuid binary from within the container which can be executed as an unprivileged user on the host to gain root privileges. A patch for this issue is expected in versions 6.0.6 and 6.19.0. As a workaround,	N/A	More Details

	permissions can be manually restricted until a patched version of Incus is deployed.		
CVE-2025-64502	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. The MongoDB `explain()` method provides detailed information about query execution plans, including index usage, collection scanning behavior, and performance metrics. Prior to version 8.5.0-alpha.5, Parse Server permits any client to execute explain queries without requiring the master key. This exposes database schema structure and field names, index configurations and query optimization details, query execution statistics and performance metrics, and potential attack vectors for database performance exploitation. In version 8.5.0-alpha.5, a new `databaseOptions.allowPublicExplain` configuration option has been introduced that allows to restrict `explain` queries to the master key. The option defaults to `true` for now to avoid a breaking change in production systems that depends on public `explain` availability. In addition, a security warning is logged when the option is not explicitly set, or set to `true`. In a future major release of Parse Server, the default will change to `false`. As a workaround, implement middleware to block explain queries from non-master-key requests, or monitor and alert on explain query usage in production environments.	N/A	More Details
CVE-2025-64183	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. In versions 3.2.0 through 3.2.4, 3.3.0 through 3.3.5, and 3.4.0 through 3.4.2, there is a use-after-free in PyObject_StealAttrString of pyOpenEXR_old.cpp. The legacy adapter defines PyObject_StealAttrString that calls PyObject_GetAttrString to obtain a new reference, immediately decrefs it, and returns the pointer. Callers then pass this dangling pointer to APIs like PyLong_AsLong/PyFloat_AsDouble, resulting in a use-after-free. This is invoked in multiple places (e.g., reading PixelType.v, Box2i, V2f, etc.) Versions 3.2.5, 3.3.6, and 3.4.3 fix the issue.	N/A	More Details
CVE-2025-64182	OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. In versions 3.2.0 through 3.2.4, 3.3.0 through 3.3.5, and 3.4.0 through 3.4.2, a memory safety bug in the legacy OpenEXR Python adapter (the deprecated OpenEXR.InputFile wrapper) allow crashes and likely code execution when opening attacker-controlled EXR files or when passing crafted Python objects. Integer overflow and unchecked allocation in InputFile.channel() and InputFile.channels() can lead to heap overflow (32 bit) or a NULL deref (64 bit). Versions 3.2.5, 3.3.6, and 3.4.3 contain a patch for the issue.	N/A	More Details
CVE-2025-63397	Improper input validation in OneFlow v0.9.0 allows attackers to cause a segmentation fault via adding a Python sequence to the native code during broadcasting/type conversion.	N/A	More Details
CVE-2025-12430	Object lifecycle issue in Media in Google Chrome prior to 142.0.7444.59 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2025-63617	ktg-mes before commit a484f96 (2025-07-03) has a fastjson deserialization vulnerability. This is because it uses a vulnerable version of fastjson and deserializes unsafe input data.	N/A	More Details
CVE-2025-63296	KERUI K259 5MP Wi-Fi / Tuya Smart Security Camera firmware v33.53.87 contains a code execution vulnerability in its boot/update logic: during startup /usr/sbin/anyka_service.sh scans mounted TF/SD cards and, if /mnt/update.nor.sh is present, copies it to /tmp/net.sh and executes it as root.	N/A	More Details
CVE-2025-63384	A vulnerability was discovered in RISC-V Rocket-Chip v1.6 and before implementation where the SRET (Supervisor-mode Exception Return) instruction fails to correctly transition the processor's privilege level. Instead of downgrading from Machine-mode (M-mode) to Supervisor-mode (S-mode) as specified by the	N/A	More Details

	sstatus.SPP bit, the processor incorrectly remains in M-mode, leading to a critical privilege retention vulnerability.		
