SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 01 October 2025

Generated on 01 October 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-2025-58384	In DOXENSE WATCHDOC before 6.1.1.5332, Deserialization of Untrusted Data can lead to remote code execution through the .NET Remoting library in the Watchdoc administration interface.	10.0	More Details
CVE-2025-60219	Unrestricted Upload of File with Dangerous Type vulnerability in HaruTheme WooCommerce Designer Pro allows Upload a Web Shell to a Web Server. This issue affects WooCommerce Designer Pro: from n/a through 1.9.24.	10.0	More Details
CVE-2025-10725	A flaw was found in Red Hat Openshift AI Service. A low-privileged attacker with access to an authenticated account, for example as a data scientist using a standard Jupyter notebook, can escalate their privileges to a full cluster administrator. This allows for the complete compromise of the cluster's confidentiality, integrity, and availability. The attacker can steal sensitive data, disrupt all services, and take control of the underlying infrastructure, leading to a total breach of the platform and all applications hosted on it.	9.9	More Details
CVE-2025-59832	Horilla is a free and open source Human Resource Management System (HRMS). Prior to version 1.4.0, there is a stored XSS vulnerability in the ticket comment editor. A low-privilege authenticated user could run arbitrary JavaScript in an admin’s browser, exfiltrate the admin’s cookies/CSRF token, and hijack their session. This issue has been patched in version 1.4.0.	9.9	More Details
CVE-2025-20333	A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to improper validation of user-supplied input in HTTP(S) requests. An attacker with valid VPN user credentials could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as root, possibly resulting in the complete compromise of the affected device.	9.9	More Details
CVE-2025-55187	In DriveLock 24.1.4 before 24.1.5, 24.2.5 before 24.2.6, and 25.1.2 before 25.1.4, attackers can gain elevated privileges.	9.9	More Details
CVE-2025-41715	The database for the web application is exposed without authentication, allowing an unauthenticated remote attacker to gain unauthorized access and potentially compromise it.	9.8	More Details
	The MultiLoca - WooCommerce Multi Locations Inventory Management plugin for WordPress is		

CVE-2025-9054	vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the 'wcmlim_settings_ajax_handler' function in all versions up to, and including, 4.2.8. This makes it possible for unauthenticated attackers to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	9.8	More Details
CVE-2025-9762	The Post By Email plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the save_attachments function in all versions up to, and including, 1.0.4b. 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-2025-8625	The Copypress Rest API plugin for WordPress is vulnerable to Remote Code Execution via copyreap_handle_image() Function in versions 1.1 to 1.2. The plugin falls back to a hard-coded JWT signing key when no secret is defined and does not restrict which file types can be fetched and saved as attachments. As a result, unauthenticated attackers can forge a valid token to gain elevated privileges and upload an arbitrary file (e.g. a PHP script) through the image handler, leading to remote code execution.	9.8	More Details
CVE-2025-11148	All versions of the package check-branches are vulnerable to Command Injection check-branches is a command-line tool that is interacted with locally, or via CI, to confirm no conflicts exist in git branches. However, the library follows these conventions which can be abused: 1. It trusts branch names as they are (plain text) 2. It spawns git commands by concatenating user input Since a branch name is potentially a user input - as users can create branches remotely via pull requests, or simply due to privileged access to a repository - it can effectively be abused to run any command.	9.8	More Details
CVE-2025-54875	FreshRSS is a free, self-hostable RSS aggregator. In versions 1.16.0 and above through 1.26.3, an unprivileged attacker can create a new admin user when registration is enabled through the use of a hidden field used only in the user management admin page, new_user_is_admin. This is fixed in version 1.27.0.	9.8	More Details
CVE-2025-57266	An issue was discovered in file AssistantController.java in ThriveX Blogging Framework 2.5.9 thru 3.1.3 allowing unauthenticated attackers to gain sensitive information such as API Keys via the /api/assistant/list endpoint.	9.8	More Details
CVE-2024-13150	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Fayton Software and Consulting Services fayton.Pro ERP allows SQL Injection.This issue affects fayton.Pro ERP: through 20250929.	9.8	More Details
CVE-2025-8868	In Progress Chef Automate, versions earlier than 4.13.295, on Linux x86 platform, an authenticated attacker can gain access to Chef Automate restricted functionality in the compliance service via improperly neutralized inputs used in an SQL command using a well-known token.	9.8	More Details
CVE-2025-11126	A security flaw has been discovered in Apeman ID71 218.53.203.117. This vulnerability affects unknown code of the file /system/www/system.ini. The manipulation results in hard-coded credentials. The attack may be performed from remote. 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.	9.8	More Details
CVE-2025-10659	The Telenium Online Web Application is vulnerable due to a PHP endpoint accessible to unauthenticated network users that improperly handles user-supplied input. This vulnerability occurs due to the insecure termination of a regular expression check within the endpoint. Because the input is not correctly validated or sanitized, an unauthenticated attacker can inject arbitrary operating system commands through a crafted HTTP request, leading to remote code execution on the server in the context of the web application service account.	9.8	More Details
CVE-2025-59841	Flag Forge is a Capture The Flag (CTF) platform. In versions from 2.2.0 to before 2.3.1, the FlagForge web application improperly handles session invalidation. Authenticated users can continue to access protected endpoints, such as /api/profile, even after logging out. CSRF tokens are also still valid post-logout, which can allow unauthorized actions. This issue has been patched in version 2.3.1.	9.8	More Details
CVE-2025-10542	iMonitor EAM 9.6394 ships with default administrative credentials that are also displayed within the management client’s connection dialog. If the administrator does not change these defaults, a remote attacker can authenticate to the EAM server and gain full control over monitored agents and data. This enables reading highly sensitive telemetry (including keylogger output) and issuing arbitrary actions to all connected clients.	9.8	More Details
CVE-2025-59834	ADB MCP Server is a MCP (Model Context Protocol) server for interacting with Android devices through ADB. In versions 0.1.0 and prior, the MCP Server is written in a way that is vulnerable to command injection vulnerability attacks as part of some of its MCP Server tool definition and implementation. This issue has been patched via commit 041729c.	9.8	More Details

CVE-2025-57321	A Prototype Pollution vulnerability in the util-deps.addFileDepend function of magix-combine-ex versions thru 1.2.10 allows attackers to inject properties on Object.prototype via supplying a crafted payload, causing denial of service (DoS) as the minimum consequence.	9.8	More Details
CVE-2025-57347	A vulnerability exists in the 'dagre-d3-es' Node.js package version 7.0.9, specifically within the 'bk' module's addConflict function, which fails to properly sanitize user-supplied input during property assignment operations. This flaw allows attackers to exploit prototype pollution vulnerabilities by injecting malicious input values (e.g., "__proto__"), enabling unauthorized modification of the JavaScript Object prototype chain. Successful exploitation could lead to denial of service conditions, unexpected application behavior, or potential execution of arbitrary code in contexts where polluted properties are later accessed or executed. The issue affects versions prior to 7.0.11 and remains unpatched at the time of disclosure.	9.8	More Details
CVE-2025-10585	Type confusion in V8 in Google Chrome prior to 140.0.7339.185 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	9.8	More Details
CVE-2025-56819	An issue in Datart v.1.0.0-rc.3 allows a remote attacker to execute arbitrary code via the INIT connection parameter.	9.8	More Details
CVE-2025-27034	Memory corruption while selecting the PLMN from SOR failed list.	9.8	More Details
CVE-2025-21483	Memory corruption when the UE receives an RTP packet from the network, during the reassembly of NALUs.	9.8	More Details
CVE-2025-10894	Malicious code was inserted into the Nx (build system) package and several related plugins. The tampered package was published to the npm software registry, via a supply-chain attack. Affected versions contain code that scans the file system, collects credentials, and posts them to GitHub as a repo under user's accounts.	9.6	More Details
CVE-2025-60156	Cross-Site Request Forgery (CSRF) vulnerability in webandprint AR For WordPress allows Upload a Web Shell to a Web Server. This issue affects AR For WordPress: from n/a through 7.98.	9.6	More Details
CVE-2025-59934	Formbricks is an open source qualtrics alternative. Prior to version 4.0.1, Formbricks is missing JWT signature verification. This vulnerability stems from a token validation routine that only decodes JWTs (jwt.decode) without verifying their signatures. Both the email verification token login path and the password reset server action use the same validator, which does not check the token’s signature, expiration, issuer, or audience. If an attacker learns the victim’s actual user.id, they can craft an arbitrary JWT with an alg: "none" header and use it to authenticate and reset the victim’s password. This issue has been patched in version 4.0.1.	9.4	More Details
CVE-2025-10890	Side-channel information leakage in V8 in Google Chrome prior to 140.0.7339.207 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	9.1	More Details
CVE-2024-58040	Crypt::RandomEncryption for Perl version 0.01 uses insecure rand() function during encryption.	9.1	More Details
CVE-2025-7493	A privilege escalation flaw from host to domain administrator was found in FreeIPA. This vulnerability is similar to CVE-2025-4404, where it fails to validate the uniqueness of the krbCanonicalName. While the previously released version added validations for the admin@REALM credential, FreeIPA still does not validate the root@REALM canonical name, which can also be used as the realm administrator's name. This flaw allows an attacker to perform administrative tasks over the REALM, leading to access to sensitive data and sensitive data exfiltration.	9.1	More Details
CVE-2025-20363	A vulnerability in the web services of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, Cisco Secure Firewall Threat Defense (FTD) Software, Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an unauthenticated, remote attacker (Cisco ASA and FTD Software) or authenticated, remote attacker (Cisco IOS, IOS XE, and IOS XR Software) with low user privileges to execute arbitrary code on an affected device. This vulnerability is due to improper validation of user-supplied input in HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted web service on an affected device after obtaining additional information about the system, overcoming exploit mitigations, or both. A successful exploit could allow the attacker to execute arbitrary code as root, which may lead to the complete compromise of the affected device. For more information about this vulnerability, see the Details ["#details"] section of this advisory.	9.0	More Details

OTHER VULNERABILITIES

CVE		Base	

Number	Description	Score	Reference
CVE-2025-10467	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PROLIZ Computer Software Hardware Service Trade Ltd. Co. OBS (Student Affairs Information System) allows Stored XSS.This issue affects OBS (Student Affairs Information System): before v25.0401.	8.9	More Details
CVE-2025-11091	A security flaw has been discovered in Tenda AC21 up to 16.03.08.16. Affected by this vulnerability is the function sscanf of the file /goform/SetStaticRouteCfg. The manipulation of the argument list results in buffer overflow. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	8.8	More Details
CVE-2025-11123	A flaw has been found in Tenda AC18 15.03.05.19. This impacts an unknown function of the file /goform/saveAutoQos. This manipulation of the argument enable causes stack-based buffer overflow. The attack may be initiated remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2025-55848	An issue was discovered in DIR-823 firmware 20250416. There is an RCE vulnerability in the set_cassword settings interface, as the http_casswd parameter is not filtered by '&'to allow injection of reverse connection commands.	8.8	More Details
CVE-2025-10953	A security vulnerability has been detected in UTT 1200GW and 1250GW up to 3.0.0-170831/3.2.2-200710. This vulnerability affects unknown code of the file /goform/formApMail. The manipulation of the argument senderEmail leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-7052	The LatePoint plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.1.94. This is due to missing nonce validation on the change_password() function of its customer_cabinet__change_password AJAX route. The plugin hooks this endpoint via wp_ajax and wp_ajax_nopriv but does not verify a nonce or user capability before resetting the user’s password. This makes it possible for unauthenticated attackers who trick a logged-in customer (or, with “WP users as customers” enabled, an administrator) into visiting a malicious link to take over their account.	8.8	More Details
CVE-2025-6724	In Progress Chef Automate, versions earlier than 4.13.295, on Linux x86 platform, an authenticated attacker can gain access to Chef Automate restricted functionality in multiple services via improperly neutralized inputs used in an SQL command.	8.8	More Details
CVE-2025-55847	Wavlink M86X3A_V240730 contains a buffer overflow vulnerability in the /cgi-bin/ExportAllSettings.cgi file. The vulnerability arises because the Cookie parameter does not properly validate the length of input data. Attackers can exploit this to execute arbitrary code or cause a denial of service (DoS) on the system	8.8	More Details
CVE-2025-10500	Use after free in Dawn in Google Chrome prior to 140.0.7339.185 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-10501	Use after free in WebRTC in Google Chrome prior to 140.0.7339.185 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-10502	Heap buffer overflow in ANGLE in Google Chrome prior to 140.0.7339.185 allowed a remote attacker to potentially exploit heap corruption via malicious network traffic. (Chromium security severity: High)	8.8	More Details
CVE-2025-10891	Integer overflow in V8 in Google Chrome prior to 140.0.7339.207 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-10892	Integer overflow in V8 in Google Chrome prior to 140.0.7339.207 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-11120	A weakness has been identified in Tenda AC8 16.03.34.06. The affected element is the function formSetServerConfig of the file /goform/SetServerConfig. Executing manipulation can lead to buffer overflow. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited.	8.8	More Details
CVE-2025-11117	A vulnerability was determined in Tenda CH22 1.0.0.1. This vulnerability affects the function formWrlExtraGet of the file /goform/GstDhcpSetSer. This manipulation of the argument dips causes buffer overflow. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details

CVE-2025-20334	A vulnerability in the HTTP API subsystem of Cisco IOS XE Software could allow a remote attacker to inject commands that will execute with root privileges into the underlying operating system. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by authenticating to an affected system and performing an API call with crafted input. Alternatively, an unauthenticated attacker could persuade a legitimate user with administrative privileges who is currently logged in to the system to click a crafted link. A successful exploit could allow the attacker to execute arbitrary commands as the root user.	8.8	More Details
CVE-2025-60126	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in PluginOps Testimonial Slider allows PHP Local File Inclusion. This issue affects Testimonial Slider: from n/a through 3.5.8.6.	8.8	More Details
CVE-2025-56816	Datart 1.0.0-rc.3 is vulnerable to Directory Traversal. The configuration file handling of the application allows attackers to upload arbitrary YAML files to the config/jdbc-driver-ext.yml path. The application parses this file using SnakeYAML's unsafe load() or loadAs() method without input sanitization. This allows deserialization of attacker-controlled YAML content, leading to arbitrary class instantiation. Under certain conditions, this can be exploited to achieve remote code execution (RCE).	8.8	More Details
CVE-2025-59814	This vulnerability allows malicious actors to gain unauthorized access to the Zenitel ICX500 and ICX510 Gateway Billing Admin endpoint, enabling them to read the entire contents of the Billing Admin database.	8.8	More Details
CVE-2025-10948	A vulnerability has been found in MikroTik RouterOS 7. This affects the function parse_json_element of the file /rest/ip/address/print of the component libjson.so. The manipulation leads to buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-60111	Cross-Site Request Forgery (CSRF) vulnerability in javothemes Javo Core allows Authentication Bypass. This issue affects Javo Core: from n/a through 3.0.0.266.	8.8	More Details
CVE-2025-36245	IBM InfoSphere 11.7.0.0 through 11.7.1.6 Information Server could allow an authenticated user to execute arbitrary commands with elevated privileges on the system due to improper validation of user supplied input.	8.8	More Details
CVE-2025-10942	A vulnerability was identified in H3C Magic B3 up to 100R002. This affects the function AddMacList of the file /goform/aspForm. The manipulation of the argument param leads to buffer overflow. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-59939	WeGIA is a Web manager for charitable institutions. Prior to version 3.5.0, WeGIA is vulnerable to SQL Injection attacks in the control.php endpoint with the following parameters: nomeClasse=ProdutoControle&metodo=excluir&id_produto=[malicious command]. It is necessary to apply prepared statements methods, sanitization, and validations on theid_produto parameter. This issue has been patched in version 3.5.0.	8.8	More Details
CVE-2025-11122	A vulnerability was detected in Tenda AC18 15.03.05.19. This affects an unknown function of the file /goform/WizardHandle. The manipulation of the argument WANT/mtuvalue results in stack-based buffer overflow. The attack can be launched remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2025-9642	An issue has been discovered in GitLab CE/EE affecting all versions from 14.10 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1 that could allow an attacker to inject malicious content that may lead to account takeover.	8.7	More Details
CVE-2025-23293	NVIDIA Delegated Licensing Service for all appliance platforms contains a vulnerability where an User/Attacker may cause an authorized action. A successful exploit of this vulnerability may lead to information disclosure.	8.7	More Details
CVE-2025-59839	The EmbedVideo Extension is a MediaWiki extension which adds a parser function called #ev and various parser tags for embedding video clips from various video sharing services. In versions 4.0.0 and prior, the EmbedVideo extension allows adding arbitrary attributes to an HTML element, allowing for stored XSS through wikitext. This issue has been patched via commit 4e075d3.	8.6	More Details
CVE-2025-20315	A vulnerability in the Network-Based Application Recognition (NBAR) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, causing a denial of service (DoS) condition. This vulnerability is due to improper handling of malformed Control and Provisioning of Wireless Access Points (CAPWAP) packets. An attacker could exploit this vulnerability by sending malformed CAPWAP packets through an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.	8.6	More Details
	The csvtojson package, a tool for converting CSV data to JSON with customizable parsing capabilities,		

CVE-2025-57350	csvtojson package, a tool for converting CSV data to JSON with customizable parsing capabilities, contains a prototype pollution vulnerability in versions prior to 2.0.10. This issue arises due to insufficient sanitization of nested header names during the parsing process in the parser_jsonarray component. When processing CSV input containing specially crafted header fields that reference prototype chains (e.g., using __proto__ syntax), the application may unintentionally modify properties of the base Object prototype. This vulnerability can lead to denial of service conditions or unexpected behavior in applications relying on unmodified prototype chains, particularly when untrusted CSV data is processed. The flaw does not require user interaction beyond providing a maliciously constructed CSV file.	8.6	More Details
CVE-2025-10449	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Saysis Computer Systems Trade Ltd. Co. Saysis Web Portal allows Path Traversal.This issue affects Saysis Web Portal: from 3.1.9 & 3.2.0 before 3.2.1.	8.6	More Details
CVE-2025-10438	Path Traversal: 'dir/../../filename' vulnerability in Yordam Information Technology Consulting Education and Electrical Systems Industry Trade Inc. Yordam Katalog allows Path Traversal.This issue affects Yordam Katalog: before 21.7.	8.6	More Details
CVE-2025-59932	Flag Forge is a Capture The Flag (CTF) platform. From versions 2.0.0 to before 2.3.1, the /api/resources endpoint previously allowed POST and DELETE requests without proper authentication or authorization. This could have enabled unauthorized users to create, modify, or delete resources on the platform. The issue has been fixed in FlagForge version 2.3.1.	8.6	More Details
CVE-2025-41250	VMware vCenter contains an SMTP header injection vulnerability. A malicious actor with non-administrative privileges on vCenter who has permission to create scheduled tasks may be able to manipulate the notification emails sent for scheduled tasks.	8.5	More Details
CVE-2025-60107	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup LambertGroup - AllInOne - Banner with Playlist allows Blind SQL Injection. This issue affects LambertGroup - AllInOne - Banner with Playlist: from n/a through 3.8.	8.5	More Details
CVE-2025-60108	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup LambertGroup - AllInOne - Banner with Thumbnails allows Blind SQL Injection. This issue affects LambertGroup - AllInOne - Banner with Thumbnails: from n/a through 3.8.	8.5	More Details
CVE-2025-60109	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup LambertGroup - AllInOne - Content Slider allows Blind SQL Injection. This issue affects LambertGroup - AllInOne - Content Slider: from n/a through 3.8.	8.5	More Details
CVE-2025-60110	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup AllInOne - Banner Rotator allows SQL Injection. This issue affects AllInOne - Banner Rotator: from n/a through 3.8.	8.5	More Details
CVE-2025-60118	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Potenzaglobalsolutions PGS Core allows SQL Injection. This issue affects PGS Core: from n/a through 5.9.0.	8.5	More Details
CVE-2025-10906	A flaw has been found in Magnetism Studios Endurance up to 3.3.0 on macOS. This affects the function loadModuleNamed:WithReply of the file /Applications/Endurance.app/Contents/Library/LaunchServices/com.MagnetismStudios.endurance.helper of the component NSXPC Interface. Executing manipulation can lead to missing authentication. The attack needs to be launched locally. The exploit has been published and may be used.	8.4	More Details
CVE-2025-59817	This vulnerability allows attackers to execute arbitrary commands on the underlying system. Because the web portal runs with root privileges, successful exploitation grants full control over the device, potentially compromising its availability, confidentiality, and integrity.	8.4	More Details
CVE-2025-59815	This vulnerability allows malicious actors to execute arbitrary commands on the underlying system of the Zenitel ICX500 and ICX510 Gateway, granting shell access. Exploitation can compromise the device’s availability, confidentiality, and integrity.	8.4	More Details
CVE-2025-56383	Notepad++ v8.8.3 has a DLL hijacking vulnerability, which can replace the original DLL file to execute malicious code.	8.4	More Details
CVE-2025-11130	A weakness has been identified in iHongRen pptp-vpn 1.0/1.0.1 on macOS. This issue affects the function shouldAcceptNewConnection of the file HelpTool/HelperTool.m of the component XPC Service. This manipulation causes missing authentication. The attack can only be executed locally. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	8.4	More Details
	The LatePoint plugin for WordPress is vulnerable to Authentication Bypass due to insufficient identity verification within the steps_load_step route of the latepoint_route_call AJAX endpoint in all versions up		

CVE-2025-7038	to, and including, 5.1.94. The endpoint reads the client-supplied customer email and related customer fields before invoking the internal login handler without verifying login status, capability checks, or a valid AJAX nonce. This makes it possible for unauthenticated attackers to log into any customer's account.	8.2	More Details
CVE-2025-21487	Information disclosure while decoding RTP packet received by UE from the network, when payload length mentioned is greater than the available buffer length.	8.2	More Details
CVE-2025-21488	Information disclosure while decoding this RTP packet headers received by UE from the network when the padding bit is set.	8.2	More Details
CVE-2025-60017	Unitree Go2, G1, H1, and B2 devices through 2025-09-20 allow root OS command injection via the hostapd_restart.sh wifi_ssid or wifi_pass parameter (within restart_wifi_ap and restart_wifi_sta).	8.2	More Details
CVE-2025-59845	Apollo Studio Embeddable Explorer & Embeddable Sandbox are website embeddable software solutions from Apollo GraphQL. Prior to Apollo Sandbox version 2.7.2 and Apollo Explorer version 3.7.3, a cross-site request forgery (CSRF) vulnerability was identified. The vulnerability arises from missing origin validation in the client-side code that handles window.postMessage events. A malicious website can send forged messages to the embedding page, causing the victim's browser to execute arbitrary GraphQL queries or mutations against their GraphQL server while authenticated with the victim's cookies. This issue has been patched in Apollo Sandbox version 2.7.2 and Apollo Explorer version 3.7.3.	8.2	More Details
CVE-2025-21484	Information disclosure when UE receives the RTP packet from the network, while decoding and reassembling the fragments from RTP packet.	8.2	More Details
CVE-2025-20160	A vulnerability in the implementation of the TACACS+ protocol in Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to view sensitive data or bypass authentication. This vulnerability exists because the system does not properly check whether the required TACACS+ shared secret is configured. A machine-in-the-middle attacker could exploit this vulnerability by intercepting and reading unencrypted TACACS+ messages or impersonating the TACACS+ server and falsely accepting arbitrary authentication requests. A successful exploit could allow the attacker to view sensitive information in a TACACS+ message or bypass authentication and gain access to the affected device.	8.1	More Details
CVE-2025-9993	The Bei Fen – WordPress Backup Plugin plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.4.2 via the 'task'. This makes it possible for authenticated attackers, with Subscriber-level access and above, 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. This only affects instances running PHP 7.1 or older.	8.1	More Details
CVE-2025-9991	The Tiny Bootstrap Elements Light plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 4.3.34 via the 'language' 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-2025-57483	A reflected cross-site scripting (XSS) vulnerability in tawk.to chatbox widget v4 allows attackers to execute arbitrary Javascript in the context of the user's browser via injecting a crafted payload into the vulnerable parameter.	8.1	More Details
CVE-2025-41251	VMware NSX contains a weak password recovery mechanism vulnerability. An unauthenticated malicious actor may exploit this to enumerate valid usernames, potentially enabling brute-force attacks. Impact: Username enumeration → credential brute force risk. Attack Vector: Remote, unauthenticated. Severity: Important. CVSSv3: 8.1 (High). Acknowledgments: Reported by the National Security Agency. Affected Products:VMware NSX 9.x.x.x, 4.2.x, 4.1.x, 4.0.x NSX-T 3.x VMware Cloud Foundation (with NSX) 5.x, 4.5.x Fixed Versions: NSX 9.0.1.0; 4.2.2.2/4.2.3.1 http://4.2.2.2/4.2.3.1 ; 4.1.2.7; NSX-T 3.2.4.3; CCF async patch (KB88287). Workarounds: None.	8.1	More Details
CVE-2025-35030	Medical Informatics Engineering Enterprise Health has a cross site request forgery vulnerability that allows an unauthenticated attacker to trick administrative users into clicking a crafted URL and perform actions on behalf of that administrative user. This issue is fixed as of 2025-04-08.	8.1	More Details
CVE-2025-	SysReptor is a fully customizable pentest reporting platform. In versions from 2024.74 to before 2025.83, authenticated and unprivileged (non-admin) users can assign the is_project_admin permission to their own user. This allows users to read, modify and delete pentesting projects they are not members of and	8.1	More

