SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 24 July 2025

Generated on 24 July 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-2025-54122	Manager-io/Manager is accounting software. A critical unauthenticated full read Server-Side Request Forgery (SSRF) vulnerability has been identified in the proxy handler component of both manager Desktop and Server edition versions up to and including 25.7.18.2519. This vulnerability allows an unauthenticated attacker to bypass network isolation and access restrictions, potentially enabling access to internal services, cloud metadata endpoints, and exfiltration of sensitive data from isolated network segments. This vulnerability is fixed in version 25.7.21.2525.	10.0	More Details
CVE-2025-4285	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Rolantis Information Technologies Agentis allows SQL Injection.This issue affects Agentis: before 4.32.	10.0	More Details
CVE-2025-49747	Missing authorization in Azure Machine Learning allows an authorized attacker to elevate privileges over a network.	9.9	More Details
CVE-2025-49746	Improper authorization in Azure Machine Learning allows an authorized attacker to elevate privileges over a network.	9.9	More Details
CVE-2025-5396	The Bears Backup plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.0.0. This is due to the bbackup_ajax_handle() function not having a capability check, nor validating user supplied input passed directly to call_user_func(). This makes it possible for unauthenticated attackers to execute code on the server which can be leverage to inject backdoors or create new administrative user accounts to name a few things. On WordPress sites running the Alone theme versions 7.8.4 and older, this can be chained with CVE-2025-5394 to install the Bears Backup plugin and achieve the same impact.	9.8	More Details
CVE-2025-	Certain modem models developed by Askey has a Stack-based Buffer Overflow vulnerability, allowing unauthenticated remote attackers to control the program's execution flow and	9.8	More

7921	potentially execute arbitrary code.		Details
CVE-2025-46120	An issue was discovered in CommScope Ruckus Unleashed prior to 200.15.6.212.27 and 200.18.7.1.323, and in Ruckus ZoneDirector prior to 10.5.1.0.282, where a path-traversal flaw in the web interface lets the server execute attacker-supplied EJS templates outside permitted directories, allowing a remote unauthenticated attacker who can upload a template (e.g., via FTP) to escalate privileges and run arbitrary template code on the controller.	9.8	More Details
CVE-2025-44655	In TOTOLink A7100RU V7.4, A950RG V5.9, and T10 V5.9, the chroot_local_user option is enabled in the vsftpd.conf. This could lead to unauthorized access to system files, privilege escalation, or use of the compromised server as a pivot point for internal network attacks.	9.8	More Details
CVE-2025-44658	In Netgear RAX30 V1.0.10.94, a PHP-FPM misconfiguration vulnerability is caused by not following the specification to only limit FPM to .php extensions. An attacker may exploit this by uploading malicious scripts disguised with alternate extensions and tricking the web server into executing them as PHP, bypassing security mechanisms based on file extension filtering. This may lead to remote code execution (RCE), information disclosure, or full system compromise.	9.8	More Details
CVE-2025-7393	Improper Restriction of Excessive Authentication Attempts vulnerability in Drupal Mail Login allows Brute Force.This issue affects Mail Login: from 3.0.0 before 3.2.0, from 4.0.0 before 4.2.0.	9.8	More Details
CVE-2025-36846	An issue was discovered in Eveo URVE Web Manager 27.02.2025. The application exposes a /_internal/pc/vpro.php localhost endpoint to unauthenticated users that is vulnerable to OS Command Injection. The endpoint takes an input parameter that is passed directly into the shell_exec() function of PHP. NOTE: this can be chained with CVE-2025-36845.	9.8	More Details
CVE-2025-44654	In Linksys E2500 3.0.04.002, the chroot_local_user option is enabled in the vsftpd configuration file. This could lead to unauthorized access to system files, privilege escalation, or use of the compromised server as a pivot point for internal network attacks.	9.8	More Details
CVE-2020-26799	A reflected cross-site scripting (XSS) vulnerability was discovered in index.php on Luxcal 4.5.2 which allows an unauthenticated attacker to steal other users' data.	9.8	More Details
CVE-2012-10020	The FoxyPress plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the uploadify.php file in versions up to, and including, 0.4.2.1. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected sites server which may make remote code execution possible.	9.8	More Details
CVE-2015-10137	The Website Contact Form With File Upload plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload_file()' function in versions up to, and including, 1.3.4. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected sites server which may make remote code execution possible.	9.8	More Details
CVE-2025-6187	The bSecure plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization within its order_info REST endpoint in versions 1.3.7 through 1.7.9. The plugin registers the /webhook/v2/order_info/ route with a permission_callback that always returns true, effectively bypassing all authentication. This makes it possible for unauthenticated attackers who know any user’s email to obtain a valid login cookie and fully impersonate that account.	9.8	More Details
CVE-2025-8028	On arm64, a WASM `br_table` instruction with a lot of entries could lead to the label being too far from the instruction causing truncation and incorrect computation of the branch address. This vulnerability affects Firefox < 141, Firefox ESR < 115.26, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	9.8	More Details
CVE-2025-8031	The `username:password` part was not correctly stripped from URLs in CSP reports potentially leaking HTTP Basic Authentication credentials. This vulnerability affects Firefox < 141, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	9.8	More Details
CVE-2025-8038	Thunderbird ignored paths when checking the validity of navigations in a frame. This vulnerability affects Firefox < 141, Firefox ESR < 140.1, Thunderbird < 141, and Thunderbird < 140.1.	9.8	More Details

CVE-2025-8043	Focus incorrectly truncated URLs towards the beginning instead of around the origin. This vulnerability affects Firefox < 141 and Thunderbird < 141.	9.8	More Details
CVE-2025-8044	Memory safety bugs present in Firefox 140 and Thunderbird 140. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 141 and Thunderbird < 141.	9.8	More Details
CVE-2025-54438	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Upload a Web Shell to a Web Server.This issue affects MagicINFO 9 Server: less than 21.1080.0	9.8	More Details
CVE-2025-54440	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.8	More Details
CVE-2025-54442	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.8	More Details
CVE-2025-54443	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Upload a Web Shell to a Web Server.This issue affects MagicINFO 9 Server: less than 21.1080.0	9.8	More Details
CVE-2025-54444	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.8	More Details
CVE-2025-54446	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Upload a Web Shell to a Web Server.This issue affects MagicINFO 9 Server: less than 21.1080.0	9.8	More Details
CVE-2025-54448	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.8	More Details
CVE-2025-54449	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.8	More Details
CVE-2025-54451	Improper Control of Generation of Code ('Code Injection') vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.8	More Details
CVE-2025-41687	An unauthenticated remote attacker may use a stack based buffer overflow in the u-link Management API to gain full access on the affected devices.	9.8	More Details
CVE-2025-6704	An arbitrary file writing vulnerability in the Secure PDF eXchange (SPX) feature of Sophos Firewall versions older than 21.0 MR2 (21.0.2) can lead to pre-auth remote code execution, if a specific configuration of SPX is enabled in combination with the firewall running in High Availability (HA) mode.	9.8	More Details
CVE-2025-7624	An SQL injection vulnerability in the legacy (transparent) SMTP proxy of Sophos Firewall versions older than 21.0 MR2 (21.0.2) can lead to remote code execution, if a quarantining policy is active for Email and SFOS was upgraded from a version older than 21.0 GA.	9.8	More Details
CVE-2025-46001	An arbitrary file upload vulnerability in the is_allowed_file_type() function of Filemanager v2.3.0 allows attackers to execute arbitrary code via uploading a crafted PHP file.	9.8	More Details
CVE-2025-7444	The LoginPress Pro plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 5.0.1. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email and the user does not have an already-existing account for the service returning the token.	9.8	More Details
CVE-2025-26855	A SQL injection in Articles Calendar extension 1.0.0 - 1.0.1.0007 for Joomla allows attackers to execute arbitrary SQL commands.	9.8	More Details