CVE-2025-63149	Tenda AX3 V16.03.12.10_CN was discovered to contain a stack overflow in the urls parameter of the get_parentControl_list_Info function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	More Details
CVE-2025-60876	BusyBox wget thru 1.3.7 accepted raw CR (0x0D)/LF (0x0A) and other C0 control bytes in the HTTP request-target (path/query), allowing the request line to be split and attacker-controlled headers to be injected. To preserve the HTTP/1.1 request-line shape METHOD SP request-target SP HTTP/1.1, a raw space (0x20) in the request-target must also be rejected (clients should use %20).	N/A	More Details
CVE-2025-56503	An issue in Sublime HQ Pty Ltd Sublime Text 4 4200 allows authenticated attackers with low-level privileges to escalate privileges to Administrator via replacing the uninstall file with a crafted binary in the installation folder.	N/A	More Details
CVE-2025-64454	Rejected reason: Not used	N/A	More Details
CVE-2025-12727	Inappropriate implementation in V8 in Google Chrome prior to 142.0.7444.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	N/A	More Details
CVE-2025-12445	Policy bypass in Extensions in Google Chrome prior to 142.0.7444.59 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Low)	N/A	More Details
CVE-2025-60243	Incorrect Privilege Assignment vulnerability in Holest Engineering Selling Commander for WooCommerce selling-commander-connector allows Privilege Escalation.This issue affects Selling Commander for WooCommerce: from n/a through <= 1.2.46.	N/A	More Details
CVE-2025-12437	Use after free in PageInfo in Google Chrome prior to 142.0.7444.59 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	N/A	More Details
CVE-2025-12431	Inappropriate implementation in Extensions in Google Chrome prior to 142.0.7444.59 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: High)	N/A	More Details
CVE-2025-41106	HTML injection vulnerability found in Fairsketch's RISE CRM Framework v3.8.1, which consist of an HTML code injection due to lack of proper validation of user inputs by sending a POST request in parameter 'first_name' in '/clients/save_contact/'.	N/A	More Details
CVE-2025-11085	A security issue exists within DataMosaix™ Private Cloud allowing for Persistent XSS. This vulnerability can result in the execution of malicious JavaScript, allowing for account takeover, credential theft, or redirection to a malicious website.	N/A	More Details
CVE-2025-58986	Missing Authorization vulnerability in ganddser Jock On Air Now (JOAN) joan allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Jock On Air Now (JOAN): from n/a through <= 6.0.4.	N/A	More Details
CVE-2025-58638	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins Institutions Directory institutions-directory allows Reflected XSS.This issue affects Institutions Directory: from n/a through <= 1.3.3.	N/A	More Details

CVE-2025-62689	NULL pointer dereference vulnerability exists in GNU libmicrohttpd v1.0.2 and earlier. The vulnerability was fixed in commit ff13abc on the master branch of the libmicrohttpd Git repository, after the v1.0.2 tag. A specially crafted packet sent by an attacker could cause a denial-of-service (DoS) condition.	N/A	More Details
CVE-2025-59777	NULL pointer dereference vulnerability exists in GNU libmicrohttpd v1.0.2 and earlier. The vulnerability was fixed in commit ff13abc on the master branch of the libmicrohttpd Git repository, after the v1.0.2 tag. A specially crafted packet sent by an attacker could cause a denial-of-service (DoS) condition.	N/A	More Details
CVE-2025-64451	Rejected reason: Not used	N/A	More Details
CVE-2025-40109	In the Linux kernel, the following vulnerability has been resolved: crypto: rng - Ensure set_ent is always present Ensure that set_ent is always set since only drbg provides it.	N/A	More Details