59945	own user. This allows users to read, modify and delete pentesting projects they are not members of and are therefore not supposed to access. This issue has been patched in version 2025.83.		Details
CVE-2025-58319	Delta Electronics CNCSoft-G2 lacks proper validation of the user-supplied file. If a user opens a malicious file, an attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2025-10541	iMonitor EAM 9.6394 installs a system service (eamusbsrv64.exe) that runs with NT AUTHORITY\SYSTEM privileges. This service includes an insecure update mechanism that automatically loads files placed in the C:\sysupdate\ directory during startup. Because any local user can create and write to this directory, an attacker can place malicious DLLs or executables in it. Upon service restart, the files are moved to the application’s installation path and executed with SYSTEM privileges, leading to privilege escalation.	7.8	More Details
CVE-2025-43993	Dell Wireless 5932e and Qualcomm Snapdragon X62 Firmware and GNSS/GPS Driver, versions prior to 3.2.0.22 contain an Unquoted Search Path or Element vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code Execution.	7.8	More Details
CVE-2025-58317	Delta Electronics CNCSoft-G2 lacks proper validation of the user-supplied file. If a user opens a malicious file, an attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2025-21476	Memory corruption when passing parameters to the Trusted Virtual Machine during the handshake.	7.8	More Details
CVE-2025-6034	There is a memory corruption vulnerability due to an out of bounds read in DefaultFontOptions() when using SymbolEditor in NI Circuit Design Suite. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted .sym file. This vulnerability affects NI Circuit Design Suite 14.3.1 and prior versions.	7.8	More Details
CVE-2025-23354	NVIDIA Megatron-LM for all platforms contains a vulnerability in the ensemble_classifer script where malicious data created by an attacker may cause an 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-2025-23353	NVIDIA Megatron-LM for all platforms contains a vulnerability in the msdp preprocessing script where malicious data created by an attacker may cause an 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-2025-23349	NVIDIA Megatron-LM for all platforms contains a vulnerability in the tasks/orqa/unsupervised/nq.py component, where 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-2025-23348	NVIDIA Megatron-LM for all platforms contains a vulnerability in the pretrain_gpt 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, and data tampering.	7.8	More Details
CVE-2025-10941	A vulnerability was determined in Topaz SERVCore Teller 2.14.0-RC2/2.14.1. Affected by this issue is some unknown functionality of the file SERVCoreTeller_2.0.40D.msi of the component Installer. Executing manipulation can lead to permission issues. The attack needs to be launched locally. You should upgrade the affected component. The vendor explains, that "this vulnerability was detected at the beginning of 2025, it was remediated because the latest published version of the installer no longer uses "nssm," which is responsible for this vulnerability".	7.8	More Details
CVE-2025-6033	There is a memory corruption vulnerability due to an out of bounds write in XML_Serialize() when using SymbolEditor in NI Circuit Design Suite. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted .sym file. This vulnerability affects NI Circuit Design Suite 14.3.1 and prior versions.	7.8	More Details
CVE-2025-47317	Memory corruption due to global buffer overflow when a test command uses an invalid payload type.	7.8	More Details
CVE-2025-47315	Memory corruption while handling repeated memory unmap requests from guest VM.	7.8	More Details
CVE-2025-47316	Memory corruption due to double free when multiple threads race to set the timestamp store.	7.8	More Details
CVE-2025-	Memory corruption while processing data sent by FF driver.	7.8	More

47314	Memory corruption while processing data sent by V2 driver.		Details
CVE-2025-27077	Memory corruption while processing message in guest VM.	7.8	More Details
CVE-2025-21481	Memory corruption while performing private key encryption in trusted application.	7.8	More Details
CVE-2025-41244	VMware Aria Operations and VMware Tools contain a local privilege escalation vulnerability. A malicious local actor with non-administrative privileges having access to a VM with VMware Tools installed and managed by Aria Operations with SDMP enabled may exploit this vulnerability to escalate privileges to root on the same VM.	7.8	More Details
CVE-2025-27032	memory corruption while loading a PIL authenticated VM, when authenticated VM image is loaded without maintaining cache coherency.	7.8	More Details
CVE-2025-47327	Memory corruption while encoding the image data.	7.8	More Details
CVE-2025-47329	Memory corruption while handling invalid inputs in application info setup.	7.8	More Details
CVE-2025-27037	Memory corruption while processing config_dev IOCTL when camera kernel driver drops its reference to CPU buffers.	7.8	More Details
CVE-2025-20327	A vulnerability in the web UI of Cisco IOS Software could allow an authenticated, remote attacker with low privileges to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper input validation. An attacker could exploit this vulnerability by sending a crafted URL in an HTTP request. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	7.7	More Details
CVE-2025-59002	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in SeaTheme BM Content Builder allows Path Traversal. This issue affects BM Content Builder: from n/a through n/a.	7.7	More Details
CVE-2025-20312	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS XE Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper error handling when parsing a specific SNMP request. An attacker could exploit this vulnerability by sending a specific SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition. This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMPv2c or earlier, the attacker must know a valid read-write or read-only SNMP community string for the affected system. To exploit this vulnerability through SNMPv3, the attacker must have valid SNMP user credentials for the affected system.	7.7	More Details
CVE-2025-20352	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software could allow the following: An authenticated, remote attacker with low privileges could cause a denial of service (DoS) condition on an affected device that is running Cisco IOS Software or Cisco IOS XE Software. To cause the DoS, the attacker must have the SNMPv2c or earlier read-only community string or valid SNMPv3 user credentials. An authenticated, remote attacker with high privileges could execute code as the root user on an affected device that is running Cisco IOS XE Software. To execute code as the root user, the attacker must have the SNMPv1 or v2c read-only community string or valid SNMPv3 user credentials and administrative or privilege 15 credentials on the affected device. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device over IPv4 or IPv6 networks. This vulnerability is due to a stack overflow condition in the SNMP subsystem of the affected software. A successful exploit could allow a low-privileged attacker to cause the affected system to reload, resulting in a DoS condition, or allow a high-privileged attacker to execute arbitrary code as the root user and obtain full control of the affected system. Note: This vulnerability affects all versions of SNMP.	7.7	More Details
CVE-2025-41246	VMware Tools for Windows contains an improper authorisation vulnerability due to the way it handles user access controls. A malicious actor with non-administrative privileges on a guest VM, who is already authenticated through vCenter or ESX may exploit this issue to access other guest VMs. Successful exploitation requires knowledge of credentials of the targeted VMs and vCenter or ESX.	7.6	More Details

CVE-2025-59305	Improper authorization in the background migration endpoints of Langfuse 3.1 before d67b317 allows any authenticated user to invoke migration control functions. This can lead to data corruption or denial of service through unauthorized access to TRPC endpoints such as backgroundMigrations.all, backgroundMigrations.status, and backgroundMigrations.retry.	7.6	More Details
CVE-2025-59251	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	7.6	More Details
CVE-2025-55559	An issue was discovered TensorFlow v2.18.0. A Denial of Service (DoS) occurs when padding is set to 'valid' in tf.keras.layers.Conv2D.	7.5	More Details
CVE-2025-54591	FreshRSS is a free, self-hostable RSS aggregator. Versions 1.26.3 and below expose information about feeds and tags of default admin users, due to lack of access checking in the FreshRSS_Auth::hasAccess() function used by some of the tag/feed related endpoints. FreshRSS controllers usually have a defined firstAction() method with an override to make sure that every action requires access. If one doesn't, then every action has to check for access manually, and certain endpoints use neither the firstAction() method, or do they perform a manual access check. This issue is fixed in version 1.27.0.	7.5	More Details
CVE-2025-45376	Dell Repository Manager (DRM), versions 3.4.7 and 3.4.8, contains an Improper Handling of Insufficient Permissions or Privileges vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.5	More Details
CVE-2025-55558	A buffer overflow occurs in pytorch v2.7.0 when a PyTorch model consists of torch.nn.Conv2d, torch.nn.functional.hardshrink, and torch.Tensor.view-torch.mv() and is compiled by Inductor, leading to a Denial of Service (DoS).	7.5	More Details
CVE-2025-8014	Denial of Service issue in GraphQL endpoints in Gitlab EE/CE affecting all versions from 11.10 prior to 18.2.7, 18.3 prior to 18.3.3, and 18.4 prior to 18.4.1 allows unauthenticated users to potentially bypass query complexity limits leading to resource exhaustion and service disruption.	7.5	More Details
CVE-2025-55551	An issue in the component torch.linalg.lu of pytorch v2.8.0 allows attackers to cause a Denial of Service (DoS) when performing a slice operation.	7.5	More Details
CVE-2025-59833	Flag Forge is a Capture The Flag (CTF) platform. In versions from 2.1.0 to before 2.3.0, the API endpoint GET /api/problems/:id returns challenge hints in plaintext within the question object, regardless of whether the user has unlocked them via point deduction. Users can view all hints for free, undermining the business logic of the platform and reducing the integrity of the challenge system. This issue has been patched in version 2.3.0.	7.5	More Details
CVE-2025-11021	A flaw was found in the cookie date handling logic of the libsoup HTTP library, widely used by GNOME and other applications for web communication. When processing cookies with specially crafted expiration dates, the library may perform an out-of-bounds memory read. This flaw could result in unintended disclosure of memory contents, potentially exposing sensitive information from the process using libsoup.	7.5	More Details
CVE-2025-59942	go-f3 is a Golang implementation of Fast Finality for Filecoin (F3). In versions 0.8.6 and below, go-f3 panics when it validates a "poison" messages causing Filecoin nodes consuming F3 messages to become vulnerable. A "poison" message can can cause integer overflow in the signer index validation, which can cause the whole node to crash. These malicious messages aren't self-propagating since the bug is in the validator. An attacker needs to directly send the message to all targets. This issue is fixed in version 0.8.7.	7.5	More Details
CVE-2025-59404	Flock Safety Bravo Edge AI Compute Device BRAVO_00.00_local_20241017 ships with its bootloader unlocked. This permits bypass of Android Verified Boot (AVB) and allows direct modification of partitions.	7.5	More Details
CVE-2025-10880	All versions of Dingtian DT-R002 are vulnerable to an Insufficiently Protected Credentials vulnerability that could allow an attacker to extract the proprietary "Dingtian Binary" protocol password by sending an unauthenticated GET request.	7.5	More Details
CVE-2025-57319	fast-redact is a package that provides do very fast object redaction. A Prototype Pollution vulnerability in the nestedRestore function of fast-redact version 3.5.0 and before allows attackers to inject properties on Object.prototype via supplying a crafted payload, causing denial of service (DoS) as the minimum consequence. NOTE: the Supplier disputes this because the reporter only demonstrated access to properties by an internal utility function, and there is no means for achieving prototype pollution via the public API.	7.5	More Details

CVE-2024-48014	Dell BSAFE Micro Edition Suite, versions prior to 5.0.2.3 contain an Out-of-bounds Write vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to denial of service.	7.5	More Details
CVE-2025-10858	An issue was discovered in GitLab CE/EE affecting all versions before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1 that allows unauthenticated users to cause a Denial of Service (DoS) condition while uploading specifically crafted large JSON files.	7.5	More Details
CVE-2025-26278	A prototype pollution in the lib.set function of dref v0.1.2 allows attackers to cause a Denial of Service (DoS) via supplying a crafted payload.	7.5	More Details
CVE-2025-55557	A Name Error occurs in pytorch v2.7.0 when a PyTorch model consists of torch.cummin and is compiled by Inductor, leading to a Denial of Service (DoS).	7.5	More Details
CVE-2025-57317	apidoc-core is the core parser library to generate apidoc result following the apidoc-spec. A Prototype Pollution vulnerability in the preProcess function of apidoc-core versions thru 0.15.0 allows attackers to inject properties on Object.prototype via supplying a crafted payload, causing denial of service (DoS) as the minimum consequence.	7.5	More Details
CVE-2025-41252	Description: VMware NSX contains a username enumeration vulnerability. An unauthenticated malicious actor may exploit this to enumerate valid usernames, potentially leading to unauthorized access attempts. Impact: Username enumeration → facilitates unauthorized access. Attack Vector: Remote, unauthenticated. Severity: Important. CVSSv3: 7.5 (High). Acknowledgments: Reported by the National Security Agency. Affected Products: * VMware NSX 9.x.x.x, 4.2.x, 4.1.x, 4.0.x * NSX-T 3.x * VMware Cloud Foundation (with NSX) 5.x, 4.5.x Fixed Versions: * NSX 9.0.1.0; 4.2.2.2/4.2.3.1 http://4.2.2.2/4.2.3.1 ; 4.1.2.7; NSX-T 3.2.4.3; CCF async patch (KB88287). Workarounds: None.	7.5	More Details
CVE-2025-57632	libsmb2 6.2+ is vulnerable to Buffer Overflow. When processing SMB2 chained PDUs (NextCommand), libsmb2 repeatedly calls smb2_add_iovector() to append to a fixed-size iovec array without checking the upper bound of v->niov (SMB2_MAX_VECTORS=256). An attacker can craft responses with many chained PDUs to overflow v->niov and perform heap out-of-bounds writes, causing memory corruption, crashes, and potentially arbitrary code execution. The SMB2_OPLOCK_BREAK path bypasses message ID validation.	7.5	More Details
CVE-2025-51495	An integer overflow vulnerability exists in the WebSocket component of Mongoose 7.5 thru 7.17. By sending a specially crafted WebSocket request, an attacker can cause the application to crash. If downstream vendors integrate this component improperly, the issue may lead to a buffer overflow.	7.5	More Details
CVE-2025-55560	An issue in pytorch v2.7.0 can lead to a Denial of Service (DoS) when a PyTorch model consists of torch.Tensor.to_sparse() and torch.Tensor.to_dense() and is compiled by Inductor.	7.5	More Details
CVE-2025-57446	An issue in O-RAN Near Realtime RIC ric-plt-submgr in the J-Release environment, allows remote attackers to cause a denial of service (DoS) via a crafted request to the Subscription Manager API component.	7.5	More Details
CVE-2025-59011	Missing Authorization vulnerability in shinetheme Traveler allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Traveler: from n/a through n/a.	7.5	More Details
CVE-2025-59010	Insertion of Sensitive Information Into Sent Data vulnerability in Maciej Bis Permalink Manager Lite allows Retrieve Embedded Sensitive Data. This issue affects Permalink Manager Lite: from n/a through 2.5.1.3.	7.5	More Details
CVE-2025-48707	An issue was discovered in Stormshield Network Security (SNS) before 5.0.1. TPM authentication information could, in some HA use cases, be shared among administrators, which can cause secret sharing.	7.5	More Details
CVE-2025-55553	A syntax error in the component proxy_tensor.py of pytorch v2.7.0 allows attackers to cause a Denial of Service (DoS).	7.5	More Details
CVE-2025-59830	Rack is a modular Ruby web server interface. Prior to version 2.2.18, Rack::QueryParser enforces its params_limit only for parameters separated by &, while still splitting on both & and ;. As a result, attackers could use ; separators to bypass the parameter count limit and submit more parameters than intended. Applications or middleware that directly invoke Rack::QueryParser with its default configuration (no explicit delimiter) could be exposed to increased CPU and memory consumption. This can be abused as a limited denial-of-service vector. This issue has been patched in version 2.2.18.	7.5	More Details

CVE-2025-57318	A Prototype Pollution vulnerability in the toCsv function of csvjson versions thru 5.1.0 allows attackers to inject properties on Object.prototype via supplying a crafted payload, causing denial of service (DoS) as the minimum consequence.	7.5	More Details
CVE-2025-45994	An issue in Aranda PassRecovery v1.0 allows attackers to enumerate valid user accounts in Active Directory via sending a crafted POST request to /user/existdirectory/1.	7.5	More Details
CVE-2025-57330	The web3-core-subscriptions is a package designed to manages web3 subscriptions. A Prototype Pollution vulnerability in the attachToObject function of web3-core-subscriptions version 1.10.4 and before allows attackers to inject properties on Object.prototype via supplying a crafted payload, causing denial of service (DoS) as the minimum consequence.	7.5	More Details
CVE-2025-47318	Transient DOS while parsing the EPTM test control message to get the test pattern.	7.5	More Details
CVE-2025-47326	Transient DOS while handling command data during power control processing.	7.5	More Details
CVE-2025-47328	Transient DOS while processing power control requests with invalid antenna or stream values.	7.5	More Details
CVE-2025-11149	This affects all versions of the package node-static; all versions of the package @nubosoftware/node-static. The package fails to catch an exception when user input includes null bytes. This allows attackers to access http://host/%00 and crash the server.	7.5	More Details
CVE-2024-55017	Account Takeover in Corezoid 6.6.0 in the OAuth2 implementation via an open redirect in the redirect_uri parameter allows attackers to intercept authorization codes and gain unauthorized access to victim accounts.	7.5	More Details
CVE-2025-36274	IBM Aspera HTTP Gateway 2.0.0 through 2.3.1 stores sensitive information in clear text in easily obtainable files which can be read by an unauthenticated user.	7.5	More Details
CVE-2025-8877	The AffiliateWP plugin for WordPress is vulnerable to SQL Injection via the ajax_get_affiliate_id_from_login function in all versions up to, and including, 2.28.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2025-60150	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in wpshuffle Subscribe to Download allows PHP Local File Inclusion. This issue affects Subscribe to Download: from n/a through 2.0.9.	7.5	More Details
CVE-2025-48869	Horilla is a free and open source Human Resource Management System (HRMS). Unauthenticated users can access uploaded resume files in Horilla 1.3.0 by directly guessing or predicting file URLs. These files are stored in a publicly accessible directory, allowing attackers to retrieve sensitive candidate information without authentication. At time of publication there is no known patch.	7.5	More Details
CVE-2025-48392	A vulnerability in Apache IoTDB. This issue affects Apache IoTDB: from 1.3.3 through 1.3.4, from 2.0.1-beta through 2.0.4. Users are recommended to upgrade to version 2.0.5, which fixes the issue.	7.5	More Details
CVE-2025-24525	Keysight Ixia Vision has an issue with hardcoded cryptographic material which may allow an attacker to intercept or decrypt payloads sent to the device via API calls or user authentication if the end user does not replace the TLS certificate that shipped with the device. Remediation is available in Version 6.9.1, released on September 23, 2025.	7.5	More Details
CVE-2025-9230	Issue summary: An application trying to decrypt CMS messages encrypted using password based encryption can trigger an out-of-bounds read and write. Impact summary: This out-of-bounds read may trigger a crash which leads to Denial of Service for an application. The out-of-bounds write can cause a memory corruption which can have various consequences including a Denial of Service or Execution of attacker-supplied code. Although the consequences of a successful exploit of this vulnerability could be severe, the probability that the attacker would be able to perform it is low. Besides, password based (PWRI) encryption support in CMS messages is very rarely used. For that reason the issue was assessed as Moderate severity according to our Security Policy. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as the CMS implementation is outside the OpenSSL FIPS module boundary.	7.5	More Details

CVE-2025-60153	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in wpshuffle Subscribe To Unlock allows PHP Local File Inclusion. This issue affects Subscribe To Unlock: from n/a through 1.1.5.	7.5	More Details
CVE-2025-57328	toggle-array is a package designed to enables a property on the object at the specified index, while disabling the property on all other objects. A Prototype Pollution vulnerability in the enable and disable function of toggle-array v1.0.1 and before allows attackers to inject properties on Object.prototype via supplying a crafted payload, causing denial of service (DoS) as the minimum consequence.	7.5	More Details
CVE-2025-57323	mpregular is a package that provides a small program development framework based on RegularJS. A Prototype Pollution vulnerability in the mp.addEventHandler function of mpregular version 0.2.0 and before allows attackers to inject properties on Object.prototype via supplying a crafted payload, causing denial of service (DoS) as the minimum consequence.	7.5	More Details
CVE-2025-57349	The messageformat package, an implementation of the Unicode MessageFormat 2 specification for JavaScript, is vulnerable to prototype pollution due to improper handling of message key paths in versions prior to 2.3.0. The flaw arises when processing nested message keys containing special characters (e.g., __proto__), which can lead to unintended modification of the JavaScript Object prototype. This vulnerability may allow a remote attacker to inject properties into the global object prototype via specially crafted message input, potentially causing denial of service or other undefined behaviors in applications using the affected component.	7.5	More Details
CVE-2025-57326	A Prototype Pollution vulnerability in the byGroupAndType function of sassdoc-extras v2.5.1 and before allows attackers to inject properties on Object.prototype via supplying a crafted payload, causing denial of service (DoS) as the minimum consequence.	7.5	More Details
CVE-2025-57327	spmrc is a package that provides the rc manager for spm. A Prototype Pollution vulnerability in the set and config function of spmrc version 1.2.0 and before allows attackers to inject properties on Object.prototype via supplying a crafted payload, causing denial of service (DoS) as the minimum consequence.	7.5	More Details
CVE-2025-57329	web3-core-method is a package designed to creates the methods on the web3 modules. A Prototype Pollution vulnerability in the attachToObject function of web3-core-method version 1.10.4 and before allows attackers to inject properties on Object.prototype via supplying a crafted payload, causing denial of service (DoS) as the minimum consequence.	7.5	More Details
CVE-2025-57325	rollbar is a package designed to effortlessly track and debug errors in JavaScript applications. This package includes advanced error tracking features and an intuitive interface to help you identify and fix issues more quickly. A Prototype Pollution vulnerability in the utility.set function of rollbar v2.26.4 and before allows attackers to inject properties on Object.prototype via supplying a crafted payload, causing denial of service (DoS) as the minimum consequence.	7.5	More Details
CVE-2025-20311	A vulnerability in the handling of certain Ethernet frames in Cisco IOS XE Software for Catalyst 9000 Series Switches could allow an unauthenticated, adjacent attacker to cause an egress port to become blocked and drop all outbound traffic. This vulnerability is due to improper handling of crafted Ethernet frames. An attacker could exploit this vulnerability by sending crafted Ethernet frames through an affected switch. A successful exploit could allow the attacker to cause the egress port to which the crafted frame is forwarded to start dropping all frames, resulting in a denial of service (DoS) condition.	7.4	More Details
CVE-2025-11094	A security vulnerability has been detected in code-projects E-Commerce Website 1.0. This affects an unknown part of the file /pages/admin_product_details.php. Such manipulation of the argument prod_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-11061	A vulnerability was found in Campcodes Online Learning Management System 1.0. This affects an unknown part of the file /admin/edit_student.php. Performing manipulation of the argument cys results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-11032	A flaw has been found in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. This issue affects some unknown processing of the file /Profilers/PriProfile/COUNT3s6.php. Executing manipulation of the argument CPU can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed.	7.3	More Details
CVE-2025-11062	A vulnerability was determined in Campcodes Online Learning Management System 1.0. This vulnerability affects unknown code of the file /admin/save_student.php. Executing manipulation of the argument class_id can lead to sql injection. The attack may be performed from remote. The exploit has	7.3	More Details

	been publicly disclosed and may be utilized.		
CVE-2025-11135	A vulnerability was detected in pmTicket Project-Management-Software up to 2ef379da2075f4761a2c9029cf91d073474e7486. The affected element is the function loadLanguage of the file classes/class.database.php of the component Cookie Handler. Performing manipulation of the argument user_id results in deserialization. The attack can be initiated remotely. The exploit is now public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-11109	A vulnerability was identified in Campcodes Computer Sales and Inventory System 1.0. The affected element is an unknown function of the file /pages/us_edit.php?action=edit. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-11110	A security flaw has been discovered in Campcodes Online Learning Management System 1.0. The impacted element is an unknown function of the file /admin/school_year.php. The manipulation of the argument school_year results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-59408	Flock Safety Bravo Edge AI Compute Device BRAVO_00.00_local_20241017 ships with Secure Boot disabled. This allows an attacker to flash modified firmware with no cryptographic protections.	7.3	More Details
CVE-2025-11030	A vulnerability was detected in Tutorials-Website Employee Management System up to 611887d8f8375271ce8abc704507d46340837a60. Impacted is an unknown function of the file /admin/all-applied-leave.php of the component HTTP Request Handler. The manipulation results in improper authorization. The attack may be performed from remote. The exploit is now public and may be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed.	7.3	More Details
CVE-2025-35027	Multiple robotic products by Unitree sharing a common firmware, including the Go2, G1, H1, and B2 devices, contain a command injection vulnerability. By setting a malicious string when configuring the on-board WiFi via a BLE module of an affected robot, then triggering a restart of the WiFi service, an attacker can ultimately trigger commands to be run as root via the wpa_supplicant_restart.sh shell script. All Unitree models use firmware derived from the same codebase (MIT Cheetah), and the two major forks are the G1 (humanoid) and Go2 (quadruped) branches.	7.3	More Details
CVE-2025-11111	A weakness has been identified in Campcodes Advanced Online Voting Management System 1.0. This affects an unknown function of the file /admin/candidates_edit.php. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-11057	A vulnerability has been found in SourceCodester Pet Grooming Management Software 1.0. Affected by this issue is some unknown functionality of the file /admin/print_inv.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-11055	A vulnerability was detected in SourceCodester Online Hotel Reservation System 1.0. Affected is an unknown function of the file /admin/updateaddress.php. The manipulation of the argument address results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-10973	A flaw has been found in JackieDYH Resume-management-system up to fb6b857d852dd796e748ce30c606fe5e61c18273. Affected by this issue is some unknown functionality of the file /admin/show.php. This manipulation of the argument userid causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-59816	This vulnerability allows attackers to directly query the underlying database, potentially retrieving all data stored in the Billing Admin database, including user credentials. User passwords are stored in plaintext, significantly increasing the severity of this issue.	7.3	More Details
CVE-2025-11118	A vulnerability was identified in CodeAstro Student Grading System 1.0. This issue affects some unknown processing of the file /adminLogin.php. Such manipulation of the argument staffId leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-	A vulnerability was identified in Bjskzy Zhiyou ERP up to 11.0. Affected by this vulnerability is the function openForm of the component com.artery.richclient.RichClientService. Such manipulation of the argument contentString leads to xml external entity reference. The attack can be executed remotely.	7.3	More Details

11140	The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-11116	A vulnerability was found in code-projects Simple Scheduling System 1.0. This affects an unknown part of the file /add.home.php. The manipulation of the argument faculty results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used. Other parameters might be affected as well.	7.3	More Details
CVE-2025-11052	A security flaw has been discovered in kidaze CourseSelectionSystem 1.0/5.php. The impacted element is an unknown function of the file /Profilers/PriProfile/COUNT3s5.php. Performing manipulation of the argument csslc results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-11064	A security flaw has been discovered in Campcodes Online Learning Management System 1.0. Impacted is an unknown function of the file /admin/teachers.php. The manipulation of the argument department results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-11115	A vulnerability has been found in code-projects Simple Scheduling System 1.0. Affected by this issue is some unknown functionality of the file /addtime.php. The manipulation of the argument starttime/endtime leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-11053	A weakness has been identified in PHPGurukul Small CRM 4.0. This affects an unknown function of the file /forgot-password.php. Executing manipulation of the argument email can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-11033	A vulnerability has been found in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. Impacted is an unknown function of the file /Profilers/PriProfile/COUNT3s7.php. The manipulation of the argument cbe leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	7.3	More Details
CVE-2025-11063	A vulnerability was identified in Campcodes Online Learning Management System 1.0. This issue affects some unknown processing of the file /admin/edit_department.php. The manipulation of the argument d leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-11076	A vulnerability was found in Campcodes Online Learning Management System 1.0. This impacts an unknown function of the file /admin/edit_teacher.php. Performing manipulation of the argument department results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-55322	Binding to an unrestricted ip address in GitHub allows an unauthorized attacker to execute code over a network.	7.3	More Details
CVE-2025-11046	A security flaw has been discovered in Tencent WeKnora 0.1.0. This impacts the function testEmbeddingModel of the file /api/v1/initialization/embedding/test. The manipulation of the argument baseUrl results in server-side request forgery. The attack can be launched remotely. The exploit has been released to the public and may be exploited. It is advisable to upgrade the affected component. The vendor responds: "We have confirmed that the issue mentioned in the report does not exist in the latest releases".	7.3	More Details
CVE-2025-11045	A vulnerability was identified in WAYOS LQ_04, LQ_05, LQ_06, LQ_07 and LQ_09 22.03.17. This affects an unknown function of the file /usb_paswd.asp. The manipulation of the argument Name leads to command injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-11105	A flaw has been found in code-projects Simple Scheduling System 1.0. This affects an unknown part of the file /schedulingsystem/addsubject.php. This manipulation of the argument subcode causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	7.3	More Details
CVE-2025-11102	A weakness has been identified in Campcodes Online Learning Management System 1.0. Affected is an unknown function of the file /admin/edit_content.php. Executing manipulation of the argument Title can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-	A stored cross-site scripting (XSS) vulnerability exists in the MyCourts v3 application within the LTA number profile field. An attacker can insert arbitrary JavaScript into their profile, which executes in the browser of any user viewing it, including administrators. Due to the absence of the HttpOnly flag on the	7.3	More