CVE-2025-26854	A SQL injection in Articles Good Search extension 1.0.0 - 1.2.4.0011 for Joomla allows attackers to execute arbitrary SQL commands.	9.8	More Details
CVE-2025-7696	The Integration for Pipedrive and Contact Form 7, WPForms, Elementor, Ninja Forms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.2.3 via deserialization of untrusted input within the verify_field_val() function. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain in the Contact Form 7 plugin, which is likely to be used alongside, allows attackers to delete arbitrary files, leading to a denial of service or remote code execution when the wp-config.php file is deleted.	9.8	More Details
CVE-2025-7697	The Integration for Google Sheets and Contact Form 7, WPForms, Elementor, Ninja Forms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.1.1 via deserialization of untrusted input within the verify_field_val() function. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain in the Contact Form 7 plugin, which is likely to be used alongside, allows attackers to delete arbitrary files, leading to a denial of service or remote code execution when the wp-config.php file is deleted.	9.8	More Details
CVE-2012-10019	The Front End Editor plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation via the upload.php file in versions before 2.3. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected sites server which may make remote code execution possible.	9.8	More Details
CVE-2015-10135	The WPshop 2 – E-Commerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ajaxUpload function in versions before 1.3.9.6. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected sites server which may make remote code execution possible.	9.8	More Details
CVE-2025-6222	The WooCommerce Refund And Exchange with RMA - Warranty Management, Refund Policy, Manage User Wallet theme for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'ced_rnx_order_exchange_attach_files' function in all versions up to, and including, 3.2.6. 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-2016-15043	The WP Mobile Detector plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in resize.php file in versions up to, and including, 3.5. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected sites server which may make remote code execution possible.	9.8	More Details
CVE-2015-10138	The Work The Flow File Upload plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the jQuery-File-Upload-9.5.0 server and test files in versions up to, and including, 2.5.2. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected sites server which may make remote code execution possible.	9.8	More Details
CVE-2025-53770	Deserialization of untrusted data in on-premises Microsoft SharePoint Server allows an unauthorized attacker to execute code over a network. Microsoft is aware that an exploit for CVE-2025-53770 exists in the wild. Microsoft is preparing and fully testing a comprehensive update to address this vulnerability. In the meantime, please make sure that the mitigation provided in this CVE documentation is in place so that you are protected from exploitation.	9.8	More Details
CVE-2025-7916	WinMatrix3 developed by Simopro Technology has an Insecure Deserialization vulnerability, allowing unauthenticated remote attackers to execute arbitrary code on the server by sending maliciously crafted serialized contents.	9.8	More Details
CVE-2025-7918	WinMatrix3 Web package developed by Simopro Technology has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.	9.8	More Details
CVE-2025-50240	nbcio-boot v1.0.3 was discovered to contain a SQL injection vulnerability via the userIds parameter at /sys/user/deleteRecycleBin.	9.8	More Details
CVE-2025-52046	Totolink A3300R V17.0.0cu.596_B20250515 was found to contain a command injection vulnerability in the sub_4197C0 function via the mac and desc parameters. This vulnerability allows unauthenticated attackers to execute arbitrary commands via a crafted request.	9.8	More Details

CVE-2025-25257	An improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability [CWE-89] in Fortinet FortiWeb version 7.6.0 through 7.6.3, 7.4.0 through 7.4.7, 7.2.0 through 7.2.10 and below 7.0.10 allows an unauthenticated attacker to execute unauthorized SQL code or commands via crafted HTTP or HTTPs requests.	9.8	More Details
CVE-2025-51630	TOTOLINK N350RT V9.3.5u.6139_B20201216 was discovered to contain a buffer overflow via the ePort parameter in the function setIpPortFilterRules.	9.8	More Details
CVE-2025-7343	The SFT developed by Digiwin has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.	9.8	More Details
CVE-2025-53964	GoldenDict 1.5.0 and 1.5.1 has an exposed dangerous method that allows reading and modifying files when a user adds a crafted dictionary and then searches for any term included in that dictionary.	9.6	More Details
CVE-2024-6107	Due to insufficient verification, an attacker could use a malicious client to bypass authentication checks and run RPC commands in a region. This has been addressed in MAAS and updated in the corresponding snaps.	9.6	More Details
CVE-2025-6185	Leviton AcquiSuite and Energy Monitoring Hub are susceptible to a cross-site scripting vulnerability, allowing an attacker to craft a malicious payload in URL parameters, which would execute in a client browser when accessed by a user, steal session tokens, and control the service.	9.3	More Details
CVE-2025-8037	Setting a nameless cookie with an equals sign in the value shadowed other cookies. Even if the nameless cookie was set over HTTP and the shadowed cookie included the `Secure` attribute. This vulnerability affects Firefox < 141, Firefox ESR < 140.1, Thunderbird < 141, and Thunderbird < 140.1.	9.1	More Details
CVE-2025-46117	An issue was discovered in CommScope Ruckus Unleashed prior to 200.15.6.212.14 and 200.17.7.0.139, and in Ruckus ZoneDirector prior to 10.5.1.0.279, where a hidden debug script `.ap_debug.sh` invoked from the restricted CLI does not properly sanitize its input, allowing an authenticated attacker to execute arbitrary commands as root on the controller or specified target.	9.1	More Details
CVE-2025-53882	A Reliance on Untrusted Inputs in a Security Decision vulnerability in the logrotate configuration for openSUSEs mailman3 package allows potential escalation from mailman to rootThis issue affects openSUSE Tumbleweed: from ? before 3.3.10-2.1.	9.1	More Details
CVE-2025-7712	The Madara - Core plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the wp_manga_delete_zip() function in all versions up to, and including, 2.2.3. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	9.1	More Details
CVE-2025-54455	Use of Hard-coded Credentials vulnerability in Samsung Electronics MagicINFO 9 Server allows Authentication Bypass.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.1	More Details
CVE-2025-54454	Use of Hard-coded Credentials vulnerability in Samsung Electronics MagicINFO 9 Server allows Authentication Bypass.This issue affects MagicINFO 9 Server: less than 21.1080.0.	9.1	More Details
CVE-2025-53909	mailcow: dockerized is an open source groupware/email suite based on docker. A Server-Side Template Injection (SSTI) vulnerability exists in versions prior to 2025-07 in the notification template system used by mailcow for sending quota and quarantine alerts. The template rendering engine allows template expressions that may be abused to execute code in certain contexts. The issue requires admin-level access to mailcow UI to configure templates, which are automatically rendered during normal system operation. Version 2025-07 contains a patch for the issue.	9.1	More Details
CVE-2025-46122	An issue was discovered in CommScope Ruckus Unleashed prior to 200.15.6.212.14 and 200.17.7.0.139, where the authenticated diagnostics API endpoint `/admin/_cmdstat.jsp` passes attacker-controlled input to the shell without adequate validation, enabling a remote attacker to specify a target by MAC address and execute arbitrary commands as root.	9.1	More Details
	Server-Side Request Forgery (SSRF) vulnerability exists in the URL processing functionality of		