CVE-2025-40108	In the Linux kernel, the following vulnerability has been resolved: serial: qcom-geni: Fix blocked task Revert commit 1afa70632c39 ("serial: qcom-geni: Enable PM runtime for serial driver") and its dependent commit 86fa39dd6fb7 ("serial: qcom-geni: Enable Serial on SA8255p Qualcomm platforms") because the first one causes regression - hang task on Qualcomm RB1 board (QRB2210) and unable to use serial at all during normal boot: INFO: task kworker/u16:0:12 blocked for more than 42 seconds. Not tainted 6.17.0-rc1-00004-g53e760d89498 #9 "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. task:kworker/u16:0 state:D stack:0 pid:12 tgid:12 ppid:2 task_flags:0x4208060 flags:0x00000010 Workqueue: async async_run_entry_fn Call trace: __switch_to+0xe8/0x1a0 (T) __schedule+0x290/0x7c0 schedule+0x34/0x118 rpm_resume+0x14c/0x66c rpm_resume+0x2a4/0x66c rpm_resume+0x2a4/0x66c rpm_resume+0x2a4/0x66c __pm_runtime_resume+0x50/0x9c __driver_probe_device+0x58/0x120 driver_probe_device+0x3c/0x154 __driver_attach_async_helper+0x4c/0xc0 async_run_entry_fn+0x34/0xe0 process_one_work+0x148/0x290 worker_thread+0x2c4/0x3e0 kthread+0x118/0x1c0 ret_from_fork+0x10/0x20 The issue was reported on 12th of August and was ignored by author of commits introducing issue for two weeks. Only after complaining author produced a fix which did not work, so if original commits cannot be reliably fixed for 5 weeks, they obviously are buggy and need to be dropped.	N/A	More Details
CVE-2025-64450	Rejected reason: Not used	N/A	More Details
CVE-2025-58627	Authorization Bypass Through User-Controlled Key vulnerability in kamleshyadav Miraculous Core Plugin miraculouscore allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Miraculous Core Plugin: from n/a through < 2.0.9.	N/A	More Details
CVE-2025-58629	Missing Authorization vulnerability in kamleshyadav Miraculous miraculous allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Miraculous: from n/a through < 2.0.9.	N/A	More Details
CVE-2025-58636	Deserialization of Untrusted Data vulnerability in CRM Perks WP Gravity Forms Keap/Infusionsoft gf-infusionsoft allows Object Injection.This issue affects WP Gravity Forms Keap/Infusionsoft: from n/a through <= 1.2.3.	N/A	More Details
CVE-	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. In versions 7.14.7 and below and 8.0.0-beta.1 through 8.9.0 8.0.0-beta.1, an attacker can craft a malicious call_id that alters the logic of		More

2025-64488	the SQL query or injects arbitrary SQL. An attack can lead to unauthorized data access and data ex-filtration, complete database compromise, and other various issues. This issue is fixed in versions 7.14.8 and 8.9.1.	N/A	Details
CVE-2025-64486	calibre is an e-book manager. In versions 8.13.0 and prior, calibre does not validate filenames when handling binary assets in FB2 files, allowing an attacker to write arbitrary files on the filesystem when viewing or converting a malicious FictionBook file. This can be leveraged to achieve arbitrary code execution. This issue is fixed in version 8.14.0.	N/A	More Details
CVE-2025-64485	CVAT is an open source interactive video and image annotation tool for computer vision. In versions 2.4.0 through 2.48.1, a malicious CVAT user with at least the User global role may create files in the root of the mounted file share, or overwrite existing files. If no file share is mounted, the user will be able to create files in the share directory of the import worker container, potentially filling up disk space. This issue is fixed in version 2.49.0.	N/A	More Details
CVE-2025-58964	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Enzy enzy allows Reflected XSS.This issue affects Enzy: from n/a through < 1.6.4.	N/A	More Details
CVE-2025-12943	Improper certificate validation in firmware update logic in NETGEAR RAX30 (Nighthawk AX5 5-Stream AX2400 WiFi 6 Router) and RAXE300 (Nighthawk AXE7800 Tri-Band WiFi 6E Router) allows attackers with the ability to intercept and tamper traffic destined to the device to execute arbitrary commands on the device. Devices with automatic updates enabled may already have this patch applied. If not, please check the firmware version and update to the latest. Fixed in: RAX30 firmware 1.0.14.108 or later. RAXE300 firmware 1.0.9.82 or later	N/A	More Details