2025-57424	browser of any user viewing it, including administrators. Due to the absence of the HttpOnly flag on the session cookie, this flaw could be exploited to capture session tokens and hijack user sessions, enabling elevated access.	7.3	Details
CVE-2025-11040	A vulnerability was detected in code-projects Hostel Management System 1.0. Affected by this issue is some unknown functionality of the file /justines/admin/mod_users/index.php?view=view. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-11039	A security vulnerability has been detected in Campcodes Computer Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/us_edit1.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-11106	A vulnerability has been found in code-projects Simple Scheduling System 1.0. This vulnerability affects unknown code of the file /schedulingsystem/addfaculty.php. Such manipulation of the argument falname leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-11107	A vulnerability was found in code-projects Simple Scheduling System 1.0. This issue affects some unknown processing of the file /schedulingsystem/addcourse.php. Performing manipulation of the argument corcode results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-11108	A vulnerability was determined in code-projects Simple Scheduling System 1.0. Impacted is an unknown function of the file /schedulingsystem/addroom.php. Executing manipulation of the argument room can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-11075	A vulnerability has been found in Campcodes Online Learning Management System 1.0. This affects an unknown function of the file /admin/de_activate.php. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-11074	A flaw has been found in code-projects Project Monitoring System 1.0. The impacted element is an unknown function of the file /login.php. This manipulation of the argument username/password causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-11077	A vulnerability was determined in Campcodes Online Learning Management System 1.0. Affected is an unknown function of the file /admin/add_content.php. Executing manipulation of the argument Title can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-11037	A security flaw has been discovered in code-projects E-Commerce Website 1.0. This impacts an unknown function of the file /pages/admin_index_search.php. Performing manipulation of the argument Search results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-11070	A vulnerability was identified in Projectworlds Online Shopping System 1.0. This affects an unknown part of the file /store/cart_add.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-11036	A vulnerability was identified in code-projects E-Commerce Website 1.0. This affects an unknown function of the file /pages/admin_account_update.php. Such manipulation of the argument user_id leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-10951	A vulnerability was identified in geyang ml-logger up to acf255bade5be6ad88d90735c8367b28cbe3a743. Affected by this vulnerability is the function log_handler of the file ml_logger/server.py. Such manipulation of the argument File leads to path traversal. It is possible to launch the attack remotely. The exploit is publicly available and might be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	7.3	More Details
CVE-2025-11101	A security flaw has been discovered in itsourcecode Open Source Job Portal 1.0. This impacts an unknown function of the file /jobportal/admin/company/index.php?view=edit. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-11066	A flaw has been found in code-projects Online Bidding System 1.0. This impacts an unknown function of the file /administrator/bidlist.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	7.3	More Details

CVE-2025-11089	A vulnerability was determined in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. This impacts an unknown function of the file /Profilers/PriProfile/COUNT3s4.php. Executing manipulation of the argument cbranch can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	7.3	More Details
CVE-2025-10967	A vulnerability was detected in MuFen-mker PHP-Usermm up to 37f2d24e51b04346dfc565b93fc2fc6b37bdaea9. This affects an unknown part of the file /chkuser.php. Performing manipulation of the argument Username results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-9816	The WP Statistics – The Most Popular Privacy-Friendly Analytics Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the User-Agent Header in all versions up to, and including, 14.5.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-48868	Horilla is a free and open source Human Resource Management System (HRMS). An authenticated Remote Code Execution (RCE) vulnerability exists in Horilla 1.3.0 due to the unsafe use of Python’s eval() function on a user-controlled query parameter in the project_bulk_archive view. This allows privileged users (e.g., administrators) to execute arbitrary system commands on the server. While having Django’s DEBUG=True makes exploitation visibly easier by returning command output in the HTTP response, this is not required. The vulnerability can still be exploited in DEBUG=False mode by using blind payloads such as a reverse shell, leading to full remote code execution. This issue has been patched in version 1.3.1.	7.2	More Details
CVE-2025-10747	The WP-DownloadManager plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the download-add.php file in all versions up to, and including, 1.68.11. 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-2025-60172	Cross-Site Request Forgery (CSRF) vulnerability in flytedesk Flytedesk Digital allows Stored XSS. This issue affects Flytedesk Digital: from n/a through 20181101.	7.1	More Details
CVE-2025-60171	Cross-Site Request Forgery (CSRF) vulnerability in yourplugins Conditional Cart Messages for WooCommerce – YourPlugins.com allows Stored XSS. This issue affects Conditional Cart Messages for WooCommerce – YourPlugins.com: from n/a through 1.2.10.	7.1	More Details
CVE-2025-4957	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Metagauss ProfileGrid allows Reflected XSS. This issue affects ProfileGrid : from n/a through 5.9.5.7.	7.1	More Details
CVE-2025-60164	Cross-Site Request Forgery (CSRF) vulnerability in NewsMAN NewsmanApp allows Stored XSS. This issue affects NewsmanApp: from n/a through 2.7.7.	7.1	More Details
CVE-2025-60173	Cross-Site Request Forgery (CSRF) vulnerability in Ashwani kumar GST for WooCommerce allows Stored XSS. This issue affects GST for WooCommerce: from n/a through 2.0.	7.1	More Details
CVE-2025-60169	Cross-Site Request Forgery (CSRF) vulnerability in W3S Cloud Technology W3SCloud Contact Form 7 to Zoho CRM allows Stored XSS. This issue affects W3SCloud Contact Form 7 to Zoho CRM: from n/a through 3.0.	7.1	More Details
CVE-2025-59012	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in shinetheme Traveler allows Reflected XSS. This issue affects Traveler: from n/a through n/a.	7.1	More Details
CVE-2025-58385	In DOXENSE WATCHDOC before 6.1.0.5094, private user puk codes can be disclosed for Active Directory registered users (there is hard-coded and predictable data).	7.1	More Details
CVE-2025-56815	Datart 1.0.0-rc.3 is vulnerable to Directory Traversal in the POST /viz/image interface, since the server directly uses MultipartFile.transferTo() to save the uploaded file to a path controllable by the user, and lacks strict verification of the file name.	7.1	More Details

CVE-2025-48107	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in undsgn Uncode allows Reflected XSS. This issue affects Uncode: from n/a through n/a.	7.1	More Details
CVE-2025-21482	Cryptographic issue while performing RSA PKCS padding decoding.	7.1	More Details
CVE-2025-60170	Cross-Site Request Forgery (CSRF) vulnerability in Taraprasad Swain HTACCESS IP Blocker allows Stored XSS. This issue affects HTACCESS IP Blocker: from n/a through 1.0.	7.1	More Details
CVE-2025-57692	PiranhaCMS 12.0 allows stored XSS in the Text content block of Standard and Standard Archive Pages via /manager/pages, enabling execution of arbitrary JavaScript in another user s browser.	6.8	More Details
CVE-2025-56463	Mercusys MW305R 3.30 and below is has a Transport Layer Security (TLS) certificate private key disclosure.	6.8	More Details
CVE-2025-61659	bash-git-prompt 2.6.1 through 2.7.1 insecurely uses the /tmp/git-index-private$$ file, which has a predictable name.	6.8	More Details
CVE-2025-59948	FreshRSS is a free, self-hostable RSS aggregator. Versions 1.26.3 and below do not sanitize certain event handler attributes in feed content, so by finding a page that renders feed entries without CSP, it is possible to execute an XSS payload. The Allow API access authentication setting needs to be enabled by the instance administrator beforehand for the attack to work as it relies on api/query.php. An account takeover is possible by sending a change password request via the XSS payload / setting UserJS for persistence / stealing the autofill password / displaying a phishing page with a spoofed URL using history.replaceState() If the victim is an administrator, the attacker can also perform administrative actions. This issue is fixed in version 1.27.0.	6.7	More Details
CVE-2025-43943	Dell Cloud Disaster Recovery, version(s) prior to 19.20, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary commands with root privileges.	6.7	More Details
CVE-2025-59950	FreshRSS is a free, self-hostable RSS aggregator. In versions 1.26.3 and below, due to a bypass of double clickjacking protection (confirmation dialog), it is possible to trick the admin into clicking the Promote button in another user's management page after the admin double clicks on a button inside an attacker-controlled website. A successful attack can allow the attacker to promote themselves to "admin" and log into other users' accounts; the attacker has to know the specific instance URL they're targeting. This issue is fixed in version 1.27.0.	6.7	More Details
CVE-2025-1862	An arbitrary file upload vulnerability exists in multiple WSO2 products due to improper validation of user-supplied filenames in the BPEL uploader SOAP service endpoint. A malicious actor with administrative privileges can upload arbitrary files to a user-controlled location on the server. By leveraging this vulnerability, an attacker can upload a specially crafted payload and achieve remote code execution (RCE), potentially compromising the server and its data.	6.7	More Details
CVE-2025-20314	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to an affected device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to improper validation of software packages. An attacker could exploit this vulnerability by placing a crafted file into a specific location on an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Because this vulnerability allows an attacker to bypass a major security feature of a device, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.	6.7	More Details
CVE-2025-20313	Multiple vulnerabilities in Cisco IOS XE Software of could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. These vulnerabilities are due path traversal and improper image integrity validation. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Because this allows the attacker to bypass a major security feature of the device, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. For more information about these vulnerabilities, see the Details ["#details"] section of this advisory. ERP	6.7	More Details
CVE-	Improper input validation in Retail Mode prior to version 5.59.4 allows self attackers to execute privileged		More

2025- 21056	Improper Input Validation in Retail Mode prior to version 3.59.4 allows self attackers to execute privileged commands on their own devices.	6.6	More Details
CVE-2025-60114	Improper Control of Generation of Code ('Code Injection') vulnerability in YayCommerce YayCurrency allows Code Injection. This issue affects YayCurrency: from n/a through 3.2.	6.6	More Details
CVE-2025-60040	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fkrauthan wp-mpdf allows Stored XSS. This issue affects wp-mpdf: from n/a through 3.9.1.	6.5	More Details
CVE-2025-60102	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Syam Mohan WPFront User Role Editor allows Stored XSS. This issue affects WPFront User Role Editor: from n/a through 4.2.3.	6.5	More Details
CVE-2025-59938	Wazuh is a free and open source platform used for threat prevention, detection, and response. In versions starting from 3.8.0 to before 4.11.0, wazuh-analysisd is vulnerable to a heap buffer overflow when parsing XML elements from Windows EventChannel messages. This issue has been patched in version 4.11.0.	6.5	More Details
CVE-2025-60105	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in metaphorcreations Ditty allows Stored XSS. This issue affects Ditty: from n/a through 3.1.58.	6.5	More Details
CVE-2025-60112	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Syed Balkhi aThemes Addons for Elementor allows Stored XSS. This issue affects aThemes Addons for Elementor: from n/a through 1.1.3.	6.5	More Details
CVE-2025-60099	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in awsm.in Embed Any Document allows Stored XSS. This issue affects Embed Any Document: from n/a through 2.7.7.	6.5	More Details
CVE-2025-60098	Missing Authorization vulnerability in Jeff Farthing Theme My Login allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Theme My Login: from n/a through 7.1.12.	6.5	More Details
CVE-2024-43192	IBM Storage TS4500 Library 1.11.0.0 and 2.11.0.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	6.5	More Details
CVE-2025-10307	The Backuply – Backup, Restore, Migrate and Clone plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete backup functionality in all versions up to, and including, 1.4.8. 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-2025-54831	Apache Airflow 3 introduced a change to the handling of sensitive information in Connections. The intent was to restrict access to sensitive connection fields to Connection Editing Users, effectively applying a "write-only" model for sensitive values. In Airflow 3.0.3, this model was unintentionally violated: sensitive connection information could be viewed by users with READ permissions through both the API and the UI. This behavior also bypassed the `AIRFLOW__CORE__HIDE_SENSITIVE_VAR_CONN_FIELDS` configuration option. This issue does not affect Airflow 2.x, where exposing sensitive information to connection editors was the intended and documented behavior. Users of Airflow 3.0.3 are advised to upgrade Airflow to >=3.0.4.	6.5	More Details
CVE-2025-58917	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nick Verwymeren Quantities and Units for WooCommerce allows Stored XSS. This issue affects Quantities and Units for WooCommerce: from n/a through 1.0.13.	6.5	More Details
CVE-2025-48326	Missing Authorization vulnerability in Acclectic Media Acclectic Media Organizer allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Acclectic Media Organizer: from n/a through 1.4.	6.5	More Details
CVE-2025-27006	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themeplugs Authorsy allows Stored XSS. This issue affects Authorsy: from n/a through 1.0.5.	6.5	More Details
CVE-2025-60138	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sonalsinha21 SKT Blocks allows Stored XSS. This issue affects SKT Blocks: from n/a through 2.5.	6.5	More Details

CVE-2025-60142	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DaganLev Simple Meta Tags allows DOM-Based XSS. This issue affects Simple Meta Tags: from n/a through 1.5.	6.5	More Details
CVE-2025-60147	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HT Plugins HT Feed allows Stored XSS. This issue affects HT Feed: from n/a through 1.3.0.	6.5	More Details
CVE-2025-9958	An issue has been discovered in GitLab CE/EE affecting all versions from 14.10 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1, that could have allowed Guest users to access sensitive information stored in virtual registry configurations.	6.5	More Details
CVE-2025-7691	A privilege escalation issue has been discovered in GitLab EE affecting all versions from 16.6 prior to 18.2.7, 18.3 prior to 18.3.3, and 18.4 prior to 18.4.1 that could have allowed a developer with specific group management permissions to escalate their privileges and obtain unauthorized access to additional system capabilities.	6.5	More Details
CVE-2025-60163	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Robin W bbp topic count allows DOM-Based XSS. This issue affects bbp topic count: from n/a through 3.1.	6.5	More Details
CVE-2025-60157	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in emarket-design WP Ticket Customer Service Software & Support Ticket System allows Stored XSS. This issue affects WP Ticket Customer Service Software & Support Ticket System: from n/a through 6.0.2.	6.5	More Details
CVE-2025-60162	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PickPlugins Job Board Manager allows DOM-Based XSS. This issue affects Job Board Manager: from n/a through 2.1.61.	6.5	More Details
CVE-2025-60124	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ryan Hellyer Simple Colorbox allows Stored XSS. This issue affects Simple Colorbox: from n/a through 1.6.1.	6.5	More Details
CVE-2025-55556	TensorFlow v2.18.0 was discovered to output random results when compiling Embedding, leading to unexpected behavior in the application.	6.5	More Details
CVE-2025-29155	An issue in petstore v.1.0.7 allows a remote attacker to execute arbitrary code via the DELETE endpoint	6.5	More Details
CVE-2025-57320	json-schema-editor-visual is a package that provides jsonschema editor. A Prototype Pollution vulnerability in the setData and deleteData function of json-schema-editor-visual versions thru 1.1.1 allows attackers to inject or delete properties on Object.prototype via supplying a crafted payload, causing denial of service (DoS) as the minimum consequence.	6.5	More Details
CVE-2025-8559	The All in One Music Player plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.3.1 via the 'theme' parameter. This makes it possible for authenticated attackers, with Contributor-level access and above, to read the contents of files on the server, which can contain sensitive information.	6.5	More Details
CVE-2025-59956	AgentAPI is an HTTP API for Claude Code, Goose, Aider, Gemini, Amp, and Codex. Versions 0.3.3 and below are susceptible to a client-side DNS rebinding attack when hosted over plain HTTP on localhost. An attacker can gain access to the /messages endpoint served by the Agent API. This allows for the unauthorized exfiltration of sensitive user data, specifically local message history, which can include secret keys, file system contents, and intellectual property the user was working on locally. This issue is fixed in version 0.4.0.	6.5	More Details
CVE-2025-57354	A vulnerability exists in the 'counterpart' library for Node.js and the browser due to insufficient sanitization of user-controlled input in translation key processing. The affected versions prior to 0.18.6 allow attackers to manipulate the library's translation functionality by supplying maliciously crafted keys containing prototype chain elements (e.g., __proto__), leading to prototype pollution. This weakness enables adversaries to inject arbitrary properties into the JavaScript Object prototype through the first parameter of the translate method when combined with specific separator configurations, potentially resulting in denial-of-service conditions or remote code execution in vulnerable applications. The issue arises from the library's failure to properly validate or neutralize special characters in translation key inputs before processing.	6.5	More Details
CVE-2025-56769	An issue was discovered in chinabugotech hutool before 5.8.4 allowing attackers to execute arbitrary expressions that lead to arbitrary method invocation and potentially remote code execution (RCE) via the QLExpressEngine class.	6.5	More Details

CVE-2025-10540	iMonitor EAM 9.6394 transmits communication between the EAM client agent and the EAM server, as well as between the EAM monitor management software and the server, in plaintext without authentication or encryption. An attacker with network access can intercept sensitive information (such as credentials, keylogger data, and personally identifiable information) and tamper with traffic. This allows both unauthorized disclosure and modification of data, including issuing arbitrary commands to client agents.	6.5	More Details
CVE-2025-20149	A vulnerability in the CLI of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to a buffer overflow. An attacker with a low-privileged account could exploit this vulnerability by using crafted commands at the CLI prompt. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	6.5	More Details
CVE-2025-57348	The node-cube package (prior to version 5.0.0) contains a vulnerability in its handling of prototype chain initialization, which could allow an attacker to inject properties into the prototype of built-in objects. This issue, categorized under CWE-1321, arises from improper validation of user-supplied input in the package's resource initialization process. Successful exploitation may lead to denial of service or arbitrary code execution in affected environments. The vulnerability affects versions up to and including 5.0.0-beta.19, and no official fix has been released to date.	6.5	More Details
CVE-2025-29157	An issue in petstore v.1.0.7 allows a remote attacker to execute arbitrary code via accessing a non-existent endpoint/cart, the server returns a 404-error page exposing sensitive information including the Servlet name (default) and server version	6.5	More Details
CVE-2025-57351	A prototype pollution vulnerability exists in the ts-fns package versions prior to 13.0.7, where insufficient validation of user-provided keys in the assign function allows attackers to manipulate the Object.prototype chain. By leveraging this flaw, adversaries may inject arbitrary properties into the global object's prototype, potentially leading to application crashes, unexpected code execution behaviors, or bypasses of security-critical validation logic dependent on prototype integrity. The vulnerability stems from improper handling of deep property assignment operations within the library's public API functions. This issue remains unaddressed in the latest available version.	6.5	More Details
CVE-2025-52043	In Frappe ERPNext v15.57.5, the function import_coa() at erpnext/accounts/doctype/chart_of_accounts_importer/chart_of_accounts_importer.py is vulnerable to SQL injection, which allows an attacker to extract all information from databases by injecting a SQL query into the company parameter.	6.5	More Details
CVE-2025-52047	In Frappe ErpNext v15.57.5, the function get_income_account() at erpnext/controllers/queries.py is vulnerable to SQL Injection, which allows an attacker to extract all information from databases by injecting a SQL query into the filters.disabled parameter.	6.5	More Details
CVE-2025-57324	parse is a package designed to parse JavaScript SDK. A Prototype Pollution vulnerability in the SingleInstanceStateController.initializeState function of parse version 5.3.0 and before allows attackers to inject properties on Object.prototype via supplying a crafted payload, causing denial of service (DoS) as the minimum consequence.	6.5	More Details
CVE-2025-52049	In Frappe ErpNext v15.57.5, the function get_timesheet_detail_rate() at erpnext/projects/doctype/timesheet/timesheet.py is vulnerable to SQL Injection, which allows an attacker to extract all information from databases by injecting SQL query into the timelog parameter.	6.5	More Details
CVE-2025-52050	In Frappe ERPNext 15.57.5, the function get_loyalty_program_details_with_points() at erpnext/accounts/doctype/loyalty_program/loyalty_program.py is vulnerable to SQL Injection, which allows an attacker to extract all information from databases by injecting a SQL query into the expiry_date parameter.	6.5	More Details
CVE-2025-59940	mkdocs-include-markdown-plugin is an Mkdocs Markdown includer plugin. In versions 7.1.7 and below, there is a vulnerability where unvalidated input can collide with substitution placeholders. This issue is fixed in version 7.1.8.	6.5	More Details
CVE-2025-9231	Issue summary: A timing side-channel which could potentially allow remote recovery of the private key exists in the SM2 algorithm implementation on 64 bit ARM platforms. Impact summary: A timing side-channel in SM2 signature computations on 64 bit ARM platforms could allow recovering the private key by an attacker.. While remote key recovery over a network was not attempted by the reporter, timing measurements revealed a timing signal which may allow such an attack. OpenSSL does not directly support certificates with SM2 keys in TLS, and so this CVE is not relevant in most TLS contexts. However, given that it is possible to add support for such certificates via a custom provider, coupled with the fact that in such a custom provider context the private key may be recoverable via remote timing measurements, we consider this to be a Moderate severity issue. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as SM2 is not an approved algorithm.	6.5	More Details

CVE-2025-55191	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Versions between 2.1.0 and 2.14.19, 3.2.0-rc1, 3.1.0-rc1 through 3.1.7, and 3.0.0-rc1 through 3.0.18 contain a race condition in the repository credentials handler that can cause the Argo CD server to panic and crash when concurrent operations are performed on the same repository URL. The vulnerability is located in numerous repository related handlers in the util/db/repository_secrets.go file. A valid API token with repositories resource permissions (create, update, or delete actions) is required to trigger the race condition. This vulnerability causes the entire Argo CD server to crash and become unavailable. Attackers can repeatedly and continuously trigger the race condition to maintain a denial-of-service state, disrupting all GitOps operations. This issue is fixed in versions 2.14.20, 3.2.0-rc2, 3.1.8 and 3.0.19.	6.5	More Details
CVE-2025-20362	A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to access restricted URL endpoints that are related to remote access VPN that should otherwise be inaccessible without authentication. This vulnerability is due to improper validation of user-supplied input in HTTP(S) requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted web server on a device. A successful exploit could allow the attacker to access a restricted URL without authentication.	6.5	More Details
CVE-2025-10189	The BP Direct Menus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'bpdm_login' shortcode in all versions up to, and including, 1.0.0 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-2025-10191	The Big Post Shipping for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wooboigpost_shipping_status' shortcode in all versions up to, and including, 2.1.1 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-2025-10182	The dbview plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'dbview' shortcode in all versions up to, and including, 0.5.5 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-2025-10179	The My AskAI plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'myaskai' shortcode in all versions up to, and including, 1.0.0 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-2025-61792	Quadient DS-700 iQ devices through 2025-09-30 might have a race condition during the quick clicking of (in order) the Question Mark button, the Help Button, the About button, and the Help Button, leading to a transition out of kiosk mode into local administrative access. NOTE: the reporter indicates that the "behavior was observed sporadically" during "limited time on the client site," making it not "possible to gain more information about the specific kiosk mode crashing issue," and the only conclusion was "there appears to be some form of race condition." Accordingly, there can be doubt that a reproducible cybersecurity vulnerability was identified; sporadic software crashes can also be caused by a hardware fault on a single device (for example, transient RAM errors). The reporter also describes a variety of other issues, including initial access via USB because of the absence of a "lock-pick resistant locking solution for the External Controller PC cabinet," which is not a cybersecurity vulnerability (section 4.1.5 of the CNA Operational Rules). Finally, it is unclear whether the device or OS configuration was inappropriate, given that the risks are typically limited to insider threats within the mail operations room of a large company.	6.4	More Details
CVE-2025-10168	The Any News Ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'any-ticker' shortcode in all versions up to, and including, 3.1.1 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-2025-10131	The All Social Share Options plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'sc' 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-	The Layers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'webcam' shortcode in all versions up to, and including, 0.5 due to insufficient input sanitization and output		

CVE-2025-10130	shortcode in all versions up to, and including, 6.5 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-2025-10196	The Survey Anyplace plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'surveyanyplace_embed' shortcode in all versions up to, and including, 1.0.0 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-2025-10128	The Eulerpool Research Systems plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'aaq' shortcode in all versions up to, and including, 4.0.1 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-2025-10000	The Qyrr – simply and modern QR-Code creation plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the blob_to_file() function in all versions up to, and including, 2.0.7. 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.	6.4	More Details
CVE-2025-8440	The Team Members plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the first and last name fields in all versions up to, and including, 5.3.5 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-2025-36352	IBM License Metric Tool 9.2.0 through 9.2.40 is vulnerable to stored 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.	6.4	More Details
CVE-2025-10136	The TweetThis Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'tweetthis' shortcode in all versions up to, and including, 1.8.0 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-2025-8608	The Mihdan: Elementor Yandex Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's block attributes in all versions up to, and including, 1.6.11 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-2025-9353	The Themify Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several parameters in all versions up to, and including, 7.6.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The vulnerability was partially patched in version 7.6.9.	6.4	More Details
CVE-2025-9852	The Yoga Schedule Momoyoga plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'momoyoga-schedule' shortcode in all versions up to, and including, 2.9.0 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-2025-8777	The planetcalc plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘language’ parameter in all versions up to, and including, 2.2 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-2025-8624	The Nexa Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Google Maps widget in all versions up to, and including, 1.1.0 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-2025-8623	The WeedMaps Menu for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's weedmaps_menu shortcode in all versions up to, and including, 1.2.0 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	6.4	More Details

	that will execute whenever a user accesses an injected page.		
CVE-2025-60249	vulnerability-lookup 2.16.0 allows XSS in bundle.py, comment.py, and user.py, by a user on a vulnerability-lookup instance who can add bundles, comments, or sightings. A cross-site scripting (XSS) vulnerability was discovered in the handling of user-supplied input in the Bundles, Comments, and Sightings components. Untrusted data was not properly sanitized before being rendered in templates and tables, which could allow attackers to inject arbitrary JavaScript into the application. The issue was due to unsafe use of innerHTML and insufficient validation of dynamic URLs and model fields. This vulnerability has been fixed by escaping untrusted data, replacing innerHTML assignments with safer DOM methods, encoding URLs with encodeURIComponent, and improving input validation in the affected models.	6.4	More Details
CVE-2025-8566	The GutenBee – Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via parameters in the CountUp and Google Maps Blocks in all versions up to, and including, 2.18.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-10178	The CM Business Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'cmbd_featured_image' shortcode in all versions up to, and including, 1.5.2 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-2025-8560	The FancyTabs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘title’ parameter in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9044	The Mapster WP Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple fields in versions up to, and including, 1.20.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor-level permissions and above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8214	The The Pack Elementor addon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Typing Letter widget in all versions up to, and including, 2.1.5 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-2025-6941	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter of the 'latepoint_resources' shortcode in all versions up to, and including, 5.1.94 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-2025-8906	The Widgets for Tiktok Feed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'trustindex-feed' shortcode in all versions up to, and including, 1.7.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-9490	The Popup Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘title’ parameter in all versions up to, and including, 1.20.6 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-2025-8200	The Mega Elements – Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown Timer widget in all versions up to, and including, 1.3.2 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-2025-10180	The Markdown Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'markdown' shortcode in all versions up to, and including, 0.2.1 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-	nncp before 8.12.0 allows path traversal (for reading or writing) during freqing and file saving via a	6.4	More