CVE-2025-52362	PHProxy version 1.1.1 and prior. The input validation for the _proxurl parameter can be bypassed, allowing a remote, unauthenticated attacker to submit a specially crafted URL	9.1	More Details
CVE-2025-7643	The Attachment Manager plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the handle_actions() function in all versions up to, and including, 2.1.2. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	9.1	More Details
CVE-2025-40599	An authenticated arbitrary file upload vulnerability exists in the SMA 100 series web management interface. A remote attacker with administrative privileges can exploit this flaw to upload arbitrary files to the system, potentially leading to remote code execution.	9.1	More Details
CVE-2025-24937	File contents could be read from the local file system by an attacker. Additionally, malicious code could be inserted in the file, leading to a full compromise of the web application and the container it is running on. The vulnerable component is bound to the network stack and the set of possible attackers extends up to and including the entire Internet. The web application allows arbitrary files to be included in a file that was downloadable and executable by the web server.	9.0	More Details
CVE-2025-47158	Authentication bypass by assumed-immutable data in Azure DevOps allows an unauthorized attacker to elevate privileges over a network.	9.0	More Details
CVE-2025-23266	NVIDIA Container Toolkit for all platforms contains a vulnerability in some hooks used to initialize the container, where an attacker could execute arbitrary code with elevated permissions. A successful exploit of this vulnerability might lead to escalation of privileges, data tampering, information disclosure, and denial of service.	9.0	More Details
CVE-2025-24936	The web application allows user input to pass unfiltered to a command executed on the underlying operating system. The vulnerable component is bound to the network stack and the set of possible attackers extends up to and including the entire Internet. An attacker with low privileged access to the application has the potential to execute commands on the operating system under the context of the webserver.	9.0	More Details
CVE-2025-54309	CrushFTP 10 before 10.8.5 and 11 before 11.3.4_23, when the DMZ proxy feature is not used, mishandles AS2 validation and consequently allows remote attackers to obtain admin access via HTTPS, as exploited in the wild in July 2025.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-47917	Mbed TLS before 3.6.4 allows a use-after-free in certain situations of applications that are developed in accordance with the documentation. The function mbedtls_x509_string_to_names() takes a head argument that is documented as an output argument. The documentation does not suggest that the function will free that pointer; however, the function does call mbedtls_asn1_free_named_data_list() on that argument, which performs a deep free(). As a result, application code that uses this function (relying only on documented behavior) is likely to still hold pointers to the memory blocks that were freed, resulting in a high risk of use-after-free or double-free. In particular, the two sample programs x509/cert_write and x509/cert_req are affected (use-after-free if the san string contains more than one DN).	8.9	More Details
CVE-2025-8040	Memory safety bugs present in Firefox ESR 140.0, Thunderbird ESR 140.0, Firefox 140 and Thunderbird 140. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 141, Firefox ESR < 140.1, Thunderbird < 141, and Thunderbird < 140.1.	8.8	More Details
CVE-2015-10139	The WPLMS theme for WordPress is vulnerable to Privilege Escalation in versions 1.5.2 to 1.8.4.1 via the 'wp_ajax_import_data' AJAX action. This makes it possible for authenticated attackers to change otherwise restricted settings and potentially create a new accessible admin account.	8.8	More Details
CVE-2025-	CWE-434 Unrestricted Upload of File with Dangerous Type	8.8	More

46384			Details
CVE-2025-6190	The Realty Portal – Agent plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization within the rp_user_profile() AJAX handler in versions 0.1.0 through 0.3.9. The handler reads the client-supplied meta key and value pairs from $_POST and passes them directly to update_user_meta() without restricting to a safe whitelist. This makes it possible for authenticated attackers, with Subscriber-level access and above, to overwrite the wp_capabilities meta and grant themselves the administrator role.	8.8	More Details
CVE-2025-41684	An authenticated remote attacker can execute arbitrary commands with root privileges on affected devices due to lack of improper sanitizing of user input in the Main Web Interface (endpoint tls_iotgen_setting).	8.8	More Details
CVE-2025-41683	An authenticated remote attacker can execute arbitrary commands with root privileges on affected devices due to lack of improper sanitizing of user input in the Main Web Interface (endpoint event_mail_test).	8.8	More Details
CVE-2025-54453	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	8.8	More Details
CVE-2025-7805	A vulnerability classified as critical has been found in Tenda FH451 1.0.0.9. This affects the function fromPptpUserSetting of the file /goform/PPTPUserSetting. The manipulation of the argument delno leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-6718	The B1.lt plugin for WordPress is vulnerable to SQL Injection due to a missing capability check on the b1_run_query AJAX action in all versions up to, and including, 2.2.56. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute and run arbitrary SQL commands.	8.8	More Details
CVE-2025-46116	An issue was discovered in CommScope Ruckus Unleashed prior to 200.15.6.212.14 and 200.17.7.0.139, and in Ruckus ZoneDirector prior to 10.5.1.0.279, where an authenticated attacker can disable the passphrase requirement for a hidden CLI command `!v54!` via a management API call and then invoke it to escape the restricted shell and obtain a root shell on the controller.	8.8	More Details
CVE-2025-7908	A vulnerability was found in D-Link DI-8100 1.0. It has been declared as critical. Affected by this vulnerability is the function sprintf of the file /ddns.asp?opt=add of the component jhttpd. The manipulation of the argument mx leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7909	A vulnerability was found in D-Link DIR-513 1.0. It has been rated as critical. Affected by this issue is the function sprintf of the file /goform/formLanSetupRouterSettings of the component Boa Webserver. The manipulation of the argument curTime leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2025-7382	A command injection vulnerability in WebAdmin of Sophos Firewall versions older than 21.0 MR2 (21.0.2) can lead to adjacent attackers achieving pre-auth code execution on High Availability (HA) auxiliary devices, if OTP authentication for the admin user is enabled.	8.8	More Details
CVE-2025-33076	IBM Engineering Systems Design Rhapsody 9.0.2, 10.0, and 10.0.1 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local user could overflow the buffer and execute arbitrary code on the system.	8.8	More Details
CVE-2025-3740	The School Management System for Wordpress plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 93.1.0 via the 'page' parameter. This makes it possible for authenticated attackers, with Subscriber-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included. The Local File Inclusion exploit can be chained to include various dashboard view files in the plugin. One such chain can be leveraged to update the password of Super Administrator accounts in Multisite environments making privilege escalation possible. The vendor has updated the version numbers beginning	8.8	More Details

	with `1.93.1 (02-07-2025)` for the patched version. This version comes after version 93.1.0.		
CVE-2025-8034	Memory safety bugs present in Firefox ESR 115.25, Firefox ESR 128.12, Thunderbird ESR 128.12, Firefox ESR 140.0, Thunderbird ESR 140.0, Firefox 140 and Thunderbird 140. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 141, Firefox ESR < 115.26, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	8.8	More Details
CVE-2025-8010	Type Confusion in V8 in Google Chrome prior to 138.0.7204.168 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-51865	Ai2 playground web service (playground.allenai.org) LLM chat through 2025-06-03 is vulnerable to Insecure Direct Object Reference (IDOR), allowing attackers to gain sensitvie information via enumerating thread keys in the URL.	8.8	More Details
CVE-2025-6813	The aapanel WP Toolkit plugin for WordPress is vulnerable to Privilege Escalation due to missing authorization checks within the auto_login() function in versions 1.0 to 1.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to bypass all role checks and gain full admin privileges.	8.8	More Details
CVE-2025-51464	Cross-site Scripting (XSS) in aimhubio Aim 3.28.0 allows remote attackers to execute arbitrary JavaScript in victims browsers via malicious Python code submitted to the /api/reports endpoint, which is interpreted and executed by Pyodide when the report is viewed. No sanitisation or sandbox restrictions prevent JavaScript execution via pyodide.code.run_js().	8.8	More Details
CVE-2025-7762	A vulnerability, which was classified as critical, has been found in D-Link DI-8100 16.07.26A1. This issue affects some unknown processing of the file /menu_nat_more.asp of the component HTTP Request Handler. The manipulation leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-51482	Remote Code Execution in letta.server.rest_api.routers.v1.tools.run_tool_from_source in letta-ai Letta 0.7.12 allows remote attackers to execute arbitrary Python code and system commands via crafted payloads to the /v1/tools/run endpoint, bypassing intended sandbox restrictions.	8.8	More Details
CVE-2025-7758	A vulnerability, which was classified as critical, has been found in TOTOLINK T6 up to 4.1.5cu.748_B20211015. Affected by this issue is the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi of the component HTTP POST Request Handler. The manipulation of the argument ip leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7344	The EAI developed by Digiwin has a Privilege Escalation vulnerability, allowing remote attackers with regular privileges to elevate their privileges to administrator level via a specific API.	8.8	More Details
CVE-2025-8019	A vulnerability was found in Shenzhen Libituo Technology LBT-T300-T310 2.2.3.6. It has been rated as critical. Affected by this issue is the function sub_40B6F0 of the file at/appy.cgi. The manipulation of the argument wan_proto leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7837	A vulnerability was found in TOTOLINK T6 4.1.5cu.748_B20211015 and classified as critical. Affected by this issue is the function recvSlaveStaInfo of the component MQTT Service. The manipulation of the argument dest leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7433	A local privilege escalation vulnerability in Sophos Intercept X for Windows with Central Device Encryption 2025.1 and older allows arbitrary code execution.	8.8	More Details
CVE-2025-8060	A vulnerability has been found in Tenda AC23 16.03.07.52 and classified as critical. Affected by this vulnerability is the function sub_46C940 of the file /goform/setMacFilterCfg of the component httpd. The manipulation of the argument deviceList leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details