CVE-2025-12418	Potential Denial of Service issue in all supported versions of Revenera InstallShield version 2025 R1, 2024 R2, 2023 R2, and prior. When e.g., a local administrator performs an uninstall, a symlink may get followed on removal of a user writeable configuration directory and induce a Denial of Service as a result. The issue is resolved through the hotfixes InstallShield2025R1-CVE-2025-12418-SecurityPatch, InstallShield2024R2-CVE-2025-12418-SecurityPatch, and InstallShield2023R2-CVE-2025-12418-SecurityPatch.	N/A	More Details
CVE-2020-36870	Various Ruijie Gateway EG and NBR models firmware versions 11.1(6)B9P1 < 11.9(4)B12P1 contain a code execution vulnerability in the EWEB management system that can be abused via front-end functionality. Attackers can exploit front-end code when features such as guest authentication, local server authentication, or screen mirroring are enabled to gain access or execute commands on affected devices. Exploitation evidence was first observed by the Shadowserver Foundation on 2025-06-07 UTC.	N/A	More Details
CVE-2025-64442	HumHub is an Open Source Enterprise Social Network. Versions below 1.17.4 have a XSS vulnerability in the Meta-Search feature which allows malicious input to be executed in search previews. This issue is fixed in version 1.17.4.	N/A	More Details
CVE-2025-64439	LangGraph SQLite Checkpoint is an implementation of LangGraph CheckpointSaver that uses SQLite DB (both sync and async, via aiosqlite). In versions 2.1.2 and below, the JsonPlusSerializer (used as the default serialization protocol for all checkpointing) contains a Remote Code Execution (RCE) vulnerability when deserializing payloads saved in the "json" serialization mode. By default, the serializer attempts to use "msgpack" for serialization. However, prior to version 3.0 of the checkpointer library, if illegal Unicode surrogate values caused serialization to fail, it would fall back to using the "json" mode. This issue is fixed in version 3.0.0.	N/A	More Details

CVE-2025-63544	TechStore 1.0 is vulnerable to Cross Site Scripting (XSS) in /order_notes via the id parameter.	N/A	More Details
CVE-2025-63543	TechStore 1.0 is vulnerable to Cross Site Scripting (XSS) in the /search_results endpoint via the q parameter.	N/A	More Details
CVE-2025-58972	Path Traversal: '.../...//' vulnerability in Dmitry V. (CEO of "UKR Solution") Barcode Scanner with Inventory & Order Manager barcode-scanner-lite-pos-to-manage-products-inventory-and-orders allows Path Traversal.This issue affects Barcode Scanner with Inventory & Order Manager: from n/a through <= 1.10.4.	N/A	More Details
CVE-2025-63640	Sourcecodester Medicine Reminder App v1.0 is vulnerable to Cross-Site Scripting (XSS) in the "Medicine Name" and "Notes (Optional)" fields when creating an "Upcoming Reminder", allowing an attacker to inject arbitrary potentially malicious HTML/JavaScript code that executes in the victim's browser upon clicking the "Save Reminder" button.	N/A	More Details
CVE-2025-63639	The chat feature in the application Sourcecodester FAQ Bot with AI Assistant v1.0 is vulnerable to Cross-Site Scripting (XSS) due to improper handling of user-supplied input. An attacker can inject malicious HTML or JavaScript into chat messages, which executes in the browser of any user viewing the conversation.	N/A	More Details
CVE-2025-63638	Sourcecodester AI-Powered To-Do List App v1.0 is vulnerable to Cross-Site Scripting (XSS) in the "Task Title" and "Description (Optional)" fields when creating a Task, allowing an attacker to inject arbitrary potentially malicious HTML/JavaScript code that executes in the victim's browser upon clicking the "Add Task" button.	N/A	More Details
CVE-2025-64431	Zitadel is an open source identity management platform. Versions 4.0.0-rc.1 through 4.6.2 are vulnerable to secure Direct Object Reference (IDOR) attacks through its V2Beta API, allowing authenticated users with specific administrator roles within one organization to access and modify data belonging to other organizations. Note that this vulnerability is limited to organization-level data (name, domains, metadata). No other related data (such as users, projects, applications, etc.) is affected. This issue is fixed in version 4.6.3.	N/A	More Details