60020	crafted path in packet data.		Details
CVE-2025-11038	A weakness has been identified in itsourcecode Online Clinic Management System 1.0. Affected is an unknown function of the file /details.php?action=post. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-11048	A security vulnerability has been detected in Portabilis i-Educar up to 2.10. Affected by this vulnerability is an unknown functionality of the file /consulta-dispensas. Such manipulation leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-11047	A weakness has been identified in Portabilis i-Educar up to 2.10. Affected is an unknown function of the file /module/Api/aluno. This manipulation of the argument aluno_id causes improper authorization. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-11035	A vulnerability was determined in Jinher OA 2.0. The impacted element is an unknown function of the file /c6/Jhsoft.Web.module/ToolBar/ManageWord.aspx/?text=GetUrl&style=1. This manipulation causes xml external entity reference. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-11041	A vulnerability has been found in itsourcecode Open Source Job Portal 1.0. Affected by this issue is some unknown functionality of the file /admin/user/index.php?view=edit. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-11097	A vulnerability has been found in D-Link DIR-823X 250416. Impacted is an unknown function of the file /goform/set_device_name. The manipulation of the argument mac leads to command injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-11098	A vulnerability was found in D-Link DIR-823X 250416. The affected element is an unknown function of the file /goform/set_wifi_blacklists. The manipulation of the argument macList results in command injection. The attack may be performed from remote. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-11121	A security vulnerability has been detected in Tenda AC18 15.03.05.19. The impacted element is an unknown function of the file /goform/AdvSetLanip. The manipulation of the argument lanIp leads to command injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-10962	A vulnerability was identified in Wavlink NU516U1 M16U1_V240425. This impacts the function sub_403198 of the file /cgi-bin/wireless.cgi of the component SetName Page. The manipulation of the argument mac_5g leads to command injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-10989	A security flaw has been discovered in yangzongzhuan RuoYi up to 4.8.1. This vulnerability affects unknown code of the file /system/role/authUser/selectAll. Performing manipulation of the argument userIds results in improper authorization. The attack can be initiated remotely. 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.	6.3	More Details
CVE-2025-10959	A vulnerability has been found in Wavlink NU516U1 M16U1_V240425. The affected element is the function sub_401778 of the file /cgi-bin/firewall.cgi. Such manipulation of the argument dmz_flag leads to command injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-10988	A vulnerability was identified in YunaiV ruoyi-vue-pro up to 2025.09. This affects an unknown part of the file /crm/business/transfer. Such manipulation leads to improper authorization. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-10960	A vulnerability was found in Wavlink NU516U1 M16U1_V240425. The impacted element is the function sub_402D1C of the file /cgi-bin/wireless.cgi of the component DeleteMac Page. Performing manipulation of the argument delete_list results in command injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-	A flaw has been found in CodeAstro Online Leave Application 1.0. Affected by this vulnerability is an unknown functionality of the file /leaveAplicationForm.php. Executing manipulation of the argument		More

2025-11114	absence[] can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	6.3	Details
CVE-2025-11054	A security vulnerability has been detected in itsourcecode Open Source Job Portal 1.0. This impacts an unknown function of the file /jobportal/admin/category/index.php?view=edit. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-10963	A security flaw has been discovered in Wavlink NU516U1 M16U1_V240425. Affected is the function sub_4016F0 of the file /cgi-bin/firewall.cgi. The manipulation of the argument del_flag results in command injection. It is possible to launch the attack remotely. 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.	6.3	More Details
CVE-2025-10974	A vulnerability has been found in giantspatula SewKinect up to 7fd963ceb3385af3706af02b8a128a13399dffb1. This affects the function pickle.loads of the file /calculate of the component Endpoint. Such manipulation of the argument body_parts/point_cloud leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases.	6.3	More Details
CVE-2025-11056	A flaw has been found in ProjectsAndPrograms School Management System 1.0. Affected by this vulnerability is an unknown functionality of the file owner_panel/fetch-data/select-students.php. This manipulation of the argument select causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	6.3	More Details
CVE-2025-10987	A vulnerability was determined in YunaiV yudao-cloud up to 2025.09. Affected by this issue is some unknown functionality of the file /crm/contact/transfer of the component HTTP Request Handler. This manipulation of the argument contactId causes improper authorization. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-11104	A vulnerability was detected in CodeAstro Electricity Billing System 1.0. Affected by this issue is some unknown functionality of the file /admin/bill.php. The manipulation of the argument uid results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2025-10975	A vulnerability was found in GuanxingLu vlarl up to 31abc0baf53ef8f5db666a1c882e1ea64def2997. This vulnerability affects the function experiments.robot.bridge.reasoning_server::run_reasoning_server of the file experiments/robot/bridge/reasoning_server.py of the component ZeroMQ. Performing manipulation of the argument Message results in deserialization. Remote exploitation of the attack is possible. The exploit has been made public and could be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided.	6.3	More Details
CVE-2025-10964	A weakness has been identified in Wavlink NU516U1. Affected by this vulnerability is the function sub_401B30 of the file /cgi-bin/firewall.cgi. This manipulation of the argument remoteManagementEnabled causes command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-10965	A security vulnerability has been detected in LazyAGI LazyLLM up to 0.6.1. Affected by this issue is the function lazyllm_call of the file lazyllm/components/deploy/relay/server.py. Such manipulation leads to deserialization. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-10958	A flaw has been found in Wavlink NU516U1 M16U1_V240425. Impacted is the function sub_403010 of the file /cgi-bin/wireless.cgi of the component AddMac Page. This manipulation of the argument macAddr causes command injection. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-11113	A vulnerability was detected in CodeAstro Online Leave Application 1.0. Affected is an unknown function of the file /signup.php. Performing manipulation of the argument city results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used. Other parameters might be affected as well.	6.3	More Details
CVE-2025-43400	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Sonoma 14.8.1, macOS Tahoe 26.0.1, macOS Sequoia 15.7.1, visionOS 26.0.1, iOS 26.0.1 and iPadOS 26.0.1, iOS 18.7.1 and iPadOS 18.7.1. Processing a maliciously crafted font may lead to unexpected app termination or corrupt process memory.	6.3	More Details
CVE-	A flaw has been found in Portabilis i-Educar up to 2.10. This affects an unknown part of the file /periodo-		More

2025- 11050	lancamento. Executing manipulation can lead to improper authorization. The attack can be executed remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-11138	A vulnerability was found in mirweiye wenkucms up to 3.4. This impacts the function createPathOne of the file app/common/common.php. The manipulation results in os command injection. The attack may be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2025-11139	A vulnerability was determined in Bjskzy Zhiyou ERP up to 11.0. Affected is the function uploadStudioFile of the component com.artery.form.services.FormStudioUpdater. This manipulation of the argument filepath causes path traversal. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-11088	A weakness has been identified in itsourcecode Open Source Job Portal 1.0. Impacted is an unknown function of the file /admin/vacancy/index.php?view=edit. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-11100	A vulnerability was identified in D-Link DIR-823X 250416. This affects the function uci_set of the file /goform/set_wifi_blacklists. Such manipulation leads to command injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-11090	A vulnerability was identified in itsourcecode Open Source Job Portal 1.0. Affected is an unknown function of the file /admin/employee/index.php?view=edit. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-11092	A weakness has been identified in D-Link DIR-823X 250416. Affected by this issue is the function sub_412E7C of the file /goform/set_switch_settings. This manipulation of the argument port causes command injection. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-10950	A vulnerability was determined in geyang ml-logger up to acf255bade5be6ad88d90735c8367b28cbe3a743. Affected is the function log_handler of the file ml_logger/server.py of the component Ping Handler. This manipulation of the argument data causes deserialization. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	6.3	More Details
CVE-2025-11096	A flaw has been found in D-Link DIR-823X 250416. This issue affects some unknown processing of the file /goform/diag_traceroute. Executing manipulation of the argument target_addr can lead to command injection. The attack can be executed remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-11078	A vulnerability was identified in itsourcecode Open Source Job Portal 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/user/controller.php?action=photos. The manipulation of the argument photo leads to unrestricted upload. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-11099	A vulnerability was determined in D-Link DIR-823X 250416. The impacted element is the function uci_del of the file /goform/delete_prohibiting. This manipulation of the argument delvalue causes command injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2025-11095	A vulnerability was detected in D-Link DIR-823X 250416. This vulnerability affects unknown code of the file /goform/delete_offline_device. Performing manipulation of the argument delvalue results in command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	6.3	More Details
CVE-2025-11049	A vulnerability was detected in Portabilis i-Educar up to 2.10. Affected by this issue is some unknown functionality of the file /unificacao-aluno. Performing manipulation results in improper authorization. Remote exploitation of the attack is possible. The exploit is now public and may be used.	6.3	More Details
CVE-2025-56200	A URL validation bypass vulnerability exists in validator.js through version 13.15.15. The isURL() function uses '://' as a delimiter to parse protocols, while browsers use ':' as the delimiter. This parsing difference allows attackers to bypass protocol and domain validation by crafting URLs leading to XSS and Open Redirect attacks.	6.1	More Details
CVE-2025-9946	The LockerPress – WordPress Security Plugin 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 a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details

CVE-2025-56018	SourceCodester Web-based Pharmacy Product Management System V1.0 is vulnerable to Cross Site Scripting (XSS) in Category Management via the category name field.	6.1	More Details
CVE-2025-6396	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Webbeyaz Website Design Website Software allows Cross-Site Scripting (XSS).This issue affects Website Software: through 2025.07.14.	6.1	More Details
CVE-2025-57292	Todoist v8484 contains a stored cross-site scripting (XSS) vulnerability in the avatar upload functionality. The application fails to properly validate the MIME type and sanitize image metadata.	6.1	More Details
CVE-2025-57872	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 11.4 and below that may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks.	6.1	More Details
CVE-2025-27036	Information disclosure when Video engine escape input data is less than expected minimum size.	6.1	More Details
CVE-2025-26258	Sourcecodester Employee Management System v1.0 is vulnerable to Cross Site Scripting (XSS) via 'Add Designation.'	6.1	More Details
CVE-2024-5200	The Postie WordPress plugin before 1.9.71 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	6.1	More Details
CVE-2025-36239	IBM Storage TS4500 Library 1.11.0.0 and 2.11.0.0 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.1	More Details
CVE-2025-59525	Horilla is a free and open source Human Resource Management System (HRMS). Prior to version 1.4.0, improper sanitization across the application allows XSS via uploaded SVG (and via allowed <embed>), which can be chained to execute JavaScript whenever users view impacted content (e.g., announcements). This can result in admin account takeover. This issue has been patched in version 1.4.0.	6.1	More Details
CVE-2025-56807	A cross-site scripting (XSS) vulnerability in FairSketch RISE Ultimate Project Manager & CRM 3.9.4 allows an administrator to store a JavaScript payload using the file explorer in the admin dashboard when creating new folders.	6.1	More Details
CVE-2025-56795	Mealie 3.0.1 and earlier is vulnerable to Stored Cross-Site Scripting (XSS) in the recipe creation functionality. Unsanitized user input in the "note" and "text" fields of the "/api/recipes/{recipe_name}" endpoint is rendered in the frontend without proper escaping leading to persistent XSS.	6.1	More Details
CVE-2025-27030	information disclosure while invoking calibration data from user space to update firmware size.	6.1	More Details
CVE-2025-59524	Horilla is a free and open source Human Resource Management System (HRMS). Prior to version 1.4.0, the file upload flow performs validation only in the browser and does not enforce server-side checks. An attacker can bypass the client-side validation (for example, with an intercepting proxy or by submitting a crafted request) to store an executable HTML document on the server. When an administrator or other privileged user views the uploaded file, the embedded script runs in their context and sends session cookies (or other credentials) to an attacker-controlled endpoint. The attacker then reuses those credentials to impersonate the admin. This issue has been patched in version 1.4.0.	6.1	More Details
CVE-2025-57879	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 11.4 and below that may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks.	6.1	More Details
CVE-2025-29156	Cross Site Scripting vulnerability in petstore v.1.0.7 allows a remote attacker to execute arbitrary code via a crafted script to the /api/v3/pet	6.1	More Details
CVE-2025-9899	The Trust Reviews plugin for Google, Tripadvisor, Yelp, Airbnb and other platforms 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 feed_save function. This makes it possible for unauthenticated attackers to create or modify feed entries via a forged request granted they can trick a site administrator	6.1	More Details

[illegible]	into performing an action such as clicking on a link.		
CVE-2025-27033	Information disclosure while running video usecase having rogue firmware.	6.1	More Details
CVE-2025-20240	A vulnerability in the Web Authentication feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting attack (XSS) on an affected device. This vulnerability is due to improper sanitization of user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to execute a reflected XSS attack and steal user cookies from the affected device.	6.1	More Details
CVE-2025-57878	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 11.4 and below that may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks.	6.1	More Details
CVE-2025-20338	A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with administrative privileges to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by logging in to the device CLI with valid administrative (level 15) credentials and using crafted commands at the CLI prompt. A successful exploit could allow the attacker to execute arbitrary commands as root.	6.0	More Details
CVE-2025-57197	In the Payeer Android application 2.5.0, an improper access control vulnerability exists in the authentication flow for the PIN change feature. A local attacker with root access to the device can dynamically instrument the app to bypass the current PIN verification check and directly modify the authentication PIN. This allows unauthorized users to change PIN without knowing the original/current PIN.	6.0	More Details
CVE-2025-59941	go-f3 is a Golang implementation of Fast Finality for Filecoin (F3). In versions 0.8.8 and below, go-f3's justification verification caching mechanism has a vulnerability where verification results are cached without properly considering the context of the message. An attacker can bypass justification verification by submitting a valid message with a correct justification and then reusing the same cached justification in contexts where it would normally be invalid. This occurs because the cached verification does not properly validate the relationship between the justification and the specific message context it's being used with. This issue is fixed in version 0.8.9.	5.9	More Details
CVE-2025-9232	Issue summary: An application using the OpenSSL HTTP client API functions may trigger an out-of-bounds read if the 'no_proxy' environment variable is set and the host portion of the authority component of the HTTP URL is an IPv6 address. Impact summary: An out-of-bounds read can trigger a crash which leads to Denial of Service for an application. The OpenSSL HTTP client API functions can be used directly by applications but they are also used by the OCSP client functions and CMP (Certificate Management Protocol) client implementation in OpenSSL. However the URLs used by these implementations are unlikely to be controlled by an attacker. In this vulnerable code the out of bounds read can only trigger a crash. Furthermore the vulnerability requires an attacker-controlled URL to be passed from an application to the OpenSSL function and the user has to have a 'no_proxy' environment variable set. For the aforementioned reasons the issue was assessed as Low severity. The vulnerable code was introduced in the following patch releases: 3.0.16, 3.1.8, 3.2.4, 3.3.3, 3.4.0 and 3.5.0. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as the HTTP client implementation is outside the OpenSSL FIPS module boundary.	5.9	More Details
CVE-2025-7698	Out-of-bounds read vulnerabilities in print processing of Generic Plus PCL6 Printer Driver / Generic Plus UFR II Printer Driver / Generic Plus LIPS4 Printer Driver / Generic Plus LIPSLX Printer Driver / Generic Plus PS Printer Driver	5.9	More Details
CVE-2025-60177	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rozx Recaptcha – wp allows Stored XSS. This issue affects Recaptcha – wp: from n/a through 0.2.6.	5.9	More Details
CVE-2025-9903	Out-of-bounds write vulnerabilities in print processing of Generic Plus PCL6 Printer Driver / Generic Plus UFR II Printer Driver / Generic Plus LIPS4 Printer Driver / Generic Plus LIPSLX Printer Driver / Generic Plus PS Printer Driver	5.9	More Details
CVE-2025-60184	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Terry L. SEO Search Permalink allows Stored XSS. This issue affects SEO Search Permalink: from n/a through 1.0.3.	5.9	More Details
CVE-2025-60185	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kontur.us kontur Admin Style allows Stored XSS. This issue affects kontur Admin Style: from n/a through 1.0.4.	5.9	More Details

60183	1.0.4.		
CVE-2025-3193	Versions of the package algoliasearch-helper from 2.0.0-rc1 and before 3.11.2 are vulnerable to Prototype Pollution in the _merge() function in merge.js, which allows constructor.prototype to be written even though doing so throws an error. In the "extreme edge-case" that the resulting error is caught, code injected into the user-supplied search parameter may be exeucted. This is related to but distinct from the issue reported in [CVE-2021-23433](https://security.snyk.io/vuln/SNYK-JS-ALGOLIASEARCHHELPER-1570421). **NOTE:** This vulnerability is not exploitable in the default configuration of InstantSearch since searchParameters are not modifiable by users.	5.9	More Details
CVE-2025-60179	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Space Studio Click & Tweet allows Stored XSS. This issue affects Click & Tweet: from n/a through 0.8.9.	5.9	More Details
CVE-2025-60186	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alex Moss Google+ Comments allows Stored XSS. This issue affects Google+ Comments: from n/a through 1.0.	5.9	More Details
CVE-2025-60136	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cartpauj User Notes allows Stored XSS. This issue affects User Notes: from n/a through 1.0.2.	5.9	More Details
CVE-2025-60154	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jennifer Moss MWW Disclaimer Buttons allows Stored XSS. This issue affects MWW Disclaimer Buttons: from n/a through 3.41.	5.9	More Details
CVE-2025-60144	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in yonifre Lenix scss compiler allows Stored XSS. This issue affects Lenix scss compiler: from n/a through 1.2.	5.9	More Details
CVE-2025-60146	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Amit Verma Map Categories to Pages allows Stored XSS. This issue affects Map Categories to Pages: from n/a through 1.3.2.	5.9	More Details
CVE-2025-26333	Dell Crypto-J generates an error message that includes sensitive information about its environment and associated data. A remote attacker could potentially exploit this vulnerability, leading to information exposure.	5.9	More Details
CVE-2025-60101	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Woostify Woostify allows Stored XSS. This issue affects Woostify: from n/a through 2.4.2.	5.9	More Details
CVE-2025-60104	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jordy Meow Gallery Custom Links allows Stored XSS. This issue affects Gallery Custom Links: from n/a through 2.2.5.	5.9	More Details
CVE-2025-60133	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DJ-Extensions.com PE Easy Slider allows Stored XSS. This issue affects PE Easy Slider: from n/a through 1.1.0.	5.9	More Details
CVE-2025-60149	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michael Ott Notely allows Stored XSS. This issue affects Notely: from n/a through 1.8.0.	5.9	More Details
CVE-2025-60141	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in thetechtribe The Tribal allows Stored XSS. This issue affects The Tribal: from n/a through 1.3.3.	5.9	More Details
CVE-2025-60158	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webmaniabr Nota Fiscal Eletrônica WooCommerce allows Stored XSS. This issue affects Nota Fiscal Eletrônica WooCommerce: from n/a through 3.4.0.6.	5.9	More Details
CVE-2025-60160	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sharkthemes Smart Related Products allows Stored XSS. This issue affects Smart Related Products: from n/a through 2.0.5.	5.9	More Details
CVE-2025-20339	A vulnerability in the access control list (ACL) processing of IPv4 packets of Cisco SD-WAN vEdge Software could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to the improper enforcement of the implicit deny all at the end of a configured ACL. An attacker could exploit this vulnerability by attempting to send unauthorized traffic to an interface on an affected device. A successful exploit could allow the attacker to bypass an ACL on the affected device.	5.8	More Details

CVE-2025-23272	NVIDIA nvJPEG library contains a vulnerability where an attacker can cause an out-of-bounds read by means of a specially crafted JPEG file. A successful exploit of this vulnerability might lead to information disclosure or denial of service.	5.7	More Details
CVE-2025-11060	A flaw was found in the live query subscription mechanism of the database engine. This vulnerability allows record or guest users to observe unauthorized records within the same table, bypassing access controls, via crafted LIVE SELECT subscriptions when other users alter or delete records.	5.7	More Details
CVE-2025-10504	Heap-based Buffer Overflow vulnerability in ABB Terra AC wallbox.This issue affects Terra AC wallbox: through 1.8.33.	5.7	More Details
CVE-2025-6815	The LatePoint – Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'service[name]' parameter in all versions up to, and including, 5.1.94 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, 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-2025-10911	A use-after-free vulnerability was found in libxslt while parsing xsl nodes that may lead to the dereference of expired pointers and application crash.	5.5	More Details
CVE-2025-10961	A vulnerability was determined in Wavlink NU516U1 M16U1_V240425. This affects the function sub_4030C0 of the file /cgi-bin/wireless.cgi of the component Delete_Mac_list Page. Executing manipulation of the argument delete_list can lead to command injection. The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2025-60181	Server-Side Request Forgery (SSRF) vulnerability in silence Silencesoft RSS Reader allows Server Side Request Forgery. This issue affects Silencesoft RSS Reader: from n/a through 0.6.	5.4	More Details
CVE-2025-60096	Missing Authorization vulnerability in CodexThemes TheGem (Elementor) allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects TheGem (Elementor): from n/a through 5.10.5.	5.4	More Details
CVE-2025-60103	Missing Authorization vulnerability in CridioStudio ListingPro allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects ListingPro: from n/a through 2.9.8.	5.4	More Details
CVE-2025-60116	Missing Authorization vulnerability in ThemeGoods Grand Conference Theme Custom Post Type allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Grand Conference Theme Custom Post Type: from n/a through 2.6.3.	5.4	More Details
CVE-2025-59402	Flock Safety Bravo Edge AI Compute Device BRAVO_00.00_local_20241017 accepts the default Thundercomm TurboX 6490 Firehose loader in EDL/QDL mode. This enables attackers with physical access to flash arbitrary firmware, dump partitions, and bypass bootloader and OS security controls.	5.4	More Details
CVE-2025-60127	Missing Authorization vulnerability in ArtistScope CopySafe Web Protection allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects CopySafe Web Protection: from n/a through 4.3.	5.4	More Details
CVE-2025-60161	Server-Side Request Forgery (SSRF) vulnerability in bdthemes ZoloBlocks allows Server Side Request Forgery. This issue affects ZoloBlocks: from n/a through 2.3.9.	5.4	More Details
CVE-2025-36132	IBM Planning Analytics Local 2.0.0 through 2.0.106 and 2.1.0 through 2.1.13 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-2025-60097	Missing Authorization vulnerability in CodexThemes TheGem allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects TheGem: from n/a through 5.10.5.	5.4	More Details
CVE-2025-10137	The Snow Monkey theme for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 29.1.5 via the request() function. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	5.4	More Details
CVE-			

2025- 46150	In PyTorch before 2.7.0, when torch.compile is used, FractionalMaxPool2d has inconsistent results.	5.3	More Details
CVE-2025-60119	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in CoSchedule CoSchedule allows Retrieve Embedded Sensitive Data. This issue affects CoSchedule: from n/a through 3.3.10.	5.3	More Details
CVE-2025-10995	A security vulnerability has been detected in Open Babel up to 3.1.1. This vulnerability affects the function zlib_stream::basic_unzip_streambuf::underflow in the library /src/zipstreamimpl.h. Such manipulation leads to memory corruption. Local access is required to approach this attack. The exploit has been disclosed publicly and may be used.	5.3	More Details
CVE-2025-60100	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in 8theme XStore allows Code Injection. This issue affects XStore: from n/a through 9.5.3.	5.3	More Details
CVE-2025-54477	Improper handling of authentication requests lead to a user enumeration vector in the passkey authentication method.	5.3	More Details
CVE-2025-46152	In PyTorch before 2.7.0, bitwise_right_shift produces incorrect output for certain out-of-bounds values of the "other" argument.	5.3	More Details
CVE-2025-46149	In PyTorch before 2.7.0, when inductor is used, nn.Fold has an assertion error.	5.3	More Details
CVE-2025-20293	A vulnerability in the Day One setup process of Cisco IOS XE Software for Catalyst 9800 Series Wireless Controllers for Cloud (9800-CL) could allow an unauthenticated, remote attacker to access the public-key infrastructure (PKI) server that is running on an affected device. This vulnerability is due to incomplete cleanup upon completion of the Day One setup process. An attacker could exploit this vulnerability by sending Simple Certificate Enrollment Protocol (SCEP) requests to an affected device. A successful exploit could allow the attacker to request a certificate from the virtual wireless controller and then use the acquired certificate to join an attacker-controlled device to the virtual wireless controller.	5.3	More Details
CVE-2025-10952	A security flaw has been discovered in geyang ml-logger up to acf255bade5be6ad88d90735c8367b28cbe3a743. Affected by this issue is the function stream_handler of the file ml_logger/server.py of the component File Handler. Performing manipulation of the argument key results in information disclosure. The attack can be initiated remotely. The exploit has been released to the public and may be exploited. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	5.3	More Details
CVE-2025-46153	PyTorch before 3.7.0 has a bernoulli_p decompose function in decompositions.py even though it lacks full consistency with the eager CPU implementation, negatively affecting nn.Dropout1d, nn.Dropout2d, and nn.Dropout3d for fallback_random=True.	5.3	More Details
CVE-2025-10954	Versions of the package github.com/nyaruka/phonenumbers before 1.2.2 are vulnerable to Improper Validation of Syntactic Correctness of Input in the phonenumbers.Parse() function. An attacker can cause a panic by providing crafted input causing a "runtime error: slice bounds out of range".	5.3	More Details
CVE-2025-10997	A flaw has been found in Open Babel up to 3.1.1. Impacted is the function ChemKinFormat::CheckSpecies of the file /src/formats/chemkinformat.cpp. Executing manipulation can lead to heap-based buffer overflow. The attack can only be executed locally. The exploit has been published and may be used.	5.3	More Details
CVE-2025-10994	A weakness has been identified in Open Babel up to 3.1.1. This affects the function GAMESSOutputFormat::ReadMolecule of the file gamessformat.cpp. This manipulation causes use after free. It is possible to launch the attack on the local host. The exploit has been made available to the public and could be exploited.	5.3	More Details
CVE-2025-10992	A vulnerability was determined in roncoo roncoo-pay up to 9428382af21cd5568319eae7429b7e1d0332ff40. Affected is an unknown function of the file /user/info/lookupList. Executing manipulation can lead to improper authorization. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-	A vulnerability has been found in GNU Binutils 2.45. The affected element is the function elf_swap_shdr in the library bfd/elfcode.h of the component Linker. The manipulation leads to heap-based buffer overflow.		More