CVE-2025-51480	Path Traversal vulnerability in onnx.external_data_helper.save_external_data in ONNX 1.17.0 allows attackers to overwrite arbitrary files by supplying crafted external_data.location paths containing traversal sequences, bypassing intended directory restrictions.	8.8	More Details
CVE-2025-8011	Type Confusion in V8 in Google Chrome prior to 138.0.7204.168 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2025-7853	A vulnerability was found in Tenda FH451 1.0.0.9. It has been rated as critical. This issue affects the function fromSetIpBind of the file /goform/SetIpBind. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7854	A vulnerability classified as critical has been found in Tenda FH451 1.0.0.9. Affected is the function fromVirtualSer of the file /goform/VirtualSer. The manipulation of the argument page leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7855	A vulnerability classified as critical was found in Tenda FH451 1.0.0.9. Affected by this vulnerability is the function fromqossetting of the file /goform/qossetting. The manipulation of the argument page leads to stack-based buffer overflow. The attack can be launched remotely.	8.8	More Details
CVE-2025-7910	A vulnerability classified as critical has been found in D-Link DIR-513 1.10. This affects the function sprintf of the file /goform/formSetWanNonLogin of the component Boa Webserver. The manipulation of the argument curTime leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2025-33077	IBM Engineering Systems Design Rhapsody 9.0.2, 10.0, and 10.0.1 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local user could overflow the buffer and execute arbitrary code on the system.	8.8	More Details
CVE-2024-13972	A vulnerability related to registry permissions in the Intercept X for Windows updater prior to version 2024.3.2 can lead to a local user gaining SYSTEM level privileges during a product upgrade.	8.8	More Details
CVE-2025-50151	File access paths in configuration files uploaded by users with administrator access are not validated. This issue affects Apache Jena version up to 5.4.0. Users are recommended to upgrade to version 5.5.0, which does not allow arbitrary configuration upload.	8.8	More Details
CVE-2025-7806	A vulnerability classified as critical was found in Tenda FH451 1.0.0.9. This vulnerability affects the function fromSafeClientFilter of the file /goform/SafeClientFilter. The manipulation of the argument Go/page leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7945	A vulnerability was found in D-Link DIR-513 up to 20190831. It has been declared as critical. This vulnerability affects the function formSetWanDhcpplus of the file /goform/formSetWanDhcpplus. The manipulation of the argument curTime leads to buffer overflow. The attack can be initiated remotely. This vulnerability only affects products that are no longer supported by the maintainer.	8.8	More Details
CVE-2025-50585	StudentManage v1.0 was discovered to contain a SQL injection vulnerability via the component /admin/adminStudentUrl.	8.8	More Details
CVE-2025-7807	A vulnerability, which was classified as critical, has been found in Tenda FH451 1.0.0.9. This issue affects the function fromSafeUrlFilter of the file /goform/SafeUrlFilter. The manipulation of the argument Go/page leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7796	A vulnerability, which was classified as critical, was found in Tenda FH451 1.0.0.9. This affects the function fromPptpUserAdd of the file /goform/PPTPDClient. The manipulation of the argument Username leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-	A vulnerability, which was classified as critical, has been found in Tenda FH451 1.0.0.9. Affected by this issue is the function fromP2pListFilter of the file /goform/P2pListFilter. The manipulation		

2025-7795	of the argument page leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-8022	All versions of the package bun are vulnerable to Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in the $ shell API due to improper neutralization of user input. An attacker can exploit this by providing specially crafted input that includes command-line arguments or shell metacharacters, leading to unintended command execution.	8.8	More Details
CVE-2025-7794	A vulnerability classified as critical was found in Tenda FH451 1.0.0.9. Affected by this vulnerability is the function fromNatStaticSetting of the file /goform/NatStaticSetting. The manipulation of the argument page leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7793	A vulnerability classified as critical has been found in Tenda FH451 1.0.0.9. Affected is the function formWebTypeLibrary of the file /goform/webtypelibrary. The manipulation of the argument webSiteId leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7792	A vulnerability was found in Tenda FH451 1.0.0.9. It has been rated as critical. This issue affects the function formSafeEmailFilter of the file /goform/SafeEmailFilter. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2015-10140	The Ajax Load More plugin before 2.8.1.2 does not have authorisation in some of its AJAX actions, allowing any authenticated users, such as subscriber, to upload and delete arbitrary files.	8.8	More Details
CVE-2025-7914	A vulnerability has been found in Tenda AC6 15.03.06.50 and classified as critical. Affected by this vulnerability is the function setparentcontrolinfo of the component httpd. The manipulation leads to buffer overflow. The attack can be launched remotely.	8.8	More Details
CVE-2025-8017	A vulnerability was found in Tenda AC7 15.03.06.44. It has been classified as critical. Affected is the function formSetMacFilterCfg of the file /goform/setMacFilterCfg of the component httpd. The manipulation of the argument deviceList leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-54439	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	8.8	More Details
CVE-2025-7913	A vulnerability, which was classified as critical, was found in TOTOLINK T6 4.1.5cu.748_B20211015. Affected is the function updateWifiInfo of the component MQTT Service. The manipulation of the argument serverIp leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-54441	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	8.8	More Details
CVE-2025-7911	A vulnerability classified as critical was found in D-Link DI-8100 1.0. This vulnerability affects the function sprintf of the file /upnp_ctrl.asp of the component jhttpd. The manipulation of the argument remove_ext_proto/remove_ext_port leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7747	A vulnerability classified as critical has been found in Tenda FH451 1.0.0.9. This affects the function fromWizardHandle of the file /goform/WizardHandle of the component POST Request Handler. The manipulation of the argument PPW leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-7912	A vulnerability, which was classified as critical, has been found in TOTOLINK T6 4.1.5cu.748_B20211015. This issue affects the function recvSlaveUpgstatus of the component MQTT Service. The manipulation of the argument s leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details

CVE-2025-7790	A vulnerability was found in D-Link DI-8100 16.07.26A1. It has been classified as critical. This affects an unknown part of the file /menu_nat.asp of the component HTTP Request Handler. The manipulation of the argument out_addr/in_addr/out_port/proto leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-8035	Memory safety bugs present in Firefox ESR 128.12, Thunderbird ESR 128.12, Firefox ESR 140.0, Thunderbird ESR 140.0, Firefox 140 and Thunderbird 140. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 141, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	8.8	More Details
CVE-2025-7722	The Social Streams plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.0.1. This is due to the plugin not properly validating a user's identity prior to updating their user meta information in the update_user_meta() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change their user type to that of an administrator.	8.8	More Details
CVE-2025-53762	Permissive list of allowed inputs in Microsoft Purview allows an authorized attacker to elevate privileges over a network.	8.7	More Details
CVE-2025-4700	An issue has been discovered in GitLab CE/EE affecting all versions from 15.10 before 18.0.5, 18.1 before 18.1.3, and 18.2 before 18.2.1 that, under specific circumstances, could have potentially allowed a successful attacker to trigger unintended content rendering leading to XSS.	8.7	More Details
CVE-2025-46385	CWE-918 Server-Side Request Forgery (SSRF)	8.6	More Details
CVE-2025-36845	An issue was discovered in Eveo URVE Web Manager 27.02.2025. The endpoint /_internal/redirect.php allows for Server-Side Request Forgery (SSRF). The endpoint takes a URL as input, sends a request to this address, and reflects the content in the response. This can be used to request endpoints only reachable by the application server.	8.6	More Details
CVE-2025-23267	NVIDIA Container Toolkit for all platforms contains a vulnerability in the update-ldcache hook, where an attacker could cause a link following by using a specially crafted container image. A successful exploit of this vulnerability might lead to data tampering and denial of service.	8.5	More Details
CVE-2025-54317	An issue was discovered in Logpoint before 7.6.0. An attacker with operator privileges can exploit a path traversal vulnerability when creating a Layout Template, which can lead to remote code execution (RCE).	8.4	More Details
CVE-2025-24938	The web application allows user input to pass unfiltered to a command executed on the underlying operating system. An attacker with high privileged access (administrator) to the application has the potential execute commands on the operating system under the context of the webserver. The vulnerable component is bound to the network stack and the set of possible attackers extends up to and including the entire Internet. Has the potential to inject command while creating a new User from User Management.	8.4	More Details
CVE-2025-54075	MDC is a tool to take regular Markdown and write documents interacting deeply with a Vue component. Prior to version 0.17.2, a remote script-inclusion / stored cross-site scripting vulnerability in @nuxtjs/mdc lets a Markdown author inject a `<base href="https://attacker.tld">` element. The `<base>` tag rewrites how all subsequent relative URLs are resolved, so an attacker can make the page load scripts, styles, or images from an external, attacker-controlled origin and execute arbitrary JavaScript in the site’s context. Version 0.17.2 contains a fix for the issue.	8.3	More Details
CVE-2025-54445	Improper Restriction of XML External Entity Reference vulnerability in Samsung Electronics MagicINFO 9 Server allows Server Side Request Forgery.This issue affects MagicINFO 9 Server: less than 21.1080.0.	8.2	More Details
CVE-2025-52164	Software GmbH Agorum core open v11.9.2 & v11.10.1 was discovered to store credentials in plaintext.	8.2	More Details