CVE-2025-63717	The change password functionality at /pet_grooming/admin/change_pass.php in SourceCodester Pet Grooming Management Software 1.0 is vulnerable to Cross-Site Request Forgery (CSRF) attacks. The application does not implement adequate anti-CSRF tokens or same-site cookie restrictions, allowing attackers to trick authenticated users into unknowingly changing their passwords.	N/A	More Details
CVE-2025-12944	Improper input validation in NETGEAR DGN2200v4 (N300 Wireless ADSL2+ Modem Router) allows attackers with direct network access to the device to potentially execute code on the device. Please check the firmware version and update to the latest. Fixed in: DGN2200v4 firmware 1.0.0.132 or later	N/A	More Details
CVE-2025-12942	Improper Input Validation vulnerability in NETGEAR R6260 and NETGEAR R6850 allows unauthenticated attackers connected to LAN with ability to perform MiTM attacks and control over DNS Server to perform command execution.This issue affects R6260: through 1.1.0.86; R6850: through 1.1.0.86.	N/A	More Details
CVE-2025-11696	A local server-side request forgery (SSRF) security issue exists within Studio 5000® Simulation Interface™ via the API. This vulnerability allows any Windows user on the system to trigger outbound SMB requests, enabling the capture of NTLM hashes.	N/A	More Details
CVE-2025-13015	Spoofing issue in Firefox. This vulnerability affects Firefox < 145, Firefox ESR < 140.5, and Firefox ESR < 115.30.	N/A	More Details

CVE-2025-11697	A local code execution security issue exists within Studio 5000® Simulation Interface™ via the API. This vulnerability allows any Windows user on the system to extract files using path traversal sequences, resulting in execution of scripts with Administrator privileges on system reboot.	N/A	More Details
CVE-2025-11862	A security issue was discovered within Verve Asset Manager allowing unauthorized read-only users to read, update, and delete users via the API.	N/A	More Details
CVE-2025-12101	Cross-Site Scripting (XSS) in NetScaler ADC and NetScaler Gateway when the appliance is configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server	N/A	More Details
CVE-2025-64452	Rejected reason: Not used	N/A	More Details
CVE-2025-12405	An improper privilege management vulnerability was found in Looker Studio. It impacted all JDBC-based connectors. A Looker Studio user with report view access could make a copy of the report and execute arbitrary SQL that would run on the data source database due to the stored credentials attached to the report. This vulnerability was patched on 21 July 2025, and no customer action is needed.	N/A	More Details
CVE-2024-57695	An issue in Agnitum Outpost Security Suite 7.5.3 (3942.608.1810) and 7.6 (3984.693.1842) allows a local attacker to execute arbitrary code via the lock function. The manufacturer fixed the vulnerability in version 8.0 (4164.652.1856) from December 17, 2012.	N/A	More Details
CVE-2025-41107	Stored Cross Site Scripting (XSS) vulnerability in Smart School 7.0 due to lack of proper validation of user input when sending a POST request to '/online_admission', wich affects the parameters 'firstname', 'lastname', 'guardian_name' and others. This vulnerability could allow a remote user to send a specially crafted query to an authenticated user and steal his/her session cookie details.	N/A	More Details
CVE-2025-12409	A SQL injection vulnerability was discovered in Looker Studio that allowed for data exfiltration from BigQuery data sources. By creating a malicious report with native functions enabled, and having the victim access the report, an attacker could execute injected SQL queries with the victim's permissions in BigQuery. This vulnerability was patched on 07 July 2025, and no customer action is needed.	N/A	More Details
CVE-2025-12397	A SQL injection vulnerability was found in Looker Studio. A Looker Studio user with report view access could inject malicious SQL that would execute with the report owner's permissions. The vulnerability affected to reports with BigQuery as the data source. This vulnerability was patched on 21 July 2025, and no customer action is needed.	N/A	More Details