2025- 11083	The attack must be carried out locally. The exploit has been disclosed to the public and may be used. The identifier of the patch is 9ca499644a21ceb3f946d1c179c38a83be084490. To fix this issue, it is recommended to deploy a patch. The code maintainer replied with "[f]ixed for 2.46".	5.3	More Details
CVE-2025-11082	A flaw has been found in GNU Binutils 2.45. Impacted is the function _bfd_elf_parse_eh_frame of the file bfd/elf-eh-frame.c of the component Linker. Executing manipulation can lead to heap-based buffer overflow. The attack is restricted to local execution. The exploit has been published and may be used. This patch is called ea1a0737c7692737a644af0486b71e4a392cbca8. A patch should be applied to remediate this issue. The code maintainer replied with "[f]ixed for 2.46".	5.3	More Details
CVE-2025-11079	A security flaw has been discovered in Campcodes Farm Management System 1.0. Affected by this issue is some unknown functionality. The manipulation results in file and directory information exposure. The attack may be performed from remote. The exploit has been released to the public and may be exploited.	5.3	More Details
CVE-2025-57623	A NULL pointer dereference in TOTOLINK N600R firmware v4.3.0cu.7866_B2022506 allows attackers to cause a Denial of Service.	5.3	More Details
CVE-2025-10879	All versions of Dingtian DT-R002 are vulnerable to an Insufficiently Protected Credentials vulnerability that could allow an attacker to retrieve the current user's username without authentication.	5.3	More Details
CVE-2025-10745	The Banhammer – Monitor Site Traffic, Block Bad Users and Bots plugin for WordPress is vulnerable to Blocking Bypass in all versions up to, and including, 3.4.8. This is due to a site-wide “secret key” being deterministically generated from a constant character set using md5() and base64_encode() and then stored in the `banhammer_secret_key` option. This makes it possible for unauthenticated attackers to bypass the plugin’s logging and blocking by appending a GET parameter named `banhammer-process_{SECRET}` where `{SECRET}` is the predictable value, thereby causing Banhammer to abort its protections for that request.	5.3	More Details
CVE-2025-9984	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the fifu_api_debug_posts() function in all versions up to, and including, 5.2.7. This makes it possible for unauthenticated attackers to read private/password protected posts.	5.3	More Details
CVE-2025-9985	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 5.2.7 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-2025-55554	pytorch v2.8.0 was discovered to contain an integer overflow in the component torch.nan_to_num-.long().	5.3	More Details
CVE-2025-55552	pytorch v2.8.0 was discovered to display unexpected behavior when the components torch.rot90 and torch.randn_like are used together.	5.3	More Details
CVE-2025-60121	Missing Authorization vulnerability in Ex-Themes WooEvents allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WooEvents: from n/a through 4.1.7.	5.3	More Details
CVE-2025-9904	Unallocated memory access vulnerability in print processing of Generic Plus PCL6 Printer Driver / Generic Plus UFR II Printer Driver / Generic Plus LIPS4 Printer Driver / Generic Plus LIPSLX Printer Driver / Generic Plus PS Printer Driver	5.3	More Details
CVE-2025-58919	Missing Authorization vulnerability in guihom Wide Banner allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Wide Banner: from n/a through 1.0.4.	5.3	More Details
CVE-2025-60092	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Shahjada Download Manager allows Retrieve Embedded Sensitive Data. This issue affects Download Manager: from n/a through 3.3.24.	5.3	More Details
CVE-2025-60120	Missing Authorization vulnerability in wpdirectorykit WP Directory Kit allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Directory Kit: from n/a through 1.3.8.	5.3	More Details
CVE-2025-48459	Deserialization of Untrusted Data vulnerability in Apache IoTDB. This issue affects Apache IoTDB: from 1.0.0 before 2.0.5. Users are recommended to upgrade to version 2.0.5, which fixes the issue.	5.3	More Details

48459			
CVE-2025-46148	In PyTorch through 2.6.0, when eager is used, nn.PairwiseDistance(p=2) produces incorrect results.	5.3	More Details
CVE-2025-60140	Insertion of Sensitive Information Into Sent Data vulnerability in thetechtribe The Tribal allows Retrieve Embedded Sensitive Data. This issue affects The Tribal: from n/a through 1.3.3.	5.3	More Details
CVE-2025-20316	A vulnerability in the access control list (ACL) programming of Cisco IOS XE Software for Cisco Catalyst 9500X and 9600X Series Switches could allow an unauthenticated, remote attacker to bypass a configured ACL on an affected device. This vulnerability is due to the flooding of traffic from an unlearned MAC address on a switch virtual interface (SVI) that has an egress ACL applied. An attacker could exploit this vulnerability by causing the VLAN to flush its MAC address table. This condition can also occur if the MAC address table is full. A successful exploit could allow the attacker to bypass an egress ACL on an affected device.	5.3	More Details
CVE-2025-60155	Missing Authorization vulnerability in loopus WP Virtual Assistant allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Virtual Assistant: from n/a through 3.0.	5.3	More Details
CVE-2025-57352	A vulnerability exists in the 'min-document' package prior to version 2.19.0, stemming from improper handling of namespace operations in the removeAttributeNS method. By processing malicious input involving the __proto__ property, an attacker can manipulate the prototype chain of JavaScript objects, leading to denial of service or arbitrary code execution. This issue arises from insufficient validation of attribute namespace removal operations, allowing unintended modification of critical object prototypes. The vulnerability remains unaddressed in the latest available version.	5.3	More Details
CVE-2025-57353	The Runtime components of messageformat package for Node.js prior to version 3.0.1 contain a prototype pollution vulnerability. Due to insufficient validation of nested message keys during the processing of message data, an attacker can manipulate the prototype chain of JavaScript objects by providing specially crafted input. This can result in the injection of arbitrary properties into the Object.prototype, potentially leading to denial of service conditions or unexpected application behavior. The vulnerability allows attackers to alter the prototype of base objects, impacting all subsequent object instances throughout the application's lifecycle. This issue remains unaddressed in the latest available version.	5.3	More Details
CVE-2025-55178	Llama Stack prior to version v0.2.20 accepted unverified parameters in the resolve_ast_by_type function which could potentially allow for remote code execution.	5.3	More Details
CVE-2025-11010	A vulnerability has been found in vstakhov libucl up to 0.9.2. Affected by this vulnerability is the function ucl_include_common of the file /src/ucl_util.c. Such manipulation leads to heap-based buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2025-11012	A vulnerability was determined in BehaviorTree up to 4.7.0. This affects the function ParseScript of the file /src/script_parser.cpp of the component Diagnostic Message Handler. Executing manipulation of the argument error_msgs_buffer can lead to stack-based buffer overflow. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized. This patch is called cb6c7514efa628adb8180b58b4c9ccdebbe096e3. A patch should be applied to remediate this issue.	5.3	More Details
CVE-2025-11014	A security flaw has been discovered in OGRECave Ogre up to 14.4.1. This issue affects the function STBIImageCodec::encode of the file /ogre/PlugIns/STBICodec/src/OgreSTBICodec.cpp of the component Image Handler. The manipulation results in heap-based buffer overflow. The attack is only possible with local access. The exploit has been released to the public and may be exploited.	5.3	More Details
CVE-2025-11025	Insertion of Sensitive Information Into Sent Data vulnerability in Vimesoft Information Technologies and Software Inc. Vimesoft Corporate Messaging Platform allows Retrieve Embedded Sensitive Data.This issue affects Vimesoft Corporate Messaging Platform: from V1.3.0 before V2.0.0.	5.3	More Details
CVE-2025-56764	Trivision NC-227WF firmware 5.80 (build 20141010) login mechanism reveals whether a username exists or not by returning different error messages ("Unknown user" vs. "Wrong password"), allowing an attacker to enumerate valid usernames.	5.3	More Details
CVE-2025-11018	A flaw has been found in Four-Faith Water Conservancy Informatization Platform 1.0. This affects an unknown function of the file /sysRole/index.do/../../generalReport/download.do;usrlogout.do.do. Executing manipulation of the argument fileName can lead to path traversal. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details

CVE-2025-11028	A security flaw has been discovered in givanz Vvveb up to 1.0.7.2. This affects an unknown part of the component Image Handler. Performing manipulation results in information disclosure. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited. Once again the project maintainer reacted very professional: "I accept the existence of these vulnerabilities. (...) I fixed the code to remove these vulnerabilities and will push the code to github and make a new release."	5.3	More Details
CVE-2025-10947	A flaw has been found in Sistemas Pleno Gestão de Locação up to 2025.7.x. The impacted element is an unknown function of the file /api/areacliente/pessoa/validarCpf of the component CPF Handler. Executing manipulation of the argument pes_cpf can lead to authorization bypass. The attack can be executed remotely. The exploit has been published and may be used. Upgrading to version 2025.8.0 is sufficient to resolve this issue. It is advisable to upgrade the affected component.	5.3	More Details
CVE-2025-11015	A weakness has been identified in OGRECave Ogre up to 14.4.1. Impacted is the function STBIImageCodec::encode of the file /ogre/PlugIns/STBICodec/src/OgreSTBICodec.cpp. This manipulation causes mismatched memory management routines. The attack is restricted to local execution. The exploit has been made available to the public and could be exploited.	5.3	More Details
CVE-2025-10996	A vulnerability was detected in Open Babel up to 3.1.1. This issue affects the function OBSmilesParser::ParseSmiles of the file /src/formats/smilesformat.cpp. Performing manipulation results in heap-based buffer overflow. The attack needs to be approached locally. The exploit is now public and may be used.	5.3	More Details
CVE-2025-60125	Insertion of Sensitive Information Into Sent Data vulnerability in themelooks FoodBook allows Retrieve Embedded Sensitive Data. This issue affects FoodBook: from n/a through 4.7.1.	5.3	More Details
CVE-2025-41716	The web application allows an unauthenticated remote attacker to learn information about existing user accounts with their corresponding role due to missing authentication for critical function.	5.3	More Details
CVE-2025-11031	A flaw has been found in DataTables up to 1.10.13. The affected element is an unknown function of the file /examples/resources/examples.php. This manipulation of the argument src causes path traversal. It is possible to initiate the attack remotely. The exploit has been published and may be used. Upgrading to version 1.10.15 is sufficient to fix this issue. Patch name: 3b24f99ac4ddb7f9072076b0d07f0b1a408f177a. Upgrading the affected component is advised. This vulnerability was initially reported for code-projects Faculty Management System but appears to affect DataTables as an upstream component instead. The vendor of DataTables explains: "I would suggest that the author upgrade to the latest versions of DataTables (actually, they shouldn't really be deploying that file to their own server at all - it is only relevant for the DataTables examples)."	5.3	More Details
CVE-2025-60129	Missing Authorization vulnerability in Yext Yext allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Yext: from n/a through 1.1.3.	5.3	More Details
CVE-2025-60130	Missing Authorization vulnerability in wedos.com WEDOS Global allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects WEDOS Global: from n/a through 1.2.2.	5.3	More Details
CVE-2025-57852	A container privilege escalation flaw was found in KServe ModelMesh container images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.	5.2	More Details
CVE-2025-60251	Unitree Go2, G1, H1, and B2 devices through 2025-09-20 accept any handshake secret with the unitree substring.	5.0	More Details
CVE-2025-26482	Dell PowerEdge Server BIOS and Dell iDRAC9, all versions, contains an Information Disclosure vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information Disclosure.	4.9	More Details
CVE-2025-10036	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to SQL Injection via the get_all_urls() function in all versions up to, and including, 5.2.7 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-2025-10037	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to SQL Injection via the get_posts_with_internal_featured_image() function in all versions up to, and including, 5.2.7 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-2025-60106	Missing Authorization vulnerability in Roxnor EmailKit allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects EmailKit: from n/a through 1.6.0.	4.9	More Details
CVE-2025-36262	IBM Planning Analytics Local 2.0.0 through 2.0.106 and 2.1.0 through 2.1.13 could allow a malicious privileged user to bypass the UI to gain unauthorized access to sensitive information due to the improper validation of input.	4.9	More Details
CVE-2025-36099	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A privileged user could exploit this vulnerability to cause the server to consume memory resources.	4.9	More Details
CVE-2025-41245	VMware Aria Operations contains an information disclosure vulnerability. A malicious actor with non-administrative privileges in Aria Operations may exploit this vulnerability to disclose credentials of other users of Aria Operations.	4.9	More Details
CVE-2025-57877	There is a reflected cross site scripting vulnerability in Esri Portal for ArcGIS 11.4 and below that may allow a remote authenticated attacker with administrative access to supply a crafted string which would execute arbitrary JavaScript code in the browser.	4.8	More Details
CVE-2025-57871	There is a reflected cross site scripting vulnerability in Esri Portal for ArcGIS 11.4 and below that may allow a remote authenticated attacker with administrative access to supply a crafted string which would execute arbitrary JavaScript code in the browser.	4.8	More Details
CVE-2025-57873	There is a reflected cross site scripting vulnerability in Esri Portal for ArcGIS 11.4 and below that may allow a remote authenticated attacker with administrative access to supply a crafted string which would execute arbitrary JavaScript code in the browser.	4.8	More Details
CVE-2025-57874	There is a reflected cross site scripting vulnerability in Esri Portal for ArcGIS 11.4 and below that may allow a remote authenticated attacker with administrative access to supply a crafted string which would execute arbitrary JavaScript code in the browser.	4.8	More Details
CVE-2025-57875	There is a reflected cross site scripting vulnerability in Esri Portal for ArcGIS 11.4 and below that may allow a remote authenticated attacker with administrative access to supply a crafted string which would execute arbitrary JavaScript code in the browser.	4.8	More Details
CVE-2025-57876	There is a stored Cross-site Scripting vulnerability in Esri Portal for ArcGIS 11.4 and below that may allow a remote, authenticated attacker to inject malicious a file with an embedded xss script which when loaded could potentially execute arbitrary JavaScript code in the victim’s browser. The privileges required to execute this attack are high. The attack could disclose a privileged token which may result in the attacker gaining full control of the Portal.	4.8	More Details
CVE-2025-28016	A Reflected Cross-Site Scripting (XSS) vulnerability was found in loginsystem/edit-profile.php of the PHPGurukul User Registration & Login and User Management System V3.3. This vulnerability allows remote attackers to execute arbitrary JavaScript code via the fname, lname, and contact parameters.	4.8	More Details
CVE-2025-60018	glib-networking's OpenSSL backend fails to properly check the return value of a call to BIO_write(), resulting in an out of bounds read.	4.8	More Details
CVE-2025-48867	Horilla is a free and open source Human Resource Management System (HRMS). A stored cross-site scripting (XSS) vulnerability in Horilla HRM 1.3.0 allows authenticated admin or privileged users to inject malicious JavaScript payloads into multiple fields in the Project and Task modules. These payloads persist in the database and are executed when viewed by an admin or other privileged users through the web interface. Although the issue is not exploitable by unauthenticated users, it still poses a high risk of session hijacking and unauthorized action within high-privilege accounts. At time of publication there is no known patch.	4.8	More Details
CVE-2025-11103	A security vulnerability has been detected in Projectworlds Online Tours and Travels 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/change-image.php. The manipulation of the argument packageimage leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	4.7	More Details

CVE-2025-11136	A flaw has been found in YiFang CMS up to 2.0.2. The impacted element is the function webUploader of the file app/app/controller/File.php of the component Backend. Executing manipulation of the argument uploadpath can lead to unrestricted upload. The attack can be launched remotely. The exploit has been published and may be used.	4.7	More Details
CVE-2025-10993	A security flaw has been discovered in MuYuCMS up to 2.7. Affected by this issue is some unknown functionality of the file /admin.php of the component Template Management. The manipulation results in code injection. It is possible to launch the attack remotely.	4.7	More Details
CVE-2025-11141	A security flaw has been discovered in Ruijie NBR2100G-E up to 20250919. Affected by this issue is the function listAction of the file /itbox_pi/branch_passw.php?a=list. Performing manipulation of the argument city results in os command injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited. Other parameters might be affected as well. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-60250	Unitree Go2, G1, H1, and B2 devices through 2025-09-20 decrypt BLE packet data by using the df98b715d5c6ed2b25817b6f2554124a key and the 2841ae97419c2973296a0d4bdfe19a4f IV.	4.7	More Details
CVE-2025-11073	A vulnerability was detected in Keyfactor RG-EW5100BE EW_3.0B11P280_EW5100BE-PRO_12183019. The affected element is an unknown function of the file /cgi-bin/luci/api/cmd of the component HTTP POST Request Handler. The manipulation of the argument url results in command injection. The attack can be launched remotely. The exploit is now public and may be used.	4.7	More Details
CVE-2025-11071	A security vulnerability has been detected in SeaCMS 13.3.20250820. Impacted is an unknown function of the file /admin_cron.php of the component Cron Task Management Module. The manipulation of the argument resourcefrom/collectID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	4.7	More Details
CVE-2025-23292	NVIDIA Delegated Licensing Service for all appliance platforms contains a SQL injection vulnerability where an User/Attacker may cause an authorized action. A successful exploit of this vulnerability may lead to partial denial of service (UI component).	4.6	More Details
CVE-2025-23274	NVIDIA nvJPEG contains a vulnerability in jpeg encoding where a user may cause an out-of-bounds read by providing a maliciously crafted input image with dimensions that cause integer overflows in array index calculations. A successful exploit of this vulnerability may lead to denial of service.	4.5	More Details
CVE-2025-33116	IBM Watson Studio 4.0 through 5.2.0 on Cloud Pak for Data is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	4.4	More Details
CVE-2025-10490	The Zephyr Project Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.3.202 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-2025-11163	The SmartCrawl SEO checker, analyzer & optimizer plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the update_submodule() function in all versions up to, and including, 3.14.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugin's setttings.	4.3	More Details
CVE-2025-9948	The Chat by Chatwee plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1.3. This is due to missing or incorrect nonce validation on the admin settings page. This makes it possible for unauthenticated attackers to modify plugin 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-2025-10752	The OAuth Single Sign On – SSO (OAuth Client) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.26.12. This is due to using a predictable state parameter (base64 encoded app name) without any randomness in the OAuth flow. This makes it possible for unauthenticated attackers to forge OAuth authorization requests and potentially hijack the OAuth flow 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-2025-36351	IBM License Metric Tool 9.2.0 through 9.2.40 could allow an authenticated user to bypass access controls in the REST API interface and perform unauthorized actions.	4.3	More Details
CVE-	A vulnerability in the IPv6 Router Advertisement (RA) packet processing of Cisco Access Point Software could allow an unauthenticated, adjacent attacker to modify the IPv6 gateway on an affected device. This vulnerability is due to a logic error in the processing of IPv6 RA packets that are received from wireless		

2025-20365	clients. An attacker could exploit this vulnerability by associating to a wireless network and sending a series of crafted IPv6 RA packets. A successful exploit could allow the attacker to temporarily change the IPv6 gateway of an affected device. This could also lead to intermittent packet loss for any wireless clients that are associated with the affected device.	4.3	More Details
CVE-2025-35034	Medical Informatics Engineering Enterprise Health has a reflected cross site scripting vulnerability in the 'portlet_user_id' URL parameter. A remote, unauthenticated attacker can craft a URL that can execute arbitrary JavaScript in the victim's browser. This issue is fixed as of 2025-03-14.	4.3	More Details
CVE-2025-10981	A vulnerability was detected in JeecgBoot up to 3.8.2. This impacts an unknown function of the file /sys/tenant/exportXls. Performing manipulation results in improper authorization. The attack can be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-10980	A security vulnerability has been detected in JeecgBoot up to 3.8.2. This affects an unknown function of the file /sys/position/exportXls. Such manipulation leads to improper authorization. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-10979	A weakness has been identified in JeecgBoot up to 3.8.2. The impacted element is an unknown function of the file /sys/role/exportXls. This manipulation causes improper authorization. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-10978	A security flaw has been discovered in JeecgBoot up to 3.8.2. The affected element is an unknown function of the file /sys/user/exportXls of the component Filter Handler. The manipulation results in improper authorization. The attack may be performed from remote. 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.	4.3	More Details
CVE-2025-11125	A vulnerability was found in langleyfcu Online Banking System up to 57437e6400ce0ae240e692c24e6346b8d0c17d7a. Affected by this vulnerability is an unknown functionality of the file /connection_error.php of the component Error Message Handler. Performing manipulation of the argument Error results in cross site scripting. Remote exploitation of the attack is possible. The exploit has been made public and could be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided.	4.3	More Details
CVE-2025-11112	A security vulnerability has been detected in PHPGurukul Employee Record Management System 1.3. This impacts an unknown function of the file /myprofile.php. Such manipulation of the argument First name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2025-20364	A vulnerability in the Device Analytics action frame processing of Cisco Wireless Access Point (AP) Software could allow an unauthenticated, adjacent attacker to inject wireless 802.11 action frames with arbitrary information. This vulnerability is due to insufficient verification checks of incoming 802.11 action frames. An attacker could exploit this vulnerability by sending 802.11 Device Analytics action frames with arbitrary parameters. A successful exploit could allow the attacker to inject Device Analytics action frames with arbitrary information, which could modify the Device Analytics data of valid wireless clients that are connected to the same wireless controller.	4.3	More Details
CVE-2025-9031	Observable Timing Discrepancy vulnerability in DivvyDrive Information Technologies Inc. DivvyDrive Web allows Cross-Domain Search Timing.This issue affects DivvyDrive Web: from 4.8.2.2 before 4.8.2.15.	4.3	More Details
CVE-2025-59426	Lobe Chat is an open-source artificial intelligence chat framework. Prior to version 1.130.1, the project's OIDC redirect handling logic constructs the host and protocol of the final redirect URL based on the X-Forwarded-Host or Host headers and the X-Forwarded-Proto value. In deployments where a reverse proxy forwards client-supplied X-Forwarded-* headers to the origin as-is, or where the origin trusts them without validation, an attacker can inject an arbitrary host and trigger an open redirect that sends users to a malicious domain. This issue has been patched in version 1.130.1.	4.3	More Details
CVE-2025-60166	Missing Authorization vulnerability in wpshuffle WP Subscription Forms PRO allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Subscription Forms PRO: from n/a through 2.0.5.	4.3	More Details
CVE-2025-58457	Improper permission check in ZooKeeper AdminServer lets authorized clients to run snapshot and restore command with insufficient permissions. This issue affects Apache ZooKeeper: from 3.9.0 before 3.9.4. Users are recommended to upgrade to version 3.9.4, which fixes the issue. The issue can be mitigated by disabling both commands (via admin.snapshot.enabled and admin.restore.enabled), disabling the whole AdminServer interface (via admin.enableServer), or ensuring that the root ACL does not provide open	4.3	More Details

	permissions. (Note that ZooKeeper ACLs are not recursive, so this does not impact operations on child nodes besides notifications from recursive watches.)		
CVE-2025-11119	A security flaw has been discovered in itsourcecode Hostel Management System 1.0. Impacted is an unknown function of the file /justines/index.php of the component POST Request Handler. Performing manipulation of the argument from results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	4.3	More Details
CVE-2025-60167	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in honzat Page Manager for Elementor allows Retrieve Embedded Sensitive Data. This issue affects Page Manager for Elementor: from n/a through 2.0.5.	4.3	More Details
CVE-2025-11051	A vulnerability has been found in SourceCodester Pet Grooming Management Software 1.0. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. The attack is possible to be carried out remotely.	4.3	More Details
CVE-2025-60095	Insertion of Sensitive Information Into Sent Data vulnerability in Benjamin Intal Stackable allows Retrieve Embedded Sensitive Data. This issue affects Stackable: from n/a through 3.18.1.	4.3	More Details
CVE-2025-60113	Cross-Site Request Forgery (CSRF) vulnerability in grooni Groovy Menu allows Cross Site Request Forgery. This issue affects Groovy Menu: from n/a through 1.4.3.	4.3	More Details
CVE-2025-11016	A security vulnerability has been detected in kalcaddle kodbox up to 1.61.09. The affected element is the function fileOut of the file app/controller/explorer/index.class.php. Such manipulation of the argument path leads to path traversal. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2025-10377	The System Dashboard plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.8.20. This is due to missing nonce validation on the sd_toggle_logs() function. This makes it possible for unauthenticated attackers to toggle critical logging settings including Page Access Logs, Error Logs, and Email Delivery Logs 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-2025-60143	Missing Authorization vulnerability in netgsm Netgsm allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Netgsm: from n/a through 2.9.58.	4.3	More Details
CVE-2025-60145	Cross-Site Request Forgery (CSRF) vulnerability in yonifre Lenix scss compiler allows Cross Site Request Forgery. This issue affects Lenix scss compiler: from n/a through 1.2.	4.3	More Details
CVE-2025-9944	The Professional Contact Form 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 or incorrect nonce validation on the watch_for_contact_form_submit function. This makes it possible for unauthenticated attackers to trigger test email sending 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-2025-9898	The cForms – Light speed fast Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.0. This is due to missing or incorrect nonce validation on the cforms_api function. This makes it possible for unauthenticated attackers to modify forms and their 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-2025-60115	Cross-Site Request Forgery (CSRF) vulnerability in instapagedev Instapage Plugin allows Cross Site Request Forgery. This issue affects Instapage Plugin: from n/a through 3.5.12.	4.3	More Details
CVE-2025-60094	Missing Authorization vulnerability in Benjamin Intal Stackable allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Stackable: from n/a through 3.18.1.	4.3	More Details
CVE-2025-9896	The HidePost plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.3.8. This is due to missing or incorrect nonce validation on the options.php settings page. This makes it possible for unauthenticated attackers to modify plugin 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-	The Sync Feedly plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing or incorrect nonce validation on the crsf_cron_job_func		