CVE-2025-8020	All versions of the package private-ip are vulnerable to Server-Side Request Forgery (SSRF) where an attacker can provide an IP or hostname that resolves to a multicast IP address (224.0.0.0/4) which is not included as part of the private IP ranges in the package's source code.	8.2	More Details
CVE-2024-13974	A business logic vulnerability in the Up2Date component of Sophos Firewall older than version 21.0 MR1 (20.0.1) can lead to attackers controlling the firewall’s DNS environment to achieve remote code execution.	8.1	More Details
CVE-2025-54447	Unrestricted Upload of File with Dangerous Type vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	8.1	More Details
CVE-2025-31700	A vulnerability has been found in Dahua products. Attackers could exploit a buffer overflow vulnerability by sending specially crafted malicious packets, potentially causing service disruption (e.g., crashes) or remote code execution (RCE). Some devices may have deployed protection mechanisms such as Address Space Layout Randomization (ASLR), which reduces the likelihood of successful RCE exploitation. However, denial-of-service (DoS) attacks remain a concern.	8.1	More Details
CVE-2025-8032	XSLT document loading did not correctly propagate the source document which bypassed its CSP. This vulnerability affects Firefox < 141, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	8.1	More Details
CVE-2025-8029	Thunderbird executed `javascript:` URLs when used in `object` and `embed` tags. This vulnerability affects Firefox < 141, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	8.1	More Details
CVE-2025-8030	Insufficient escaping in the “Copy as cURL” feature could potentially be used to trick a user into executing unexpected code. This vulnerability affects Firefox < 141, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	8.1	More Details
CVE-2025-31701	A vulnerability has been found in Dahua products. Attackers could exploit a buffer overflow vulnerability by sending specially crafted malicious packets, potentially causing service disruption (e.g., crashes) or remote code execution (RCE). Some devices may have deployed protection mechanisms such as Address Space Layout Randomization (ASLR), which reduces the likelihood of successful RCE exploitation. However, denial-of-service (DoS) attacks remain a concern.	8.1	More Details
CVE-2025-41425	DuraComm SPM-500 DP-10iN-100-MU is vulnerable to a cross-site scripting attack. This could allow an attacker to prevent legitimate users from accessing the web interface.	8.1	More Details
CVE-2025-8039	In some cases search terms persisted in the URL bar even after navigating away from the search page. This vulnerability affects Firefox < 141, Firefox ESR < 140.1, Thunderbird < 141, and Thunderbird < 140.1.	8.1	More Details
CVE-2025-6585	The WP JobHunt plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 7.2 via the cs_remove_profile_callback() function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete accounts of other users including admins.	8.1	More Details
CVE-2025-7692	The Orion Login with SMS plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.0.5. This is due to the olws_handle_verify_phone() function not utilizing a strong enough OTP value, exposing the hash needed to generate the OTP value, and no restrictions on the number of attempts to submit the code. This makes it possible for unauthenticated attackers to log in as other users, including administrators, if they have access to their phone number.	8.1	More Details
CVE-2025-8036	Thunderbird cached CORS preflight responses across IP address changes. This allowed circumventing CORS with DNS rebinding. This vulnerability affects Firefox < 141, Firefox ESR < 140.1, Thunderbird < 141, and Thunderbird < 140.1.	8.1	More Details
CVE-2025-	The Extensions For CF7 (Contact form 7 Database, Conditional Fields and Redirection) plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'delete-file' field in all versions up to, and including, 3.2.8. This makes it possible for	8.1	More

7645	unauthenticated attackers to delete arbitrary files on the server, when an administrator deletes the submission, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).		Details
CVE-2025-7766	Lantronix Provisioning Manager is vulnerable to XML external entity attacks in configuration files supplied by network devices, leading to unauthenticated remote code execution on hosts with Provisioning Manager installed.	8.0	More Details
CVE-2024-41921	A code injection vulnerability has been discovered in the Robot Operating System (ROS) 'rostopic' command-line tool, affecting ROS distributions Noetic Ninjemys and earlier. The vulnerability lies in the 'echo' verb, which allows a user to introspect a ROS topic and accepts a user-provided Python expression via the --filter option. This input is passed directly to the eval() function without sanitization, allowing a local user to craft and execute arbitrary code.	7.8	More Details
CVE-2025-2633	Out of bounds read vulnerability due to improper bounds checking in NI LabVIEW in lvre!UDecStrToNum that may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q1 and prior versions.	7.8	More Details
CVE-2025-2634	Out of bounds read vulnerability due to improper bounds checking in NI LabVIEW in fontmgr may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q1 and prior versions.	7.8	More Details
CVE-2025-41459	Insufficient protection against brute-force and runtime manipulation in the local authentication component in Two App Studio Journey 5.5.6 on iOS allows local attackers to bypass biometric and PIN-based access control via repeated PIN attempts or dynamic code injection.	7.8	More Details
CVE-2025-6018	A Local Privilege Escalation (LPE) vulnerability has been discovered in pam-config within Linux Pluggable Authentication Modules (PAM). This flaw allows an unprivileged local attacker (for example, a user logged in via SSH) to obtain the elevated privileges normally reserved for a physically present, "allow_active" user. The highest risk is that the attacker can then perform all allow_active yes Polkit actions, which are typically restricted to console users, potentially gaining unauthorized control over system configurations, services, or other sensitive operations.	7.8	More Details
CVE-2025-5042	A maliciously crafted RFA file, when parsed through Autodesk Revit, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2025-54377	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. In versions 3.23.18 and below, RooCode does not validate line breaks (\n) in its command input, allowing potential bypass of the allow-list mechanism. The project appears to lack parsing or validation logic to prevent multi-line command injection. When commands are evaluated for execution, only the first line or token may be considered, enabling attackers to smuggle additional commands in subsequent lines. This is fixed in version 3.23.19.	7.8	More Details
CVE-2025-8069	During the AWS Client VPN client installation on Windows devices, the install process references the C:\usr\local\windows-x86_64-openssl-localbuild\ssl directory location to fetch the OpenSSL configuration file. As a result, a non-admin user could place arbitrary code in the configuration file. If an admin user starts the AWS Client VPN client installation process, that code could be executed with root-level privileges. This issue does not affect Linux or Mac devices. We recommend users discontinue any new installations of AWS Client VPN on Windows prior to version 5.2.2.	7.8	More Details
CVE-2025-7883	A vulnerability classified as critical has been found in Eluktronics Control Center 5.23.51.41. Affected is an unknown function of the file \AiStoneService\MyControlCenter\Command of the component Powershell Script Handler. The manipulation leads to command injection. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.8	More Details
CVE-2025-6231	An improper validation vulnerability was reported in Lenovo Vantage that under certain conditions could allow a local attacker to execute code with elevated permissions by modifying an application configuration file.	7.8	More Details
CVE-2025-	An incorrect permissions vulnerability was reported in Elliptic Labs Virtual Lock Sensor that could allow a local, authenticated user to escalate privileges.	7.8	More Details