CVE-2025-13012	Race condition in the Graphics component. This vulnerability affects Firefox < 145, Firefox ESR < 140.5, and Firefox ESR < 115.30.	N/A	More Details
CVE-2025-13013	Mitigation bypass in the DOM: Core & HTML component. This vulnerability affects Firefox < 145, Firefox ESR < 140.5, and Firefox ESR < 115.30.	N/A	More Details
CVE-2025-13014	Use-after-free in the Audio/Video component. This vulnerability affects Firefox < 145, Firefox ESR < 140.5, and Firefox ESR < 115.30.	N/A	More Details
CVE-2025-	Incorrect boundary conditions in the JavaScript: WebAssembly component. This	N/A	More

13016	vulnerability affects Firefox < 145 and Firefox ESR < 140.5.		Details
CVE-2025-12940	Login credentials are inadvertently recorded in logs if a Syslog Server is configured in NETGEAR WAX610 and WAX610Y (AX1800 Dual Band PoE Multi-Gig Insight Managed WiFi 6 Access Points). An user having access to the syslog server can read the logs containing these credentials. This issue affects WAX610: before 10.8.11.4; WAX610Y: before 10.8.11.4. Devices managed with Insight get automatic updates. If not, please check the firmware version and update to the latest. Fixed in: WAX610 firmware 11.8.0.10 or later. WAX610Y firmware 11.8.0.10 or later.	N/A	More Details
CVE-2025-13017	Same-origin policy bypass in the DOM: Notifications component. This vulnerability affects Firefox < 145 and Firefox ESR < 140.5.	N/A	More Details
CVE-2025-13018	Mitigation bypass in the DOM: Security component. This vulnerability affects Firefox < 145 and Firefox ESR < 140.5.	N/A	More Details
CVE-2025-13019	Same-origin policy bypass in the DOM: Workers component. This vulnerability affects Firefox < 145 and Firefox ESR < 140.5.	N/A	More Details
CVE-2025-13020	Use-after-free in the WebRTC: Audio/Video component. This vulnerability affects Firefox < 145 and Firefox ESR < 140.5.	N/A	More Details
CVE-2025-13021	Incorrect boundary conditions in the Graphics: WebGPU component. This vulnerability affects Firefox < 145.	N/A	More Details
CVE-2025-13022	Incorrect boundary conditions in the Graphics: WebGPU component. This vulnerability affects Firefox < 145.	N/A	More Details
CVE-2025-13023	Sandbox escape due to incorrect boundary conditions in the Graphics: WebGPU component. This vulnerability affects Firefox < 145.	N/A	More Details
CVE-2025-13024	JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability affects Firefox < 145.	N/A	More Details
CVE-2025-13025	Incorrect boundary conditions in the Graphics: WebGPU component. This vulnerability affects Firefox < 145.	N/A	More Details
CVE-2025-13026	Sandbox escape due to incorrect boundary conditions in the Graphics: WebGPU component. This vulnerability affects Firefox < 145.	N/A	More Details
CVE-2025-13027	Memory safety bugs present in Firefox 144 and Thunderbird 144. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 145.	N/A	More Details
CVE-	A Command Injection vulnerability, resulting from improper file path sanitization (Directory Traversal) in Looker allows an attacker with Developer permission to execute arbitrary shell commands when a user is deleted on the host system. Looker-hosted and Self-hosted were found to be vulnerable. This issue has already been mitigated for Looker-hosted instances. No user action is required for these.		More

2025-12155	Self-hosted instances must be upgraded as soon as possible. This vulnerability has been patched in all supported versions of Self-hosted. The versions below have all been updated to protect from this vulnerability. You can download these versions at the Looker download page https://download.looker.com/ : * 24.12.100+ * 24.18.192+ * 25.0.69+ * 25.6.57+ * 25.8.39+ * 25.10.22+	N/A	Details
CVE-2025-60242	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Anatoly Download Counter download-counter allows Path Traversal.This issue affects Download Counter: from n/a through <= 1.4.	N/A	More Details