CVE-2025-9894	and including, 1.0.1. This is due to missing or incorrect nonce validation on the crsf_cron_job_run() function. This makes it possible for unauthenticated attackers to trigger content synchronization from Feedly, potentially creating multiple posts 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-2025-9893	The VM Menu Reorder plugin 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 or incorrect nonce validation on the vm_set_to_default function. This makes it possible for unauthenticated attackers to reset all menu reordering 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-2025-10498	The Ninja Forms – The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.12.0. This is due to missing or incorrect nonce validation when exporting CSV files. This makes it possible for unauthenticated attackers to delete those files granted they can trick an administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-10499	The Ninja Forms – The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.12.0. This is due to missing or incorrect nonce validation on the maybe_opt_in() function. This makes it possible for unauthenticated attackers to opt an affected site into usage statistics collection 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-2025-58914	Cross-Site Request Forgery (CSRF) vulnerability in Di Themes Di Themes Demo Site Importer allows Cross Site Request Forgery. This issue affects Di Themes Demo Site Importer: from n/a through 1.2.	4.3	More Details
CVE-2025-60093	Cross-Site Request Forgery (CSRF) vulnerability in Shahjada Download Manager allows Cross Site Request Forgery. This issue affects Download Manager: from n/a through 3.3.24.	4.3	More Details
CVE-2025-11029	A weakness has been identified in givanz Vvveb up to 1.0.7.2. This vulnerability affects unknown code. Executing manipulation can lead to cross-site request forgery. The attack can be executed remotely. The exploit has been made available to the public and could be exploited. Once again the project maintainer reacted very professional: "I accept the existence of these vulnerabilities. (...) I fixed the code to remove these vulnerabilities and will push the code to github and make a new release."	4.3	More Details
CVE-2025-60139	Cross-Site Request Forgery (CSRF) vulnerability in Joovii Sendle Shipping allows Cross Site Request Forgery. This issue affects Sendle Shipping: from n/a through 6.02.	4.3	More Details
CVE-2025-60165	Missing Authorization vulnerability in HaruTheme Frames allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Frames: from n/a through 1.5.7.	4.3	More Details
CVE-2025-60159	Missing Authorization vulnerability in webmaniabr Nota Fiscal Eletrônica WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Nota Fiscal Eletrônica WooCommerce: from n/a through 3.4.0.6.	4.3	More Details
CVE-2025-60152	Missing Authorization vulnerability in wpshuffle Subscribe To Unlock allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Subscribe To Unlock: from n/a through 1.1.5.	4.3	More Details
CVE-2025-11080	A security vulnerability has been detected in zhuimengshaonian wisdom-education up to 1.0.4. This vulnerability affects the function selectStudentExamInfoList of the file src/main/java/com/education/api/controller/student/ExamInfoController.java. Such manipulation of the argument subjectId leads to improper authorization. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2025-60148	Missing Authorization vulnerability in wpshuffle Subscribe to Download allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Subscribe to Download: from n/a through 2.0.9.	4.3	More Details
CVE-2025-60117	Cross-Site Request Forgery (CSRF) vulnerability in TangibleWP Vehica Core allows Cross Site Request Forgery. This issue affects Vehica Core: from n/a through 1.0.100.	4.3	More Details
CVE-2025-11042	An issue was discovered in GitLab CE/EE affecting all versions starting from 17.2 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1, that allows an attacker to cause uncontrolled CPU consumption, potentially leading to a Denial of Service (DoS) condition while using specific GraphQL queries.	4.3	More Details
CVE-			

CVE-2025-60137	Cross-Site Request Forgery (CSRF) vulnerability in Galaxy Weblinks Post Featured Video allows Cross Site Request Forgery. This issue affects Post Featured Video: from n/a through 1.7.	4.3	More Details
CVE-2025-11034	A vulnerability was found in Dibo Data Decision Making System up to 2.7.0. The affected element is the function downloadImpTemplet of the file /common/dep/common_dep.action.jsp. The manipulation of the argument filePath results in path traversal. It is possible to launch the attack remotely. The exploit has been made public and could be used.	4.3	More Details
CVE-2025-60128	Missing Authorization vulnerability in WP Delicious Delisho allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Delisho: from n/a through 1.1.3.	4.3	More Details
CVE-2025-60123	Missing Authorization vulnerability in HivePress HivePress Claim Listings allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects HivePress Claim Listings: from n/a through 1.1.3.	4.3	More Details
CVE-2025-60122	Missing Authorization vulnerability in HivePress HivePress Claim Listings allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects HivePress Claim Listings: from n/a through 1.1.3.	4.3	More Details
CVE-2025-23275	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in nvJPEG where a local authenticated user may cause a GPU out-of-bounds write by providing certain image dimensions. A successful exploit of this vulnerability may lead to denial of service and information disclosure.	4.2	More Details
CVE-2025-35033	Medical Informatics Engineering Enterprise Health has a CSV injection vulnerability that allows a remote, authenticated attacker to inject macros in downloadable CSV files. This issue is fixed as of 2025-03-14.	4.1	More Details
CVE-2025-10859	Cookie storage for non-HTML temporary documents was being shared incorrectly with normal browsing content, allowing information from private tabs to escape Incognito mode even after the user closed all tabs This vulnerability affects Firefox for iOS < 143.1.	4.0	More Details
CVE-2025-59362	Squid through 7.1 mishandles ASN.1 encoding of long SNMP OIDs. This occurs in asn_build_objid in lib/snmplib/asn1.c.	4.0	More Details
CVE-2025-36601	Dell PowerScale OneFS, versions 9.5.0.0 through 9.11.0.0, contains an exposure of sensitive information to an unauthorized actor vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to Information disclosure.	4.0	More Details
CVE-2025-5494	ZohoCorp ManageEngine Endpoint Central was impacted by an improper privilege management issue in the agent setup. This issue affects Endpoint Central: through 11.4.2500.25, through 11.4.2508.13.	3.9	More Details
CVE-2025-10871	An issue has been discovered in GitLab EE affecting all versions from 16.6 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1. Project Maintainers can exploit a vulnerability where they can assign custom roles to users with permissions exceeding their own, effectively granting themselves elevated privileges.	3.8	More Details
CVE-2025-36326	IBM Cognos Controller 11.0.0 through 11.0.1, and IBM Controller 11.1.0 through 11.1.1 could allow an attacker to obtain sensitive information due to the use of hardcoded cryptographic keys for signing session cookies.	3.7	More Details
CVE-2025-60019	glib-networking's OpenSSL backend fails to properly check the return value of memory allocation routines. An out of memory condition could potentially result in writing to an invalid memory location.	3.7	More Details
CVE-2025-1396	A username enumeration vulnerability exists in multiple WSO2 products when Multi-Attribute Login is enabled. In this configuration, the system returns a distinct "User does not exist" error message to the login form, regardless of the validate_username setting. This behavior allows malicious actors to determine which usernames exist in the system based on observable discrepancies in the application's responses. Exploitation of this vulnerability could aid in brute-force attacks, targeted phishing campaigns, or other social engineering techniques by confirming the validity of user identifiers within the system.	3.7	More Details
CVE-2025-10868	An issue has been discovered in GitLab CE/EE affecting all versions from 17.4 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1 where certain string conversion methods exhibit performance degradation with large inputs.	3.5	More Details
CVE-	The EKEN video doorbell T6 BT60PLUS_MAIN_V1.0_GC1084_20230531 periodically sends debug logs to		More

2025- 56675	the EKEN cloud servers with sensitive information such as the Wi-Fi SSID and password.	3.5	More Details
CVE-2025-10943	A security flaw has been discovered in MikeCen WeChat-Face-Recognition up to 6e3f72bf8547d80b59e330f1137e4aa505f492c1. This vulnerability affects the function valid of the file wx.php. The manipulation of the argument echostr results in cross site scripting. The attack can be launched remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-5069	An issue has been discovered in GitLab CE/EE affecting all versions from 17.10 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1 that could have allowed an authenticated user to gain unauthorized access to confidential issues by creating a project with an identical name to the victim's project.	3.5	More Details
CVE-2025-55795	The openml/openml.org web application version v2.0.20241110 uses incremental user IDs and insufficient email ownership verification during email update workflows. An authenticated attacker controlling a user account with a lower user ID can update their email address to that of another user with a higher user ID without proper verification. This results in the victim's email being reassigned to the attacker's account, causing the victim to be locked out immediately and unable to log in. The vulnerability leads to denial of service via account lockout but does not grant the attacker direct access to the victim's private data.	3.5	More Details
CVE-2025-11137	A vulnerability has been found in Gstarsoft GstarCAD up to 9.4.0. This affects an unknown function of the component File Renaming Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Applying a patch is the recommended action to fix this issue.	3.5	More Details
CVE-2025-11026	A vulnerability was determined in givanz Vvveb up to 1.0.7.2. Affected by this vulnerability is an unknown functionality of the component Configuration File Handler. This manipulation causes information disclosure. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. Once again the project maintainer reacted very professional: "I accept the existence of these vulnerabilities. (...) I fixed the code to remove these vulnerabilities and will push the code to github and make a new release."	3.5	More Details
CVE-2025-10945	A security vulnerability has been detected in nuz007 smsboom up to 01b2f35bbbc23f3e0f60f38ca0e3d1b286f8d674. Impacted is an unknown function of the file d.php. Such manipulation of the argument hm leads to cross site scripting. 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.	3.5	More Details
CVE-2025-11124	A vulnerability has been found in code-projects Project Monitoring System 1.0. Affected is an unknown function of the file /onlineJobSearchEngine/postjob.php. Such manipulation of the argument txtapplyto leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	3.5	More Details
CVE-2025-10867	An issue has been discovered in GitLab CE/EE affecting all versions from 18.1 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1 that could have allowed an authenticated user to create a denial-of-service condition by exploiting an unprotected GraphQL API through repeated requests.	3.5	More Details
CVE-2025-10946	A vulnerability was detected in nuz007 smsboom up to 01b2f35bbbc23f3e0f60f38ca0e3d1b286f8d674. The affected element is an unknown function of the file dy.php. Performing manipulation of the argument hm results in cross site scripting. Remote exploitation of the attack is possible. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided.	3.5	More Details
CVE-2025-10944	A weakness has been identified in yi-ge get-header-ip up to 589b23d0eb0043c310a6a13ce4bbe2505d0d0b15. This issue affects the function ip of the file ip.php. This manipulation of the argument callback causes cross site scripting. 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. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-35032	Medical Informatics Engineering Enterprise Health allows authenticated users to upload arbitrary files. The impact of this behavior depends on how files are accessed. This issue is fixed as of 2025-04-08.	3.4	More Details
CVE-2025-23346	NVIDIA CUDA Toolkit contains a vulnerability in cuobjdump, where an unprivileged user can cause a NULL pointer dereference. A successful exploit of this vulnerability may lead to a limited denial of service.	3.3	More Details

CVE-2025-36857	Rapid7 Appspider Pro versions below 7.5.021, suffer from a broken access control vulnerability in the application's configuration file loading mechanism, whereby an attacker can place files in directories belonging to other users or projects. Affected versions allow standard users to add custom configuration files. These files, which are loaded in alphabetical order, can override or change the settings of the original configuration files, creating a security vulnerability. This issue stems from improper directory access management. This vulnerability was remediated in version 7.5.021 of the product.	3.3	More Details
CVE-2025-10999	A vulnerability was found in Open Babel up to 3.1.1. The impacted element is the function CacaoFormat::SetHilderbrandt of the file /src/formats/cacaoformat.cpp. The manipulation results in null pointer dereference. The attack is only possible with local access. The exploit has been made public and could be used.	3.3	More Details
CVE-2025-23248	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in the nvdisasm binary where a user may cause an out-of-bounds read by passing a malformed ELF file to nvdisasm. A successful exploit of this vulnerability may lead to a partial denial of service.	3.3	More Details
CVE-2025-11011	A vulnerability was found in BehaviorTree up to 4.7.0. Affected by this issue is the function JsonExporter::fromJson of the file /src/json_export.cpp. Performing manipulation of the argument Source results in null pointer dereference. The attack needs to be approached locally. The exploit has been made public and could be used. The patch is named 4b23dcaf0ce951a31299ebdd61df69f9ce99a76d. It is suggested to install a patch to address this issue.	3.3	More Details
CVE-2025-23340	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in the nvdisasm binary where a user may cause an out-of-bounds read by passing a malformed ELF file to nvdisasm. A successful exploit of this vulnerability may lead to a partial denial of service.	3.3	More Details
CVE-2025-23339	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in cuobjdump where an attacker may cause a stack-based buffer overflow by getting the user to run cuobjdump on a malicious ELF file. A successful exploit of this vulnerability may lead to arbitrary code execution at the privilege level of the user running cuobjdump.	3.3	More Details
CVE-2025-23255	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in the cuobjdump binary where a user may cause an out-of-bounds read by passing a malformed ELF file to cuobjdump. A successful exploit of this vulnerability may lead to a partial denial of service.	3.3	More Details
CVE-2025-23338	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in nvdisasm where a user may cause an out-of-bounds write by running nvdisasm on a malicious ELF file. A successful exploit of this vulnerability may lead to denial of service.	3.3	More Details
CVE-2025-23308	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in nvdisasm where an attacker may cause a heap-based buffer overflow by getting the user to run nvdisasm on a malicious ELF file. A successful exploit of this vulnerability may lead to arbitrary code execution at the privilege level of the user running nvdisasm.	3.3	More Details
CVE-2025-35031	Medical Informatics Engineering Enterprise Health includes the user's current session token in debug output. An attacker could convince a user to send this output to the attacker, thus allowing the attacker to impersonate that user. This issue is fixed as of 2025-04-08.	3.3	More Details
CVE-2025-23271	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in the nvdisasm binary where a user may cause an out-of-bounds read by passing a malformed ELF file to nvdisasm. A successful exploit of this vulnerability may lead to a partial denial of service.	3.3	More Details
CVE-2025-11017	A vulnerability was detected in OGRECave Ogre up to 14.4.1. The impacted element is the function Ogre::LogManager::stream of the file /ogre/OgreMain/src/OgreLogManager.cpp. Performing manipulation of the argument mDefaultLog results in null pointer dereference. The attack must be initiated from a local position. The exploit is now public and may be used.	3.3	More Details
CVE-2025-11013	A vulnerability was identified in BehaviorTree up to 4.7.0. This vulnerability affects the function XMLParser::PImpl::loadDocImpl of the file /src/xml_parsing.cpp of the component XML Parser. The manipulation leads to null pointer dereference. The attack can only be performed from a local environment. The exploit is publicly available and might be used.	3.3	More Details
CVE-2025-10998	A vulnerability has been found in Open Babel up to 3.1.1. The affected element is the function ChemKinFormat::ReadReactionQualifierLines of the file /src/formats/chemkinformat.cpp. The manipulation leads to null pointer dereference. The attack can only be performed from a local environment. The exploit has been disclosed to the public and may be used.	3.3	More Details
CVE-2025-11195	Rapid7 AppSpider Pro versions below 7.5.021 suffer from a project name validation vulnerability, whereby an attacker can change the project name directly in the configuration file to a name that already exists. This issue stems from a lack of effective verification of the uniqueness of project names when editing them outside the application in affected versions. This vulnerability was remediated in	3.3	More Details

11193	version 7.5.021 of the product.		
CVE-2025-11081	A vulnerability was detected in GNU Binutils 2.45. This issue affects the function dump_dwarf_section of the file binutils/objdump.c. Performing manipulation results in out-of-bounds read. The attack is only possible with local access. The exploit is now public and may be used. The patch is named f87a66db645caf8cc0e6fc87b0c28c78a38af59b. It is suggested to install a patch to address this issue.	3.3	More Details
CVE-2025-11000	A vulnerability was determined in Open Babel up to 3.1.1. This affects the function PQSFormat::ReadMolecule of the file /src/formats/PQSformat.cpp. This manipulation causes null pointer dereference. The attack is restricted to local execution. The exploit has been publicly disclosed and may be utilized.	3.3	More Details
CVE-2025-36144	IBM Lakehouse (watsonx.data 2.2) stores potentially sensitive information in log files that could be read by a local user.	3.3	More Details
CVE-2025-10977	A vulnerability was identified in JeecgBoot up to 3.8.2. Impacted is an unknown function of the file /sys/tenant/deleteBatch. The manipulation of the argument ids leads to improper authorization. The attack is possible to be carried out remotely. The complexity of an attack is rather high. The exploitability is considered difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2025-10976	A vulnerability was determined in JeecgBoot up to 3.8.2. This issue affects some unknown processing of the file /api/getDepartUserList. Executing manipulation of the argument departId can lead to improper authorization. The attack can be executed remotely. This attack is characterized by high complexity. The exploitability is assessed as difficult. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2025-10173	The ShopEngine Elementor WooCommerce Builder Addon – All in One WooCommerce Solution plugin for WordPress is vulnerable to unauthorized access due to an incorrect capability check on the post_save() function in all versions up to, and including, 4.8.3. This makes it possible for authenticated attackers, with Editor-level access and above, to update the plugin's settings.	2.7	More Details
CVE-2025-23273	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in nvJPEG where a local authenticated user may cause a divide by zero error by submitting a specially crafted JPEG file. A successful exploit of this vulnerability may lead to denial of service.	2.5	More Details
CVE-2025-11027	A vulnerability was identified in givanz Vvveb up to 1.0.7.2. Affected by this issue is some unknown functionality of the component SVG File Handler. Such manipulation leads to cross site scripting. The attack may be launched remotely. The exploit is publicly available and might be used. Once again the project maintainer reacted very professional: "I accept the existence of these vulnerabilities. (...) I fixed the code to remove these vulnerabilities and will push the code to github and make a new release."	2.4	More Details
CVE-2025-11069	A vulnerability was determined in westboy CicadasCMS 1.0. Affected by this issue is some unknown functionality of the file /system/org/save of the component Add Department Handler. This manipulation of the argument Name causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	2.4	More Details
CVE-2025-11068	A vulnerability was found in westboy CicadasCMS 1.0. Affected by this vulnerability is an unknown functionality of the file /system/cms/category/save. The manipulation of the argument categoryName results in cross site scripting. The attack can be executed remotely. The exploit has been made public and could be used.	2.4	More Details
CVE-2025-11067	A vulnerability has been found in Projectworlds Visitor Management System 1.0. Affected is an unknown function of the file /myform.php of the component Add Visitor Page. The manipulation of the argument Name leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2025-11134	A security vulnerability has been detected in Cudy TR1200 1.16.3-20230804-164635. Impacted is an unknown function of the file /cgi-bin/luci/admin/network/wireless/config/ of the component Wireless Settings Page. Such manipulation of the argument SSID leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-10940	A vulnerability was found in Total.js CMS 1.0.0. Affected by this vulnerability is the function layouts_save of the file /admin/ of the component Layout Page. Performing manipulation of the argument HTML results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-	A vulnerability has been found in Total.js CMS up to 19.9.0. This impacts an unknown function of the		More

2025- 11019	component Files Menu. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2025-10909	A security flaw has been discovered in Mangati NovoSGA up to 2.2.9. The impacted element is an unknown function of the file /admin of the component SVG File Handler. Performing manipulation of the argument logoNavbar/logoLogin results in cross site scripting. Remote exploitation of the attack is possible. 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.	2.4	More Details
CVE-2025-23291	NVIDIA Delegated Licensing Service for all appliance platforms contains a vulnerability where an User/Attacker may cause an authorized action. A successful exploit of this vulnerability may lead to information disclosure.	2.4	More Details
CVE-2025-10949	A vulnerability was found in Changsha Developer Technology iView Editor up to 1.1.1. This impacts an unknown function of the component Markdown Handler. The manipulation results in cross site scripting. The attack may be performed from remote. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-41095	Insecure Direct Object Reference (IDOR) vulnerability in BOLD Workplanner in versions prior to 2.5.25 (4935b438f9b), consisting of a lack of adequate validation of user input, allowing an authenticated user to access to planning counter details using unauthorised internal identifiers.	N/A	More Details
CVE-2025-41096	Insecure Direct Object Reference (IDOR) vulnerability in BOLD Workplanner in versions prior to 2.5.25 (4935b438f9b), consisting of a lack of adequate validation of user input, allowing an authenticated user to access to the dates of the current contract details using unauthorised internal identifiers.	N/A	More Details
CVE-2025-10991	The attacker may obtain root access by connecting to the UART port and this vulnerability requires the attacker to have the physical access to the device. This issue affects Tapo D230S1 V1.20: before 1.2.2 Build 20250907.	N/A	More Details
CVE-2025-61633	Rejected reason: Not used	N/A	More Details
CVE-2025-61632	Rejected reason: Not used	N/A	More Details
CVE-2025-61631	Rejected reason: Not used	N/A	More Details
CVE-2025-61630	Rejected reason: Not used	N/A	More Details
CVE-2025-61629	Rejected reason: Not used	N/A	More Details
CVE-2025-61628	Rejected reason: Not used	N/A	More Details
CVE-2025-61627	Rejected reason: Not used	N/A	More Details
CVE-2025-61626	Rejected reason: Not used	N/A	More Details
CVE-2023-47538	Rejected reason: Not used	N/A	More Details
CVE-2025-61584	serverless-dns is a RethinkDNS resolver that deploys to Cloudflare Workers, Deno Deploy, Fastly, and Fly.io. Versions through abd including 0.1.30 have a vulnerability where the pr.yml GitHub Action interpolates in an unsafe manner untrusted input, specifically the github.event.pull_request.head.repo.clone_url and github.head_ref, to a command in the runner. Due to the action using the pull_request_target trigger it has permissive permissions by default. An unauthorized	N/A	More Details

01584	attacker can exploit this vulnerability to push arbitrary data to the repository. The subsequent impact on the end-user is executing the attackers' code when running serverless-dns. This is fixed in commit c5537dd, and expected to be released in 0.1.31.		
CVE-2025-41091	Insecure Direct Object Reference (IDOR) vulnerability in BOLD Workplanner in versions prior to 2.5.25 (4935b438f9b), consisting of a lack of adequate validation of user input, allowing an authenticated user to access to calendar details using unauthorised internal identifiers.	N/A	More Details
CVE-2025-59927	Rejected reason: Not used	N/A	More Details
CVE-2025-43826	Stored cross-site scripting (XSS) vulnerabilities in Web Content translation in Liferay Portal 7.4.0 through 7.4.3.112, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.8, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and older unsupported versions allow remote attackers to inject arbitrary web script or HTML via any rich text field in a web content article.	N/A	More Details
CVE-2025-57254	An SQL injection vulnerability in user-login.php and index.php of Karthikg1908 Hospital Management System (HMS) 1.0 allows remote attackers to execute arbitrary SQL queries via the username and password POST parameters. The application fails to properly sanitize input before embedding it into SQL queries, leading to unauthorized access or potential data breaches. This can result in privilege escalation, account takeover, or exposure of sensitive medical data.	N/A	More Details
CVE-2025-56513	NiceHash QuickMiner 6.12.0 perform software updates over HTTP without validating digital signatures or hash checks. An attacker capable of intercepting or redirecting traffic to the update url and can hijack the update process and deliver arbitrary executables that are automatically executed, resulting in full remote code execution. This constitutes a critical supply chain attack vector.	N/A	More Details
CVE-2025-41092	Insecure Direct Object Reference (IDOR) vulnerability in BOLD Workplanner in versions prior to 2.5.25 (4935b438f9b), consisting of a lack of adequate validation of user input, allowing an authenticated user to access to time records details using unauthorised internal identifiers.	N/A	More Details
CVE-2025-59926	Rejected reason: Not used	N/A	More Details
CVE-2025-59954	Knowage is an open source analytics and business intelligence suite. Versions 8.1.26 and below are vulnerable to Remote Code Exection through using an unsafe org.apache.commons.jxpath.JXPathContext in MetaService.java service. This issue is fixed in version 8.1.27.	N/A	More Details
CVE-2025-10360	In Puppet Enterprise versions 2025.4.0 and 2025.5, the encryption key used for encrypting content in the Infra Assistant database was not excluded from the files gathered by Puppet backup. The key is only present on the system if the user has a Puppet Enterprise Advanced license and has enabled the Infra Assistant feature. The key is used for encrypting one particular bit of data in the Infra Assistant database: the API key for their AI provider account. This has been fixed in Puppet Enterprise version 2025.6, and release notes for 2025.6 have remediation steps for users of affected versions who can't update to the latest version.	N/A	More Details
CVE-2025-41099	Insecure Direct Object Reference (IDOR) vulnerability in BOLD Workplanner in versions prior to 2.5.25 (4935b438f9b), consisting of a lack of adequate validation of user input, allowing an authenticated user to access to the list of permissions using unauthorised internal identifiers.	N/A	More Details
CVE-2025-41093	Insecure Direct Object Reference (IDOR) vulnerability in BOLD Workplanner in versions prior to 2.5.25 (4935b438f9b), consisting of a lack of adequate validation of user input, allowing an authenticated user to access to basic contract details using unauthorised internal identifiers.	N/A	More Details
CVE-2025-41098	Insecure Direct Object Reference (IDOR) vulnerability in BOLD Workplanner in versions prior to 2.5.25 (4935b438f9b), consisting of a misuse of the general enquiry web service.	N/A	More Details
CVE-2025-41094	Insecure Direct Object Reference (IDOR) vulnerability in BOLD Workplanner in versions prior to 2.5.25 (4935b438f9b), consisting of a lack of adequate validation of user input, allowing an authenticated user to access to functional contract details using unauthorised internal identifiers.	N/A	More Details
CVE-2025-41097	Insecure Direct Object Reference (IDOR) vulnerability in BOLD Workplanner in versions prior to 2.5.25 (4935b438f9b), consisting of a lack of adequate validation of user input, allowing an authenticated user to access to basic employee details using unauthorised internal identifiers.	N/A	More Details
CVE-2025-59668	Multiple versions of Central Monitor CNS-6201 contain a NULL pointer dereference vulnerability. When processing a crafted certain UDP packet, the affected device may abnormally terminate.	N/A	More Details