0886			
CVE-2025-3753	A code execution vulnerability has been identified in the Robot Operating System (ROS) 'rosbag' tool, affecting ROS distributions Noetic Ninjemys and earlier. The vulnerability arises from the use of the eval() function to process unsanitized, user-supplied input in the 'rosbag filter' command. This flaw enables attackers to craft and execute arbitrary Python code.	7.8	More Details
CVE-2024-41148	A code injection vulnerability has been discovered in the Robot Operating System (ROS) 'rostopic' command-line tool, affecting ROS distributions Noetic Ninjemys and earlier. The vulnerability lies in the 'hz' verb, which reports the publishing rate of a topic and accepts a user-provided Python expression via the --filter option. This input is passed directly to the eval() function without sanitization, allowing a local user to craft and execute arbitrary code.	7.8	More Details
CVE-2024-39835	A code injection vulnerability has been identified in the Robot Operating System (ROS) 'roslaunch' command-line tool, affecting ROS distributions Noetic Ninjemys and earlier. The vulnerability arises from the use of the eval() method to process user-supplied, unsanitized parameter values within the substitution args mechanism, which roslaunch evaluates before launching a node. This flaw allows attackers to craft and execute arbitrary Python code.	7.8	More Details
CVE-2024-39289	A code execution vulnerability has been discovered in the Robot Operating System (ROS) 'rosparam' tool, affecting ROS distributions Noetic Ninjemys and earlier. The vulnerability stems from the use of the eval() function to process unsanitized, user-supplied parameter values via special converters for angle representations in radians. This flaw allowed attackers to craft and execute arbitrary Python code.	7.8	More Details
CVE-2025-6232	An improper validation vulnerability was reported in Lenovo Vantage that under certain conditions could allow a local attacker to execute code with elevated permissions by modifying specific registry locations.	7.8	More Details
CVE-2025-6741	Improper access control in secure message component in Devolutions Server allows an authenticated user to steal unauthorized entries via the secure message entry attachment feature This issue affects the following versions : * Devolutions Server 2025.2.2.0 through 2025.2.4.0 * Devolutions Server 2025.1.11.0 and earlier	7.7	More Details
CVE-2025-47281	Kyverno is a policy engine designed for cloud native platform engineering teams. In versions 1.14.1 and below, a Denial of Service (DoS) vulnerability exists due to improper handling of JMESPath variable substitutions. Attackers with permissions to create or update Kyverno policies can craft expressions using the {{@}} variable combined with a pipe and an invalid JMESPath function (e.g., {{@ | non_existent_function }}). This leads to a nil value being substituted into the policy structure. Subsequent processing by internal functions, specifically getValueAsStringMap, which expect string values, results in a panic due to a type assertion failure (interface {} is nil, not string). This crashes Kyverno worker threads in the admission controller and causes continuous crashes of the reports controller pod. This is fixed in version 1.14.2.	7.7	More Details
CVE-2025-4439	An issue has been discovered in GitLab CE/EE affecting all versions from 15.10 before 18.0.5, 18.1 before 18.1.3, and 18.2 before 18.2.1 that could have allowed an authenticated user to perform cross-site scripting attacks when the instance is served through certain content delivery networks.	7.7	More Details
CVE-2025-6523	Use of weak credentials in emergency authentication component in Devolutions Server allows an unauthenticated attacker to bypass authentication via brute forcing the short emergency codes generated by the server within a feasible timeframe. This issue affects the following versions : * Devolutions Server 2025.2.2.0 through 2025.2.3.0 * Devolutions Server 2025.1.11.0 and earlier	7.7	More Details
CVE-2025-23263	NVIDIA DOCA-Host and Mellanox OFED contain a vulnerability in the VGT+ feature, where an attacker on a VM might cause escalation of privileges and denial of service on the VLAN.	7.6	More Details
CVE-2025-6023	An open redirect vulnerability has been identified in Grafana OSS that can be exploited to achieve XSS attacks. The vulnerability was introduced in Grafana v11.5.0. The open redirect can be chained with path traversal vulnerabilities to achieve XSS. Fixed in versions 12.0.2+security-01, 11.6.3+security-01, 11.5.6+security-01, 11.4.6+security-01 and 11.3.8+security-01	7.6	More Details
	Cadwyn creates production-ready community-driven modern Stripe-like API versioning in		

CVE-2025-53528	FastAPI. In versions before 5.4.3, the version parameter of the "/docs" endpoint is vulnerable to a Reflected XSS (Cross-Site Scripting) attack. This XSS would notably allow an attacker to execute JavaScript code on a user's session for any application based on Cadwyn via a one-click attack. The vulnerability has been fixed in version 5.4.3.	7.6	More Details
CVE-2025-35966	A null pointer dereference vulnerability exists in the CDB2SQLQUERY protocol buffer message handling of Bloomberg Comdb2 8.1. A specially crafted protocol buffer message can lead to a denial of service. An attacker can simply connect to a database instance over TCP and send the crafted message to trigger this vulnerability.	7.5	More Details
CVE-2025-4130	Use of Hard-coded Credentials vulnerability in PAVO Inc. PAVO Pay allows Read Sensitive Constants Within an Executable.This issue affects PAVO Pay: before 13.05.2025.	7.5	More Details
CVE-2025-54140	pyLoad is a free and open-source Download Manager written in pure Python. In version 0.5.0b3.dev89, an authenticated path traversal vulnerability exists in the /json/upload endpoint of pyLoad. By manipulating the filename of an uploaded file, an attacker can traverse out of the intended upload directory, allowing them to write arbitrary files to any location on the system accessible to the pyLoad process. This may lead to: Remote Code Execution (RCE), local privilege escalation, system-wide compromise, persistence, and backdoors. This is fixed in version 0.5.0b3.dev90.	7.5	More Details
CVE-2025-4129	Authorization Bypass Through User-Controlled Key vulnerability in PAVO Inc. PAVO Pay allows Exploitation of Trusted Identifiers.This issue affects PAVO Pay: before 13.05.2025.	7.5	More Details
CVE-2025-30192	An attacker spoofing answers to ECS enabled requests sent out by the Recursor has a chance of success higher than non-ECS enabled queries. The updated version include various mitigations against spoofing attempts of ECS enabled queries by chaining ECS enabled requests and enforcing stricter validation of the received answers. The most strict mitigation done when the new setting outgoing.edns_subnet_harden (old style name edns-subnet-harden) is enabled.	7.5	More Details
CVE-2025-54073	mcp-package-docs is an MCP (Model Context Protocol) server that provides LLMs with efficient access to package documentation across multiple programming languages and language server protocol (LSP) capabilities. A command injection vulnerability exists in the `mcp-package-docs` MCP Server prior to the fix in commit cb4ad49615275379fd6f2f1cf1ec4731eec56eb9. The vulnerability is caused by the unsanitized use of input parameters within a call to `child_process.exec`, enabling an attacker to inject arbitrary system commands. Successful exploitation can lead to remote code execution under the server process's privileges. The server constructs and executes shell commands using unvalidated user input directly within command-line strings. This introduces the possibility of shell metacharacter injection (`|`, `>`, `&&`, etc.). Commit cb4ad49615275379fd6f2f1cf1ec4731eec56eb9 in version 0.1.27 contains a fix for the issue, but upgrading to 0.1.28 is recommended.	7.5	More Details
CVE-2025-40597	A Heap-based buffer overflow vulnerability in the SMA100 series web interface allows remote, unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution.	7.5	More Details
CVE-2025-54138	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring which includes support for a wide range of network hardware and operating systems. LibreNMS versions 25.6.0 and below contain an architectural vulnerability in the ajax_form.php endpoint that permits Remote File Inclusion based on user-controlled POST input. The application directly uses the type parameter to dynamically include .inc.php files from the trusted path includes/html/forms/, without validation or allowlisting. This pattern introduces a latent Remote Code Execution (RCE) vector if an attacker can stage a file in this include path — for example, via symlink, development misconfiguration, or chained vulnerabilities. This is fixed in version 25.7.0.	7.5	More Details
CVE-2025-7472	A local privilege escalation vulnerability in the Intercept X for Windows installer prior version 1.22 can lead to a local user gaining system level privileges, if the installer is run as SYSTEM.	7.5	More Details
CVE-2025-7338	Multer is a node.js middleware for handling `multipart/form-data`. A vulnerability that is present starting in version 1.4.4-lts.1 and prior to version 2.0.2 allows an attacker to trigger a Denial of Service (DoS) by sending a malformed multi-part upload request. This request causes an unhandled exception, leading to a crash of the process. Users should upgrade to version 2.0.2 to receive a patch. No known workarounds are available.	7.5	More Details

CVE-2025-49656	Users with administrator access can create databases files outside the files area of the Fuseki server. This issue affects Apache Jena version up to 5.4.0. Users are recommended to upgrade to version 5.5.0, which fixes the issue.	7.5	More Details
CVE-2025-47187	A vulnerability in the Mitel 6800 Series, 6900 Series, and 6900w Series SIP Phones, including the 6970 Conference Unit through 6.4 SP4, could allow an unauthenticated attacker to perform a file upload attack due to missing authentication mechanisms. A successful exploit could allow an attacker to upload arbitrary WAV files, which may potentially exhaust the phone's storage without affecting the phone's availability or operation.	7.5	More Details
CVE-2025-54072	yt-dlp is a feature-rich command-line audio/video downloader. In versions 2025.06.25 and below, when the --exec option is used on Windows with the default placeholder (or {}), insufficient sanitization is applied to the expanded filepath, allowing for remote code execution. This is a bypass of the mitigation for CVE-2024-22423 where the default placeholder and {} were not covered by the new escaping rules. Windows users who are unable to upgrade should avoid using --exec altogether. Instead, the --write-info-json or --dump-json options could be used, with an external script or command line consuming the JSON output. This is fixed in version 2025.07.21.	7.5	More Details
CVE-2025-53703	DuraComm SPM-500 DP-10iN-100-MU transmits sensitive data without encryption over a channel that could be intercepted by attackers.	7.5	More Details
CVE-2025-36512	A denial of service vulnerability exists in the Bloomberg Comdb2 8.1 database when handling a distributed transaction heartbeat. A specially crafted protocol buffer message can lead to a denial of service. An attacker can simply connect to a database instance over TCP and send the crafted message to trigger this vulnerability.	7.5	More Details
CVE-2025-1713	When setting up interrupt remapping for legacy PCI(-X) devices, including PCI(-X) bridges, a lookup of the upstream bridge is required. This lookup, itself involving acquiring of a lock, is done in a context where acquiring that lock is unsafe. This can lead to a deadlock.	7.5	More Details
CVE-2025-48733	DuraComm SPM-500 DP-10iN-100-MU lacks access controls for a function that should require user authentication. This could allow an attacker to repeatedly reboot the device.	7.5	More Details
CVE-2025-1469	Authorization Bypass Through User-Controlled Key vulnerability in Turtek Software Eyotek allows Exploitation of Trusted Identifiers.This issue affects Eyotek: before 11.03.2025.	7.5	More Details
CVE-2025-50708	An issue in Perplexity AI GPT-4 v.2.51.0 allows a remote attacker to obtain sensitive information via the token component in the shared chat URL	7.5	More Details
CVE-2025-54313	eslint-config-prettier 8.10.1, 9.1.1, 10.1.6, and 10.1.7 has embedded malicious code for a supply chain compromise. Installing an affected package executes an install.js file that launches the node-gyp.dll malware on Windows.	7.5	More Details
CVE-2025-51869	Insecure Direct Object Reference (IDOR) vulnerability in Liner thru 2025-06-03 allows attackers to gain sensitive information via crafted space_id, thread_id, and message_id parameters to the v1/space/{space_id}/thread/{thread_id}/message/{message_id} endpoint.	7.5	More Details
CVE-2025-51868	Insecure Direct Object Reference (IDOR) vulnerability in Dippy (chat.dippy.ai) v2 allows attackers to gain sensitive information via the conversation_id parameter to the conversation_history endpoint.	7.5	More Details
CVE-2025-7735	The Hospital Information System developed by UNIMAX has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read database contents.	7.5	More Details
CVE-2025-53832	Lara Translate MCP Server is a Model Context Protocol (MCP) Server for Lara Translate API. Versions 0.0.11 and below contain a command injection vulnerability which exists in the @translated/lara-mcp MCP Server. The vulnerability is caused by the unsanitized use of input parameters within a call to child_process.exec, enabling an attacker to inject arbitrary system commands. Successful exploitation can lead to remote code execution under the server process's privileges. The server constructs and executes shell commands using unvalidated user	7.5	More Details

	input directly within command-line strings. This introduces the possibility of shell metacharacter injection (|, >, &&, etc.). This vulnerability is fixed in version 0.0.12.		
CVE-2025-8021	All versions of the package files-bucket-server are vulnerable to Directory Traversal where an attacker can traverse the file system and access files outside of the intended directory.	7.5	More Details
CVE-2025-44652	In Netgear RAX30 V1.0.10.94_3, the USERLIMIT_GLOBAL option is set to 0 in multiple bftpd-related configuration files. This can cause DoS attacks when unlimited users are connected.	7.5	More Details
CVE-2025-7717	Missing Authorization vulnerability in Drupal File Download allows Forceful Browsing.This issue affects File Download: from 0.0.0 before 1.9.0, from 2.0.0 before 2.0.1.	7.5	More Details
CVE-2025-44653	In H3C GR2200 MiniGR1A0V100R016, the USERLIMIT_GLOBAL option is set to 0 in the /etc/bftpd.conf. This can cause DoS attacks when unlimited users are connected.	7.5	More Details
CVE-2025-44649	In the configuration file of racoon in the TRENDnet TEW-WLC100P 2.03b03, the first item of exchage_mode is set to aggressive. Aggressive mode in IKE Phase 1 exposes identity information in plaintext, is vulnerable to offline dictionary attacks, and lacks flexibility in negotiating security parameters.	7.5	More Details
CVE-2025-7438	The MasterStudy LMS Pro plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the 'install_and_activate_plugin' function in all versions up to, and including, 4.7.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. The vulnerability is difficult to exploit due to timing requirements and environmental factors.	7.5	More Details
CVE-2025-53537	LibHTP is a security-aware parser for the HTTP protocol and its related bits and pieces. In versions 0.5.50 and below, there is a traffic-induced memory leak that can starve the process of memory, leading to loss of visibility. To workaround this issue, set `suricata.yaml app-layer.protocols.http.libhtp.default-config.lzma-enabled` to false. This issue is fixed in version 0.5.51.	7.5	More Details
CVE-2025-48498	A null pointer dereference vulnerability exists in the Distributed Transaction component of Bloomberg Comdb2 8.1 when processing a number of fields used for coordination. A specially crafted protocol buffer message can lead to a denial of service. An attacker can simply connect to a database instance over TCP and send the crafted message to trigger this vulnerability.	7.5	More Details
CVE-2025-44651	In TRENDnet TPL-430AP FW1.0, the USERLIMIT_GLOBAL option is set to 0 in the bftpd-related configuration file. This can cause DoS attacks when unlimited users are connected.	7.5	More Details
CVE-2025-44650	In Netgear R7000 V1.3.1.64_10.1.36 and EAX80 V1.0.1.70_1.0.2, the USERLIMIT_GLOBAL option is set to 0 in the bftpd.conf configuration file. This can cause DoS attacks when unlimited users are connected.	7.5	More Details
CVE-2015-10136	The GI-Media Library plugin for WordPress is vulnerable to Directory Traversal in versions before 3.0 via the 'fileid' parameter. This allows unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	7.5	More Details
CVE-2025-46354	A denial of service vulnerability exists in the Distributed Transaction Commit/Abort Operation functionality of Bloomberg Comdb2 8.1. A specially crafted network packet can lead to a denial of service. An attacker can send a malicious packet to trigger this vulnerability.	7.5	More Details
CVE-2025-54141	ViewVC is a browser interface for CVS and Subversion version control repositories. In versions 1.1.0 through 1.1.31 and 1.2.0 through 1.2.3, the standalone.py script provided in the ViewVC distribution can expose the contents of the host server's filesystem though a directory traversal-style attack. This is fixed in versions 1.1.31 and 1.2.4.	7.5	More Details
CVE-2015-10134	The Simple Backup plugin for WordPress is vulnerable to Arbitrary File Download in versions up to, and including, 2.7.10. via the download_backup_file function. This is due to a lack of capability checks and file type validation. This makes it possible for attackers to download	7.5	More Details