CVE-2025-11153	This vulnerability affects Firefox < 143.0.3.	N/A	More Details
CVE-2025-7063	Due to client-controlled permission check parameter, PAD CMS's file upload functionality allows an unauthenticated remote attacker to upload files of any type and extension without restriction, which can then be executed leading to Remote Code Execution. This issue affects all 3 templates: www, bip and ww+bip. This product is End-Of-Life and producent will not publish patches for this vulnerability.	N/A	More Details
CVE-2025-56392	An Insecure Direct Object Reference (IDOR) in the /dashboard/notes endpoint of Syaqui Collegetivity v1.0.0 allows attackers to impersonate other users and perform arbitrary operations via a crafted POST request.	N/A	More Details
CVE-2025-55797	An improper access control vulnerability in FormCms v0.5.4 in the /api/schemas/history/[schemaId] endpoint allows unauthenticated attackers to access historical schema data if a valid schemaId is known or guessed.	N/A	More Details
CVE-2025-56132	LiquidFiles filetransfer server is vulnerable to a user enumeration issue in its password reset functionality. The application returns distinguishable responses for valid and invalid email addresses, allowing unauthenticated attackers to determine the existence of user accounts. Version 4.2 introduces user-based lockout mechanisms to mitigate brute-force attacks, user enumeration remains possible by default. In versions prior to 4.2, no such user-level protection is in place, only basic IP-based rate limiting is enforced. This IP-based protection can be bypassed by distributing requests across multiple IPs (e.g., rotating IP or proxies). Effectively bypassing both login and password reset security controls. Successful exploitation allows an attacker to enumerate valid email addresses registered for the application, increasing the risk of follow-up attacks such as password spraying.	N/A	More Details
CVE-2025-54476	Improper handling of input could lead to an XSS vector in the checkAttribute method of the input filter framework class.	N/A	More Details
CVE-2025-7779	Local privilege escalation due to insecure XPC service configuration. The following products are affected: Acronis True Image (macOS) before build 42389, Acronis True Image for SanDisk (macOS) before build 42198, Acronis True Image for Western Digital (macOS) before build 42197.	N/A	More Details
CVE-2025-56301	An issue was discovered in Chipsalliance Rocket-Chip commit f517abbf41abb65cea37421d3559f9739efd00a9 (2025-01-29) allowing attackers to corrupt exception handling and privilege state transitions via a flawed interaction between exception handling and MRET return mechanisms in the CSR logic when an exception is triggered during MRET execution. The Control and Status Register (CSR) logic has a flawed interaction between exception handling and exception return (MRET) mechanisms which can cause faulty trap behavior. When the MRET instruction is executed in machine mode without being in an exception state, an Instruction Access Fault may be triggered. This results in both the exception handling logic and the exception return logic activating simultaneously, leading to conflicting updates to the control and status registers.	N/A	More Details
CVE-2022-40285	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2024-13967. Reason: This record is a reservation duplicate of CVE-2024-13967. Notes: All CVE users should reference CVE-2024-13967 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-11178	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis True Image (Windows) before build 42386.	N/A	More Details
CVE-2025-56571	Finance.js v4.1.0 contains a Denial of Service (DoS) vulnerability via the IRR function’s depth parameter. Improper handling of the recursion/iteration limit can lead to excessive CPU usage, causing application stalls or crashes.	N/A	More Details
CVE-2025-59925	Rejected reason: Not used	N/A	More Details
CVE-2024-58241	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_core: Disable works on hci_unregister_dev This make use of disable_work_* on hci_unregister_dev since the hci_dev is about to be freed new submissions are not disarable.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: l2cap: Check encryption key size on incoming connection This is required for passing GAP/SEC/SEM/BI-04-C PTS test case: Security Mode 4 Level 4, Responder - Invalid Encryption Key Size - 128 bit This tests the security key with size		

CVE-2025-39889	from 1 to 15 bytes while the Security Mode 4 Level 4 requests 16 bytes key size. Currently PTS fails with the following logs: - expected:Connection Response: Code: [3 (0x03)] Code Identifier: (lt)WildCard: Exists(gt) Length: [8 (0x0008)] Destination CID: (lt)WildCard: Exists(gt) Source CID: [64 (0x0040)] Result: [3 (0x0003)] Connection refused - Security block Status: (lt)WildCard: Exists(gt), but received:Connection Response: Code: [3 (0x03)] Code Identifier: [1 (0x01)] Length: [8 (0x0008)] Destination CID: [64 (0x0040)] Source CID: [64 (0x0040)] Result: [0 (0x0000)] Connection Successful Status: [0 (0x0000)] No further information available And HCI logs: < HCI Command: Read Encrypti.. (0x05|0x0008) plen 2 Handle: 14 Address: 00:1B:DC:F2:24:10 (Vencer Co., Ltd.) > HCI Event: Command Complete (0x0e) plen 7 Read Encryption Key Size (0x05|0x0008) ncmd 1 Status: Success (0x00) Handle: 14 Address: 00:1B:DC:F2:24:10 (Vencer Co., Ltd.) Key size: 7 > ACL Data RX: Handle 14 flags 0x02 dlen 12 L2CAP: Connection Request (0x02) ident 1 len 4 PSM: 4097 (0x1001) Source CID: 64 < ACL Data TX: Handle 14 flags 0x00 dlen 16 L2CAP: Connection Response (0x03) ident 1 len 8 Destination CID: 64 Source CID: 64 Result: Connection successful (0x0000) Status: No further information available (0x0000)	N/A	More Details
CVE-2025-10217	A vulnerability exists in Asset Suite for an authenticated user to manipulate the content of performance related log data or to inject crafted data in logfile for potentially carrying out further malicious attacks. Performance logging is typically enabled for troubleshooting purposes while resolving application performance related issues.	N/A	More Details
CVE-2025-39890	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix memory leak in ath12k_service_ready_ext_event Currently, in ath12k_service_ready_ext_event(), svc_rdy_ext.mac_phy_caps is not freed in the failure case, causing a memory leak. The following trace is observed in kmemleak: unreferenced object 0xffff8b3eb5789c00 (size 1024): comm "softirq", pid 0, jiffies 4294942577 hex dump (first 32 bytes): 00 00 00 00 01 00 00 00 00 00 00 00 7b 00 00 10 ..... {... 01 00 00 00 00 00 00 00 01 00 00 00 1f 38 00 00 .....8.. backtrace (crc 44e1c357): __kmalloc_noprof+0x30b/0x410 ath12k_wmi_mac_phy_caps_parse+0x84/0x100 [ath12k] ath12k_wmi_tlv_iter+0x5e/0x140 [ath12k] ath12k_wmi_svc_rdy_ext_parse+0x308/0x4c0 [ath12k] ath12k_wmi_tlv_iter+0x5e/0x140 [ath12k] ath12k_service_ready_ext_event.isra.0+0x44/0xd0 [ath12k] ath12k_wmi_op_rx+0x2eb/0xd70 [ath12k] ath12k_htc_rx_completion_handler+0x1f4/0x330 [ath12k] ath12k_ce_recv_process_cb+0x218/0x300 [ath12k] ath12k_pci_ce_workqueue+0x1b/0x30 [ath12k] process_one_work+0x219/0x680 bh_worker+0x198/0x1f0 tasklet_action+0x13/0x30 handle_softirqs+0xca/0x460 __irq_exit_rcu+0xbe/0x110 irq_exit_rcu+0x9/0x30 Free svc_rdy_ext.mac_phy_caps in the error case to fix this memory leak. Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.4.1-00199-QCAHKSWPL_SILICONZ-1	N/A	More Details
CVE-2025-11152	This vulnerability affects Firefox < 143.0.3.	N/A	More Details
CVE-2025-59930	Rejected reason: Not used	N/A	More Details
CVE-2025-56572	An issue in finance.js v.4.1.0 allows a remote attacker to cause a denial of service via the seekZero() parameter.	N/A	More Details
CVE-2025-7065	Due to client-controlled permission check parameter, PAD CMS's photo upload functionality allows an unauthenticated remote attacker to upload files of any type and extension without restriction, which can then be executed leading to Remote Code Execution. This issue affects all 3 templates: www, bip and ww+bip. This product is End-Of-Life and producent will not publish patches for this vulnerability.	N/A	More Details
CVE-2025-8122	Improper neutralization of input provided by an authorized user in article positioning functionality allows for Blind SQL Injection attacks. This issue affects all 3 templates: www, bip and ww+bip. This product is End-Of-Life and producent will not publish patches for this vulnerability.	N/A	More Details
CVE-2025-8116	PAD CMS is vulnerable to Reflected XSS in printing and save to PDF functionality. Malicious attacker can craft special URL, which will result in arbitrary JavaScript execution in victim's browser, when opened. This issue affects all 3 templates: www, bip and www+bip. This product is End-Of-Life and producent will not publish patches for this vulnerability.	N/A	More Details
CVE-2025-8117	PAD CMS improperly initializes parameter used for password recovery, which allows to change password for any user that did not use reset password functionality. This issue affects all 3 templates: www, bip and www+bip. This product is End-Of-Life and producent will not publish patches for this vulnerability.	N/A	More Details
CVE-2025-8118	PAD CMS implements weak client-side brute-force protection by utilizing two cookies: login_count and login_timeout. Information about attempt count or timeout is not stored on the server, which allows a malicious attacker to bypass this brute-force protection by resetting those cookies. This issue affects all 3 templates: www, bip and www+bip. This product is End-Of-Life and producent will not publish patches for	N/A	More Details

	this vulnerability.		
CVE-2025-34217	Vasion Print (formerly PrinterLogic) Virtual Appliance Host and Application (VA/SaaS deployments) contain an undocumented 'printerlogic' user with a hardcoded SSH public key in '~/.ssh/authorized_keys' and a sudoers rule granting the printerlogic_ssh group 'NOPASSWD: ALL'. Possession of the matching private key gives an attacker root access to the appliance.	N/A	More Details
CVE-2025-8120	Due to client-controlled permission check parameter, PAD CMS's upload photo functionality allows an unauthenticated remote attacker to upload files of any type and extension without restriction, which can then be executed leading to Remote Code Execution.This issue affects all 3 templates: www, bip and ww+bip. This product is End-Of-Life and producent will not publish patches for this vulnerability.	N/A	More Details
CVE-2025-8121	Improper neutralization of input provided by an authorized user in article positioning functionality allows for Blind SQL Injection attacks. This issue affects all 3 templates: www, bip and ww+bip. This product is End-Of-Life and producent will not publish patches for this vulnerability.	N/A	More Details
CVE-2025-8869	When extracting a tar archive pip may not check symbolic links point into the extraction directory if the tarfile module doesn't implement PEP 706. Note that upgrading pip to a "fixed" version for this vulnerability doesn't fix all known vulnerabilities that are remediated by using a Python version that implements PEP 706. Note that this is a vulnerability in pip's fallback implementation of tar extraction for Python versions that don't implement PEP 706 and therefore are not secure to all vulnerabilities in the Python 'tarfile' module. If you're using a Python version that implements PEP 706 then pip doesn't use the "vulnerable" fallback code. Mitigations include upgrading to a version of pip that includes the fix, upgrading to a Python version that implements PEP 706 (Python >=3.9.17, >=3.10.12, >=3.11.4, or >=3.12), applying the linked patch, or inspecting source distributions (sdists) before installation as is already a best-practice.	N/A	More Details
CVE-2025-56676	TitanSystems Zender v3.9.7 contains an account takeover vulnerability in its password reset functionality. A temporary password or reset token issued to one user can be used to log in as another user, due to improper validation of token-user linkage. This allows remote attackers to gain unauthorized access to any user account by exploiting the password reset mechanism. The vulnerability occurs because the reset token is not correctly bound to the requesting account and is accepted for other user emails during login, enabling privilege escalation and information disclosure.	N/A	More Details
CVE-2025-43827	Insecure Direct Object Reference (IDOR) vulnerability with audit events in Liferay Portal 7.4.0 through 7.4.3.117, and older unsupported versions, and Liferay DXP 2024.Q1.1 through 2024.Q1.5, 2023.Q4.0 through 2023.Q4.10, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and older unsupported versions allows remote authenticated users to from one virtual instance to view the audit events from a different virtual instance via the _com_liferay_portal_security_audit_web_portlet_AuditPortlet_auditEventId parameter.	N/A	More Details
CVE-2025-56520	Dify v1.6.0 was discovered to contain a Server-Side Request Forgery (SSRF) via the component controllers.console.remote_files.RemoteFileUploadApi. A different vulnerability than CVE-2025-29720.	N/A	More Details
CVE-2025-56207	A security flaw in the '_transfer' function of a smart contract implementation for Money Making Opportunity (MMO), an Ethereum ERC721 Non-Fungible Token (NFT) project, allows users or attackers to transfer NFTs to the zero address, leading to permanent asset loss and non-compliance with the ERC721 standard. The eth address is 0x41d3d86a84c8507a7bc14f2491ec4d188fa944e7, contract name is MoneyMakingOpportunity, and compiler version is v0.8.17+commit.8df45f5f.	N/A	More Details
CVE-2025-59924	Rejected reason: Not used	N/A	More Details
CVE-2025-59928	Rejected reason: Not used	N/A	More Details
CVE-2025-59929	Rejected reason: Not used	N/A	More Details
CVE-2025-8119	PAD CMS is vulnerable to Cross-Site Request Forgery in reset password's functionality. Malicious attacker can craft special website, which when visited by the victim, will automatically send a POST request changing currently logged user's password to defined by the attacker value. This issue affects all 3 templates: www, bip and www+bip. This product is End-Of-Life and producent will not publish patches for this vulnerability.	N/A	More Details
	A security vulnerability was identified in Obsidian Scheduler's REST API 5.0.0 thru 6.3.0. If an account is locked out due to not enrolling in MFA (e.g. after the 7-day enforcement window), the REST API still		

CVE-2025-56449	allows the use of Basic Authentication to authenticate and perform administrative actions. In particular, the default admin account was found to be locked out via the web interface but still usable through the REST API. This allowed creation of a new privileged user, bypassing MFA protections. This undermines the intended security posture of MFA enforcement.	N/A	More Details
CVE-2025-52906	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in TOTOLINK X6000R allows OS Command Injection.This issue affects X6000R: through V9.4.0cu.1360_B20241207.	N/A	More Details
CVE-2025-59831	git-commiters is a Node.js function module providing committers stats for their git repository. Prior to version 0.1.2, there is a command injection vulnerability in git-commiters. This vulnerability manifests with the library's primary exported API: gitCommiters(options, callback) which allows specifying options such as cwd for current working directory and revisionRange as a revision pointer, such as HEAD. However, the library does not sanitize for user input or practice secure process execution API to separate commands from their arguments and as such, uncontrolled user input is concatenated into command execution. This issue has been patched in version 0.1.2.	N/A	More Details
CVE-2025-10341	HTML injection vulnerability in Perfex CRM v3.2.1 consisting of a stored HTML injection due to lack of proper validation of user input by sending a POST request in the parameter 'company' at the endpoint '/clients/client/x.	N/A	More Details
CVE-2025-10342	HTML injection vulnerability in Perfex CRM v3.2.1 consisting of a stored HTML injection due to lack of proper validation of user input by sending a POST request in the parameter 'name' at the endpoint '/subscriptions/create'.	N/A	More Details
CVE-2025-10343	HTML injection vulnerability in Perfex CRM v3.2.1 consisting of a stored HTML injection due to lack of proper validation of user input by sending a POST request in the parameter 'expense_name' at the endpoint '/expenses/expense'.	N/A	More Details
CVE-2025-10344	HTML injection vulnerability in Perfex CRM v3.2.1 consisting of a stored HTML injection due to lack of proper validation of user input by sending a POST request in the parameters 'name' and 'clientid' at the endpoint '/projects/project/x'.	N/A	More Details
CVE-2025-10345	HTML injection vulnerability in Perfex CRM v3.2.1 consisting of a stored HTML injection due to lack of proper validation of user input by sending a POST request in the parameters 'name' and 'address' at the endpoint 'admin/leads/lead'.	N/A	More Details
CVE-2025-10346	HTML injection vulnerability in Perfex CRM v3.2.1 consisting of a stored HTML injection due to lack of proper validation of user input by sending a POST request in the parameters 'subject' at the endpoint 'knoewledge_base/article'.	N/A	More Details
CVE-2025-11146	Reflected Cross-site scripting (XSS) in Apt-Cacher-NG v3.2.1. The vulnerability allows an attacker to execute malicious scripts (XSS) in the web management application. The vulnerability is caused by improper handling of GET inputs included in the URL in “/acng-report.html”.	N/A	More Details
CVE-2025-11147	Reflected cross-site scripting (XSS) in Apt-Cacher-NG v3.2.1. The vulnerability allows malicious scripts (XSS) to be executed in “/html/<filename>.html”.	N/A	More Details
CVE-2025-11150	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-9648	A vulnerability in the CivetWeb library's function mg_handle_form_request allows remote attackers to trigger a denial of service (DoS) condition. By sending a specially crafted HTTP POST request containing a null byte in the payload, the server enters an infinite loop during form data parsing. Multiple malicious requests will result in complete CPU exhaustion and render the service unresponsive to further requests. This issue was fixed in commit 782e189. This issue affects only the library, standalone executable pre-built by vendor is not affected.	N/A	More Details
CVE-2025-57428	Default credentials in Italy Wireless Mini Router WIRELESS-N 300M v28K.MiniRouter.20190211 allows attackers to gain access to the debug shell exposed via Telnet on Port 23 and execute hardware-level flash and register manipulation commands.	N/A	More Details
CVE-2025-57516	OS Command injection vulnerability in PublicCMS PublicCMS-V5.202506.a, and PublicCMS-V5.202506.b allowing attackers to execute arbitrary commands via crafted DATABASE, USERNAME, or PASSWORD variables to the backupDB.bat file.	N/A	More Details
CVE-2025-	The credentials required to access the device's web server are sent in base64 within the HTTP headers. Since base64 is not considered a strong cipher, an attacker could intercept the web request handling the	N/A	More

11155	login and obtain the credentials.		Details
CVE-2025-40838	Ericsson Indoor Connect 8855 contains a vulnerability where server-side security can be bypassed in the client which if exploited can lead to unauthorized disclosure of certain information.	N/A	More Details
CVE-2024-57412	An issue in SunOS Omnios v5.11 allows attackers to cause a Denial of Service (DoS) via repeatedly sending crafted TCP packets.	N/A	More Details
CVE-2025-40837	Ericsson Indoor Connect 8855 contains a missing authorization vulnerability which if exploited can allow access to the system as a user with higher privileges than intended.	N/A	More Details
CVE-2025-40836	Ericsson Indoor Connect 8855 contains an improper input validation vulnerability which if exploited can allow an attacker to execute commands with escalated privileges.	N/A	More Details
CVE-2025-56233	Openindiana, kernel SunOS 5.11 has a denial of service vulnerability. For the processing of TCP packets with RST or SYN flag set, Openindiana has a wide acceptable range of sequence numbers. It does not require the sequence number to exactly match the next expected sequence value, just to be within the current receive window, which violates RFC5961. This flaw allows attackers to send multiple random TCP RST/SYN packets to hit the acceptable range of sequence numbers, thereby interrupting normal connections and causing a denial of service attack.	N/A	More Details
CVE-2025-56234	AT_NA2000 from Nanda Automation Technology vendor has a denial-of-service vulnerability. For the processing of TCP RST packets, PLC AT_NA2000 has a wide acceptable range of sequence numbers. It does not require the sequence number to exactly match the next expected sequence value, just to be within the current receive window, which violates RFC5961. This flaw allows attackers to send multiple random TCP RST packets to hit the acceptable range of sequence numbers, thereby interrupting normal connections and causing a denial-of-service attack.	N/A	More Details
CVE-2025-7104	A mass assignment vulnerability exists in danny-avila/librechat, affecting all versions. This vulnerability allows attackers to manipulate sensitive fields by automatically binding user-provided data to internal object properties or database fields without proper filtering. As a result, any extra fields in the request body are included in agentData and passed to the database layer, allowing overwriting of any field in the schema, such as author, access_level, isCollaborative, and projectIds. Additionally, the Object.Prototype can be polluted due to the use of Object.assign with spread operators.	N/A	More Details
CVE-2025-27262	Ericsson Indoor Connect 8855 contains a command injection vulnerability which if exploited can result in an escalation of privileges.	N/A	More Details
CVE-2025-48006	Improper restriction of XML external entity reference issue exists in DataSpider Servista 4.4 and earlier. If a specially crafted request is processed, arbitrary files on the file system where the server application for the product is installed may be read, or a denial-of-service (DoS) condition may occur.	N/A	More Details
CVE-2025-59823	Project Gardener implements the automated management and operation of Kubernetes clusters as a service. Code injection may be possible in Gardener Extensions for AWS providers prior to version 1.64.0, Azure providers prior to version 1.55.0, OpenStack providers prior to version 1.49.0, and GCP providers prior to version 1.46.0. This vulnerability could allow a user with administrative privileges for a Gardener project to obtain control over the seed cluster where the shoot cluster is managed. This affects all Gardener installations where Terraformer is used/can be enabled for infrastructure provisioning with any of the affected components. This issue has been patched in Gardener Extensions for AWS providers version 1.64.0, Azure providers version 1.55.0, OpenStack providers version 1.49.0, and GCP providers version 1.46.0.	N/A	More Details
CVE-2025-59838	Monkeytype is a minimalistic and customizable typing test. In versions 25.36.0 and prior, improper handling of user input when loading a saved custom text results in XSS. This issue has been patched via commit f025b12.	N/A	More Details
CVE-2025-7647	The llama-index-core package, up to version 0.12.44, contains a vulnerability in the `get_cache_dir()` function where a predictable, hardcoded directory path `/tmp/llama_index` is used on Linux systems without proper security controls. This vulnerability allows attackers on multi-user systems to steal proprietary models, poison cached embeddings, or conduct symlink attacks. The issue affects all Linux deployments where multiple users share the same system. The vulnerability is classified under CWE-379, CWE-377, and CWE-367, indicating insecure temporary file creation and potential race conditions.	N/A	More Details
CVE-2025-	A Insufficient Session Expiration vulnerability in the Liferay Portal 7.4.3.121 through 7.3.3.131, and Liferay DXP 2024.Q4.0 through 2024.Q4.3, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through	N/A	More

43819	2024.Q2.13, and 2024.Q1.1 through 2024.Q1.12 is allow an remote non-authenticated attacker to reuse old user session by SLO API		Details
CVE-2025-10544	Unrestricted file upload vulnerability in DocAve 6.13.2, Perimeter 1.12.3, Compliance Guardian 4.7.1, and earlier versions, allowing administrator users to upload files without proper validation. An attacker could exploit this vulnerability by uploading malicious files that compromise the system. In addition, it is vulnerable to Path Traversal, which allows files to be written to arbitrary directories within the web root.	N/A	More Details
CVE-2025-9267	In Seagate Toolkit on Windows a vulnerability exists in the Toolkit Installer prior to versions 2.35.0.6 where it attempts to load DLLs from the current working directory without validating their origin or integrity. This behavior can be exploited by placing a malicious DLL in the same directory as the installer executable, leading to arbitrary code execution with the privileges of the user running the installer. The issue stems from the use of insecure DLL loading practices, such as relying on relative paths or failing to specify fully qualified paths when invoking system libraries.	N/A	More Details
CVE-2025-59842	jupyterlab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook Architecture. Prior to version 4.4.8, links generated with LaTeX typesetters in Markdown files and Markdown cells in JupyterLab and Jupyter Notebook did not include the noopener attribute. This is deemed to have no impact on the default installations. Theoretically users of third-party LaTeX-rendering extensions could find themselves vulnerable to reverse tabnabbing attacks if links generated by those extensions included target=_blank (no such extensions are known at time of writing) and they were to click on a link generated in LaTeX (typically visibly different from other links). This issue has been patched in version 4.4.8.	N/A	More Details
CVE-2025-59843	Flag Forge is a Capture The Flag (CTF) platform. From versions 2.0.0 to before 2.3.1, the public endpoint /api/user/[username] returns user email addresses in its JSON response. The problem has been patched in FlagForge version 2.3.1. The fix removes email addresses from public API responses while keeping the endpoint publicly accessible. Users should upgrade to version 2.3.1 or later to eliminate exposure. There are no workarounds for this vulnerability.	N/A	More Details
CVE-2025-59844	SonarQube Server and Cloud is a static analysis solution for continuous code quality and security inspection. A command injection vulnerability exists in SonarQube GitHub Action in version 4.0.0 to before version 6.0.0 when workflows pass user-controlled input to the args parameter on Windows runners without proper validation. This vulnerability bypasses a previous security fix and allows arbitrary command execution, potentially leading to exposure of sensitive environment variables and compromise of the runner environment. The vulnerability has been fixed in version 6.0.0. Users should upgrade to this version or later.	N/A	More Details
CVE-2025-50879	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2025-10657	In a hardened Docker environment, with Enhanced Container Isolation (ECI https://docs.docker.com/enterprise/security/hardened-desktop/enhanced-container-isolation/) enabled, an administrator can utilize the command restrictions feature https://docs.docker.com/enterprise/security/hardened-desktop/enhanced-container-isolation/config/#command-restrictions to restrict commands that a container with a Docker socket mount may issue on that socket. Due to a software bug, the configuration to restrict commands was ignored when passed to ECI, allowing any command to be executed on the socket. This grants excessive privileges by permitting unrestricted access to powerful Docker commands. The vulnerability affects only Docker Desktop 4.46.0 users that have ECI enabled and are using the Docker socket command restrictions feature. In addition, since ECI restricts mounting the Docker socket into containers by default, it only affects containers which are explicitly allowed by the administrator to mount the Docker socket.	N/A	More Details
CVE-2025-59936	get-jwks contains fetch utils for JWKS keys. In versions prior to 11.0.2, a vulnerability in get-jwks can lead to cache poisoning in the JWKS key-fetching mechanism. When the iss (issuer) claim is validated only after keys are retrieved from the cache, it is possible for cached keys from an unexpected issuer to be reused, resulting in a bypass of issuer validation. This design flaw enables a potential attack where a malicious actor crafts a pair of JWTs, the first one ensuring that a chosen public key is fetched and stored in the shared JWKS cache, and the second one leveraging that cached key to pass signature validation for a targeted iss value. The vulnerability will work only if the iss validation is done after the use of get-jwks for keys retrieval. This issue has been patched in version 11.0.2.	N/A	More Details
CVE-2025-60033	Rejected reason: Not used	N/A	More Details
CVE-2025-34227	Nagios XI < 2026R1 is vulnerable to an authenticated command injection vulnerability within the MongoDB Database, MySQL Query, MySQL Server, Postgres Server, and Postgres Query wizards. It is possible to inject shell characters into arguments provided to the service and execute arbitrary system commands on the underlying host as the `nagios` user.	N/A	More Details

CVE-2025-60032	Rejected reason: Not used	N/A	More Details
CVE-2025-60031	Rejected reason: Not used	N/A	More Details
CVE-2025-60030	Rejected reason: Not used	N/A	More Details
CVE-2025-60029	Rejected reason: Not used	N/A	More Details
CVE-2025-60028	Rejected reason: Not used	N/A	More Details
CVE-2025-60027	Rejected reason: Not used	N/A	More Details
CVE-2025-60026	Rejected reason: Not used	N/A	More Details
CVE-2025-11005	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in TOTOLINK X6000R allows OS Command Injection.This issue affects X6000R: through V9.4.0cu.1458_B20250708.	N/A	More Details
CVE-2025-43816	A memory leak in the headless API for StructuredContents in Liferay Portal 7.4.0 through 7.4.3.119, and older unsupported versions, and Liferay DXP 2024.Q1.1 through 2024.Q1.5, 2023.Q4.0 through 2024.Q4.10, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and older unsupported versions allows an attacker to cause server unavailability (denial of service) via repeatedly calling the API endpoint.	N/A	More Details
CVE-2020-36851	Rob -- W / cors-anywhere instances configured as an open proxy allow unauthenticated external users to induce the server to make HTTP requests to arbitrary targets (SSRF). Because the proxy forwards requests and headers, an attacker can reach internal-only endpoints and link-local metadata services, retrieve instance role credentials or other sensitive metadata, and interact with internal APIs and services that are not intended to be internet-facing. The vulnerability is exploitable by sending crafted requests to the proxy with the target resource encoded in the URL; many cors-anywhere deployments forward arbitrary methods and headers (including PUT), which can permit exploitation of IMDSv2 workflows as well as access to internal management APIs. Successful exploitation can result in theft of cloud credentials, unauthorized access to internal services, remote code execution or privilege escalation (depending on reachable backends), data exfiltration, and full compromise of cloud resources. Mitigation includes: restricting the proxy to trusted origins or authentication, whitelisting allowed target hosts, preventing access to link-local and internal IP ranges, removing support for unsafe HTTP methods/headers, enabling cloud provider mitigations, and deploying network-level protections.	N/A	More Details
CVE-2025-34196	Vasion Print (formerly PrinterLogic) Virtual Appliance Host versions prior to 25.1.102 and Application prior to 25.1.1413 (Windows client deployments) contain a hardcoded private key for the PrinterLogic Certificate Authority (CA) and a hardcoded password in product configuration files. The Windows client ships the CA certificate and its associated private key (and other sensitive settings such as a configured password) directly in shipped configuration files (for example clientsettings.dat and defaults.ini). An attacker who obtains these files can impersonate the CA, sign arbitrary certificates trusted by the Windows client, intercept or decrypt TLS-protected communications, and otherwise perform man-in-the-middle or impersonation attacks against the product's network communications.	N/A	More Details
CVE-2025-52907	Improper Input Validation vulnerability in TOTOLINK X6000R allows Command Injection, File Manipulation.This issue affects X6000R: through V9.4.0cu.1360_B20241207.	N/A	More Details
CVE-2025-59422	Dify is an open-source LLM app development platform. In version 1.8.1, a broken access control vulnerability on the /console/api/apps/<APP_ID>chat-messages?conversation_id=<CONVERSATION_ID>&limit=10 endpoint allows users in the same workspace to read chat messages of other users. A regular user is able to read the query data and the filename of the admins and probably	N/A	More Details

	other users chats, if they know the conversation_id. This impacts the confidentiality of chats. This issue has been patched in version 1.9.0.		
CVE-2025-10957	This vulnerability exists in the Syrotech SY-GPON-2010-WADONT router due to improper access control in its FTP service. A remote attacker could exploit this vulnerability by establishing an FTP connection using default credentials, potentially gaining unauthorized access to configuration files, user credentials, or other sensitive information stored on the targeted device.	N/A	More Details
CVE-2025-43811	Multiple stored cross-site scripting (XSS) vulnerability in the related asset selector in Liferay Portal 7.4.3.50 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.4, 2023.Q3.1 through 2023.Q3.7, and 7.4 update 50 through update 92 allows remote authenticated attackers to inject arbitrary web script or HTML via a crafted payload injected into an asset author’s (1) First Name, (2) Middle Name, or (3) Last Name text field.	N/A	More Details
CVE-2025-43815	Reflected cross-site scripting (XSS) vulnerability on the page configuration page in Liferay Portal 7.4.3.102 through 7.4.3.110, and Liferay DXP 2023.Q4.0 through 2023.Q4.2, and 2023.Q3.5 allows remote attackers to inject arbitrary web script or HTML via the com_liferay_layout_admin_web_portlet_GroupPagesPortlet_backURLTitle parameter.	N/A	More Details
CVE-2025-43818	Cross-site scripting (XSS) vulnerability in the Calendar widget in Liferay Portal 7.4.3.35 through 7.4.3.110, and Liferay DXP 2023.Q4.0 through 2023.Q4.4, 2023.Q3.1 through 2023.Q3.6, 7.4 update 35 through update 92, and 7.3 update 25 through update 36 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a Calendar's “Name” text field	N/A	More Details
CVE-2025-43820	Multiple cross-site scripting (XSS) vulnerabilities in the Calendar widget when inviting users to a event in Liferay Portal 7.4.3.35 through 7.4.3.110, and Liferay DXP 2023.Q4.0 through 2023.Q4.4, 2023.Q3.1 through 2023.Q3.6, 7.4 update 35 through update 92, and 7.3 update 25 through update 35 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a user’s (1) First Name, (2) Middle text, or (3) Last Name text fields.	N/A	More Details
CVE-2025-54592	FreshRSS is a free, self-hostable RSS aggregator. Versions 1.26.3 and below do not properly terminate the session during logout. After a user logs out, the session cookie remains active and unchanged. The unchanged cookie could be reused by an attacker if a new session were to be started. This failure to invalidate the session can lead to session hijacking and fixation vulnerabilities. This issue is fixed in version 1.27.0	N/A	More Details
CVE-2025-57769	FreshRSS is a free, self-hostable RSS aggregator. Versions 1.26.3 and below contain a vulnerability where a specially crafted page can trick a user into executing arbitrary JS code or promoting a user in FreshRSS by obscuring UI elements in iframes. If embedding an authenticated iframe is possible, this may lead to privilege escalation via obscuring the promote user button in the admin UI or XSS by tricking the user to drag content into the UserJS text area. This is fixed in version 1.27.0	N/A	More Details
CVE-2025-59163	vet is an open source software supply chain security tool. Versions 1.12.4 and below are vulnerable to a DNS rebinding attack due to lack of HTTP Host and Origin header validation. Data from the vet scan sqlite3 database may be exposed to remote attackers when vet is used as an MCP server in SSE mode with default ports through the sqlite3 query MCP tool. This issue is fixed in version 1.12.5.	N/A	More Details
CVE-2025-59933	libvips is a demand-driven, horizontally threaded image processing library. For versions 8.17.1 and below, when libvips is compiled with support for PDF input via poppler, the pdfload operation is affected by a buffer read overflow when parsing the header of a crafted PDF with a page that defines a width but not a height. Those using libvips compiled without support for PDF input are unaffected as well as thosewith support for PDF input via PDFium. This issue is fixed in version 8.17.2. A workaround for those affected is to block the VipsForeignLoadPdf operation via vips_operation_block_set, which is available in most language bindings, or to set VIPS_BLOCK_UNTRUSTED environment variable at runtime, which will block all untrusted loaders including PDF input via poppler.	N/A	More Details
CVE-2025-43812	Cross-site scripting (XSS) vulnerability in web content template in Liferay Portal 7.4.3.4 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.4, 2023.Q3.1 through 2023.Q3.8, and 7.4 GA through update 92 allows remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into a web content structure's Name text field	N/A	More Details
CVE-2025-43813	Possible path traversal vulnerability and denial-of-service in the ComboServlet in Liferay Portal 7.4.0 through 7.4.3.107, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.4, 2023.Q3.1 through 2023.Q3.8, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions allows remote attackers to access arbitrary CSS and JSS files and load the files multiple times via the query string in a URL.	N/A	More Details
CVE-2025-43817	Multiple reflected cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.4.3.74 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.6, 2023.Q3.1 through 2023.Q3.8, and 7.4 update 74 through update 92 allow remote attackers to inject arbitrary web script or HTML via the `redirect`	N/A	More Details

	parameter to (1) Announcements, or (2) Alerts.		
CVE-2025-59937	go-mail is a comprehensive library for sending mails with Go. In versions 0.7.0 and below, due to incorrect handling of the mail.Address values when a sender- or recipient address is passed to the corresponding MAIL FROM or RCPT TO commands of the SMTP client, there is a possibility of wrong address routing or even ESMTP parameter smuggling. For successful exploitation, it is required that the user's code allows for arbitrary mail address input (i. e. through a web form or similar). If only static mail addresses are used (i. e. in a config file) and the mail addresses in use do not consist of quoted local parts, this should not affect users. This issue is fixed in version 0.7.1	N/A	More Details
CVE-2025-54520	Improper Protection Against Voltage and Clock Glitches in FPGA devices, could allow an attacker with physical access to undervolt the platform resulting in a loss of confidentiality.	N/A	More Details
CVE-2025-59827	Flag Forge is a Capture The Flag (CTF) platform. In version 2.1.0, the /api/admin/assign-badge endpoint lacks proper access control, allowing any authenticated user to assign high-privilege badges (e.g., Staff) to themselves. This could lead to privilege escalation and impersonation of administrative roles. This issue has been patched in version 2.2.0.	N/A	More Details
CVE-2025-59828	Claude Code is an agentic coding tool. Prior to Claude Code version 1.0.39, when using Claude Code with Yarn versions 2.0+, Yarn plugins are auto-executed when running yarn --version. This could lead to a bypass of the directory trust dialog in Claude Code, as plugins would be executed prior to the user accepting the risks of working in an untrusted directory. Users running Yarn Classic were unaffected by this issue. This issue has been fixed in version 1.0.39. Users on standard Claude Code auto-update will have received this fix automatically. Users performing manual updates are advised to update to the latest version.	N/A	More Details
CVE-2025-59824	Omni manages Kubernetes on bare metal, virtual machines, or in a cloud. Prior to version 0.48.0, Omni Wireguard SideroLink has the potential to escape. Omni and each Talos machine establish a peer-to-peer (P2P) SideroLink connection using WireGuard to mutually authenticate and authorize access. The WireGuard interface on Omni is configured to ensure that the source IP address of an incoming packet matches the IPv6 address assigned to the Talos peer. However, it performs no validation on the packet's destination address. The Talos end of the SideroLink connection cannot be considered a trusted environment. Workloads running on Kubernetes, especially those configured with host networking, could gain direct access to this link. Therefore, a malicious workload could theoretically send arbitrary packets over the SideroLink interface. This issue has been patched in version 0.48.0.	N/A	More Details
CVE-2025-59952	MinIO Java SDK is a Simple Storage Service (aka S3) client to perform bucket and object operations to any Amazon S3 compatible object storage service. In minio-java versions prior to 8.6.0, XML tag values containing references to system properties or environment variables were automatically substituted with their actual values during processing. This unintended behavior could lead to the exposure of sensitive information, including credentials, file paths, or system configuration details, if such references were present in XML content from untrusted sources. This is fixed in version 8.6.0.	N/A	More Details
CVE-2025-61586	FreshRSS is a free, self-hostable RSS aggregator. Versions 1.26.3 and below are vulnerable to directory enumeration by setting path in theme field, allowing attackers to gain additional information about the server by checking if certain directories exist. This issue is fixed in version 1.27.0.	N/A	More Details
CVE-2025-59343	tar-fs provides filesystem bindings for tar-stream. Versions prior to 3.1.1, 2.1.3, and 1.16.5 are vulnerable to symlink validation bypass if the destination directory is predictable with a specific tarball. This issue has been patched in version 3.1.1, 2.1.4, and 1.16.6. A workaround involves using the ignore option on non files/directories.	N/A	More Details
CVE-2025-56241	Aztech DSL5005EN firmware 1.00.AZ_2013-05-10 and possibly other versions allows unauthenticated attackers to change the administrator password via a crafted POST request to sysAccess.asp. This allows full administrative control of the router without authentication.	N/A	More Details
CVE-2025-40698	SQL injection vulnerability in Prevengos v2.44 by Nedatec Consulting. This vulnerability allows an attacker to retrieve, create, update, and delete databases by sending a POST request using the parameters “mpsCentroin”, “mpsEmpresa”, “mpsProyecto”, and “mpsContrata” in “/servicios/autorizaciones.asmx/mfsRecuperarListado”.	N/A	More Details
CVE-2025-34235	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 25.1.102 and Application prior to version 25.1.1413 (Windows client deployments) contain a registry key that can be enabled by administrators, causing the client to skip SSL/TLS certificate validation. An attacker who can intercept HTTPS traffic can then inject malicious driver DLLs, resulting in remote code execution with SYSTEM privileges; a local attacker can achieve local privilege escalation via a junction-point DLL injection. This vulnerability has been confirmed to be remediated, but it is unclear as to when the patch was introduced.	N/A	More Details
	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 25.1.102 and Application prior to version 25.1.1413 (VA/SaaS deployments) contain two hardcoded private keys that are shipped in the		

CVE-2025-34234	to version 25.1.1413 (VA/SaaS deployments) contain two hardcoded private keys that are shipped in the application containers (printerlogic/pi, printerlogic/printer-admin-api, and printercloud/pi). The keys are stored in clear text under /var/www/app/config/ as keyfile.ppk.dev and keyfile.saasid.ppk.dev. The application uses these keys as the symmetric secret for AES-256-CBC encryption/decryption of the “SaaS Id” (external identifier) through the getEncryptedExternalId() / getDecryptedExternalId() methods. Because the secret is embedded in the deployed image, any attacker who can obtain a copy of the Docker image, read the configuration files, or otherwise enumerate the filesystem can recover the encryption key. This vulnerability has been confirmed to be remediated, but it is unclear as to when the patch was introduced.	N/A	More Details
CVE-2025-34220	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 25.1.102 and Application prior to version 25.1.1413 (VA/SaaS deployments) contains a /api-gateway/identity/search-groups endpoint that does not require authentication. Requests to https://<tenant>.printercloud10.com/api-gateway/identity/search-groups and adjustments to the `Host` header allow an unauthenticated remote attacker to enumerate every group object stored for that tenant. The response includes internal identifiers (group ID, source service ID, Azure AD object IDs, creation timestamps, and tenant IDs). This vulnerability has been confirmed to be remediated, but it is unclear as to when the patch was introduced.	N/A	More Details
CVE-2025-27261	Ericsson Indoor Connect 8855 contains an SQL injection vulnerability which if exploited can result in unauthorized disclosure or modification of data.	N/A	More Details
CVE-2025-30247	An OS command injection vulnerability in user interface in Western Digital My Cloud firmware prior to 5.31.108 on NAS platforms allows remote attackers to execute arbitrary system commands via a specially crafted HTTP POST.	N/A	More Details
CVE-2025-34207	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to 22.0.1049 and Application prior to 20.0.2786 (VA and SaaS deployments) configure the SSH client within Docker instances with the following options: `UserKnownHostsFile=/dev/null`, `StrictHostKeyChecking=no`, and `ForwardAgent yes`. These settings disable verification of the remote host’s SSH key and automatically forward the developer’s SSH-agent to any host that matches the configured wildcard patterns. As a result, an attacker who can reach a single compromised container can cause the container to connect to a malicious SSH server, capture the forwarded private keys, and use those keys for unrestricted lateral movement across the environment.	N/A	More Details
CVE-2025-34209	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to 22.0.862 and Application prior to 20.0.2014 (VA and SaaS deployments) contain Docker images with the private GPG key and passphrase for the account *no-reply+virtual-appliance@printerlogic.com*. The key is stored in cleartext and the passphrase is hardcoded in files. An attacker with administrative access to the appliance can extract the private key, import it into their own system, and subsequently decrypt GPG-encrypted files and sign arbitrary firmware update packages. A maliciously signed update can be uploaded by an admin-level attacker and will be executed by the appliance, giving the attacker full control of the virtual appliance.	N/A	More Details
CVE-2025-34211	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 22.0.1049 and Application prior to version 20.0.2786 (VA and SaaS deployments) contain a private SSL key and matching public certificate stored in cleartext. The key belongs to the hostname `pl-local.com` and is used by the appliance to terminate TLS connections on ports 80/443. Because the key is hardcoded, any attacker who can gain container-level access can simply read the files and obtain the private key. With the private key, the attacker can decrypt TLS traffic, perform man-in-the-middle attacks, or forge TLS certificates. This enables impersonation of the appliance’s web UI, interception of credentials, and unrestricted access to any services that trust the certificate. The same key is identical across all deployed appliances meaning a single theft compromises the confidentiality of every Vasion Print installation.	N/A	More Details
CVE-2025-34212	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 22.0.843 and Application prior to version 20.0.1923 (VA/SaaS deployments) possess CI/CD weaknesses: the build pulls an unverified third-party image, downloads the VirtualBox Extension Pack over plain HTTP without signature validation, and grants the jenkins account NOPASSWD for mount/umount. Together these allow supply chain or man-in-the-middle compromise of the build pipeline, injection of malicious firmware, and remote code execution as root on the CI host. This vulnerability has been identified by the vendor as: V-2023-007 — Supply Chain Attack.	N/A	More Details
CVE-2025-34215	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 22.0.1026 and Application prior to version 20.0.2702 (only VA deployments) expose an unauthenticated firmware-upload flow: a public page returns a signed token usable at va-api/v1/update, and every Docker image contains the appliance’s private GPG key and hard-coded passphrase. An attacker who extracts the key and obtains a token can decrypt, modify, re-sign, upload, and trigger malicious firmware, gaining remote code execution.	N/A	More Details
	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 22.0.1026 and Application		

CVE-2025-34216	prior to version 20.0.2702 (VA deployments only) expose a set of unauthenticated REST API endpoints that return configuration files and clear-text passwords. The same endpoints also disclose the Laravel APP_KEY used for cryptographic signing. Because the APP_KEY is required to generate valid signed requests, an attacker who obtains it can craft malicious payloads that are accepted by the application and achieve remote code execution on the appliance. This vulnerability has been identified by the vendor as: V-2024-018 — RCE & Leaks via API.	N/A	More Details
CVE-2025-34218	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 22.0.1049 and Application prior to version 20.0.2786 (VA/SaaS deployments) expose internal Docker containers through the gw Docker instance. The gateway publishes a /meta endpoint which lists every micro-service container together with version information. These containers are reachable directly over HTTP/HTTPS without any access-control list (ACL), authentication or rate-limiting. Consequently, any attacker on the LAN or the Internet can enumerate all internal services and their versions, interact with the exposed APIs of each microservice as an unauthenticated user, or issue malicious requests that may lead to information disclosure, privilege escalation within the container, or denial-of-service of the entire appliance. The root cause is the absence of authentication and network-level restrictions on the API-gateway's proxy to internal Docker containers, effectively turning the internal service mesh into a public attack surface. This vulnerability has been identified by the vendor as: V-2024-030 — Exposed Internal Docker Instance (LAN).	N/A	More Details
CVE-2025-34221	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 25.2.169 and Application prior to version 25.2.1518 (VA/SaaS deployments) expose every internal Docker container to the network because firewall rules allow unrestricted traffic to the Docker bridge network. Because no authentication, ACL or client-side identifier is required, the attacker can interact with any internal API, bypassing the product's authentication mechanisms entirely. The result is unauthenticated remote access to internal services, allowing credential theft, configuration manipulation and potential remote code execution. This vulnerability has been identified by the vendor as: V-2025-002 — Authentication Bypass - Docker Instances.	N/A	More Details
CVE-2025-34233	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 25.1.102 and Application prior to version 25.1.1413 (VA/SaaS deployments) contain a protection mechanism failure vulnerability within the file_get_contents() function. When an administrator configures a printer's hostname (or similar callback field), the value is passed unchecked to PHP's file_get_contents()/cURL functions, which follow redirects and impose no allow-list, scheme, or IP-range restrictions. An admin-level attacker can therefore point the hostname to a malicious web server that issues a 301 redirect to internal endpoints such as the AWS EC2 metadata service. The server follows the redirect, retrieves the metadata, and returns or stores the credentials, enabling the attacker to steal cloud IAM keys, enumerate internal services, and pivot further into the SaaS infrastructure. This vulnerability has been confirmed to be remediated, but it is unclear as to when the patch was introduced.	N/A	More Details
CVE-2025-34222	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 22.0.1049 and Application prior to version 20.0.2786 (VA/SaaS deployments) expose four admin routes – /admin/hp/cert_upload, /admin/hp/cert_delete, /admin/certs/ca, and /admin/certs/serviceclients/{scid} – without any authentication check. The routes are defined in the /var/www/app/routes/web.php file inside the printercloud/pi Docker container and are handled by the HPCertificateController class, which performs no user validation. An unauthenticated attacker can therefore upload a new TLS/SSL certificate replacing the trusted root used by the appliance, delete an existing certificate causing immediate loss of trust for services that rely on it, or download any stored CA or client certificate via the service-clients endpoint which also suffers an IDOR that allows enumeration of all client IDs. This vulnerability has been identified by the vendor as: V-2024-028 — Unauthenticated Admin APIs Used to Modify SSL Certificates.	N/A	More Details
CVE-2025-34223	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 22.0.1049 and Application prior to version 20.0.2786 (VA/SaaS deployments) contain a default admin account and an installation-time endpoint at `/admin/query/update_database.php` that can be accessed without authentication. An attacker who can reach the installation web interface can POST arbitrary `root_user` and `root_password` values, causing the script to replace the default admin credentials with attacker-controlled ones. The script also contains hard-coded SHA-512 and SHA-1 hashes of the default password, allowing the attacker to bypass password-policy validation. As a result, an unauthenticated remote attacker can obtain full administrative control of the system during the initial setup. This vulnerability has been identified by the vendor as: V-2024-022 — Insecure Installation Credentials.	N/A	More Details
CVE-2025-34224	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 22.0.1049 and Application prior to version 20.0.2786 (VA/SaaS deployments) expose a set of PHP scripts under the `console_release` directory without requiring authentication. An unauthenticated remote attacker can invoke these endpoints to re-configure networked printers, add or delete RFID badge devices, or otherwise modify device settings. This vulnerability has been identified by the vendor as: V-2024-029 — No Authentication to Modify Devices.	N/A	More Details
	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 25.1.102 and Application prior		

CVE-2025-34225	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 25.1.102 and Application prior to version 25.1.1413 (VA/SaaS deployments) contain a server-side request forgery (SSRF) vulnerability. The `console_release` directory is reachable from the internet without any authentication. Inside that directory are dozens of PHP scripts that build URLs from user-controlled values and then invoke either 'curl_exec()` or `file_get_contents()` without proper validation. Although many files attempt to mitigate SSRF by calling `filter_var', the checks are incomplete. Because the endpoint is unauthenticated, any remote attacker can supply a hostname and cause the server to issue requests to internal resources. This enables internal network reconnaissance, potential pivoting, or data exfiltration. This vulnerability has been confirmed to be remediated, but it is unclear as to when the patch was introduced.	N/A	More Details
CVE-2025-34228	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 25.1.102 and Application prior to version 25.1.1413 (VA/SaaS deployments) contain a server-side request forgery (SSRF) vulnerability. The `/var/www/app/console_release/lexmark/update.php` script is reachable from the internet without any authentication. The PHP script builds URLs from user-controlled values and then invokes either 'curl_exec()` or `file_get_contents()` without proper validation. Because the endpoint is unauthenticated, any remote attacker can supply a hostname and cause the server to issue requests to internal resources. This enables internal network reconnaissance, potential pivoting, or data exfiltration. This vulnerability has been confirmed to be remediated, but it is unclear as to when the patch was introduced.	N/A	More Details
CVE-2025-34229	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 25.1.102 and Application prior to version 25.1.1413 (VA/SaaS deployments) contain a blind server-side request forgery (SSRF) vulnerability reachable via the /var/www/app/console_release/hp/installApp.php script that can be exploited by an unauthenticated user. When a printer is registered, the software stores the printer's host name in the variable $printer_vo->str_host_address. The code later builds a URL like 'http://<host-address>:80/DevMgmt/DiscoveryTree.xml' and sends the request with curl. No validation, whitelist, or private-network filtering is performed before the request is made. Because the request is blind, an attacker cannot see the data directly, but can still: probe internal services, trigger internal actions, or gather other intelligence. This vulnerability has been confirmed to be remediated, but it is unclear as to when the patch was introduced.	N/A	More Details
CVE-2025-34230	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 25.1.102 and Application prior to version 25.1.1413 (VA/SaaS deployments) contain a blind server-side request forgery (SSRF) vulnerability reachable via the /var/www/app/console_release/hp/log_off_single_sign_on.php script that can be exploited by an unauthenticated user. When a printer is registered, the software stores the printer's host name in the variable $printer_vo->str_host_address. The code later builds a URL like 'http://<host-address>:80/DevMgmt/DiscoveryTree.xml' and sends the request with curl. No validation, whitelist, or private-network filtering is performed before the request is made. Because the request is blind, an attacker cannot see the data directly, but can still: probe internal services, trigger internal actions, or gather other intelligence. This vulnerability has been confirmed to be remediated, but it is unclear as to when the patch was introduced.	N/A	More Details
CVE-2025-34231	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 25.1.102 and Application prior to version 25.1.1413 (VA/SaaS deployments) contain a blind and non-blind server-side request forgery (SSRF) vulnerability. The '/var/www/app/console_release/hp/badgeSetup.php' script is reachable from the Internet without any authentication and builds URLs from user-controlled parameters before invoking either the custom processCurl() function or PHP's file_get_contents(); in both cases the hostname/URL is taken directly from the request with no whitelist, scheme restriction, IP-range validation, or outbound-network filtering. Consequently, any unauthenticated attacker can force the server to issue arbitrary HTTP requests to internal resources. This enables internal network reconnaissance, credential leakage, pivoting, and data exfiltration. This vulnerability has been confirmed to be remediated, but it is unclear as to when the patch was introduced.	N/A	More Details
CVE-2025-34232	Vasion Print (formerly PrinterLogic) Virtual Appliance Host prior to version 25.1.102 and Application prior to version 25.1.1413 (VA/SaaS deployments) contain a blind server-side request forgery (SSRF) vulnerability reachable via the /var/www/app/console_release/lexmark/dellCheck.php script that can be exploited by an unauthenticated user. When a printer is registered, the software stores the printer's host name in the variable $printer_vo->str_host_address. The code later builds a URL like 'http://<host-address>:80/DevMgmt/DiscoveryTree.xml' and sends the request with curl. No validation, whitelist, or private-network filtering is performed before the request is made. Because the request is blind, an attacker cannot see the data directly, but can still: probe internal services, trigger internal actions, or gather other intelligence. This vulnerability has been confirmed to be remediated, but it is unclear as to when the patch was introduced.	N/A	More Details
CVE-2025-43779	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.112, and Liferay DXP 2024.Q1.1 through 2024.Q1.18 and 7.4 GA through update 92 allows a remote authenticated attacker to inject JavaScript code via _com_liferay_commerce_product_definitions_web_internal_portlet_CPDefinitionsPortlet_productTypeName parameter. This malicious payload is then reflected and executed within the user's browser.	N/A	More Details