	sensitive files such as the wp-config.php file from the affected site.		
CVE-2025-36520	A null pointer dereference vulnerability exists in the net_connectmsg Protocol Buffer Message functionality of Bloomberg Comdb2 8.1. A specially crafted network packets can lead to a denial of service. An attacker can send packets to trigger this vulnerability.	7.5	More Details
CVE-2025-53538	Suricata is a network IDS, IPS and NSM engine developed by the OISF (Open Information Security Foundation) and the Suricata community. In versions 7.0.10 and below and 8.0.0-beta1 through 8.0.0-rc1, mishandling of data on HTTP2 stream 0 can lead to uncontrolled memory usage, leading to loss of visibility. Workarounds include disabling the HTTP/2 parser, and using a signature like drop http2 any any -> any any (frame:http2.hdr; byte_test:1,=,0,3; byte_test:4,=,0,5; sid: 1;) where the first byte test tests the HTTP2 frame type DATA and the second tests the stream id 0. This is fixed in versions 7.0.11 and 8.0.0.	7.5	More Details
CVE-2025-6248	A cross-site scripting (XSS) vulnerability was reported in the Lenovo Browser that could allow an attacker to obtain sensitive information if a user visits a web page with specially crafted content.	7.4	More Details
CVE-2025-7814	A vulnerability classified as critical was found in code-projects Food Ordering Review System 1.0. This vulnerability affects unknown code of the file /pages/signup_function.php. The manipulation of the argument fname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	7.3	More Details
CVE-2025-7861	A vulnerability, which was classified as critical, was found in code-projects Church Donation System 1.0. Affected is an unknown function of the file /members/search.php. The manipulation of the argument Username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7915	A vulnerability was found in Chanjet CRM 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /mail/mailinactive.php of the component Login Page. The manipulation 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-2025-54137	HAX CMS NodeJS allows users to manage their microsite universe with a NodeJS backend. Versions 11.0.9 and below were distributed with hardcoded default credentials for the user and superuser accounts. Additionally, the application has default private keys for JWTs. Users aren't prompted to change credentials or secrets during installation, and there is no way to change them through the UI. An unauthenticated attacker can read the default user credentials and JWT private keys from the public haxtheweb GitHub repositories. These credentials and keys can be used to access unconfigured self-hosted instances of the application, modify sites, and perform further attacks. This is fixed in version 11.0.10.	7.3	More Details
CVE-2025-7875	A vulnerability classified as critical has been found in Metasoft 美特软件 MetaCRM up to 6.4.2. This affects an unknown part of the file /debug.jsp. The manipulation leads to improper authentication. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-7832	A vulnerability classified as critical was found in code-projects Church Donation System 1.0. This vulnerability affects unknown code of the file /members/offering.php. The manipulation of the argument trcode leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7897	A vulnerability was found in harry0703 MoneyPrinterTurbo up to 1.2.6 and classified as critical. Affected by this issue is the function verify_token of the file app/controllers/base.py of the component API Endpoint. The manipulation leads to missing authentication. The attack may be launched remotely.	7.3	More Details
CVE-2025-7860	A vulnerability, which was classified as critical, has been found in code-projects Church Donation System 1.0. This issue affects some unknown processing of the file /members/login_admin.php. The manipulation of the argument Username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-	A vulnerability classified as critical was found in code-projects Church Donation System 1.0. This vulnerability affects unknown code of the file /members/update_password_admin.php. The	7.3	More

7859	manipulation of the argument new_password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		Details
CVE-2025-7886	A vulnerability, which was classified as critical, was found in pmTicket Project-Management-Software up to 2ef379da2075f4761a2c9029cf91d073474e7486. This affects the function getUserLanguage of the file classes/class.database.php. The manipulation of the argument user_id leads to sql injection. It is possible to initiate the attack remotely. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2025-7838	A vulnerability has been found in Campcodes Online Movie Theater Seat Reservation System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/manage_seat.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7823	A vulnerability was found in Jinher OA 1.2. It has been declared as problematic. This vulnerability affects unknown code of the file ProjectScheduleDelete.aspx. The manipulation leads to xml external entity reference. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7824	A vulnerability was found in Jinher OA 1.1. It has been rated as problematic. This issue affects some unknown processing of the file XmlHttp.aspx. The manipulation leads to xml external entity reference. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7829	A vulnerability was found in code-projects Church Donation System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /login.php. The manipulation of the argument Username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7830	A vulnerability was found in code-projects Church Donation System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /reg.php. The manipulation of the argument mobile leads to sql injection. 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.	7.3	More Details
CVE-2025-7833	A vulnerability, which was classified as critical, has been found in code-projects Church Donation System 1.0. This issue affects some unknown processing of the file /members/giving.php. The manipulation of the argument Amount leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7831	A vulnerability classified as critical has been found in code-projects Church Donation System 1.0. This affects an unknown part of the file /members/Tithes.php. The manipulation of the argument trcode leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7862	A vulnerability has been found in TOTOLINK T6 4.1.5cu.748_B20211015 and classified as critical. Affected by this vulnerability is the function setTelnetCfg of the file /cgi-bin/cstecgi.cgi of the component Telnet Service. The manipulation of the argument telnet_enabled with the input 1 leads to missing authentication. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-54452	Improper Authentication vulnerability in Samsung Electronics MagicINFO 9 Server allows Authentication Bypass.This issue affects MagicINFO 9 Server: less than 21.1080.0.	7.3	More Details
CVE-2025-40596	A Stack-based buffer overflow vulnerability in the SMA100 series web interface allows remote, unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution.	7.3	More Details
CVE-2025-7928	A vulnerability was found in code-projects Church Donation System 1.0 and classified as critical. This issue affects some unknown processing of the file /members/edit_user.php. The manipulation of the argument firstname leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	7.3	More Details

CVE-2025-7929	A vulnerability was found in code-projects Church Donation System 1.0. It has been classified as critical. Affected is an unknown function of the file /members/edit_Members.php. The manipulation of the argument fname leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	7.3	More Details
CVE-2025-7930	A vulnerability was found in code-projects Church Donation System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /members/add_members.php. The manipulation of the argument mobile leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	7.3	More Details
CVE-2025-31511	An issue was discovered in AlertEnterprise Guardian 4.1.14.2.2.1. One can bypass manager approval by changing the user ID in a Request%20Building%20Access requestSubmit API call.	7.3	More Details
CVE-2025-7931	A vulnerability was found in code-projects Church Donation System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /members/admin_pic.php. The manipulation of the argument image leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7801	A vulnerability has been found in BossSoft CRM 6.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /crm/module/HNDCBas_customPrmSearchDtl.jsp. The manipulation of the argument cstid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7933	A vulnerability classified as critical was found in Campcodes Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /pages/settings_update.php of the component Setting Handler. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7749	A vulnerability, which was classified as critical, has been found in code-projects Online Appointment Booking System 1.0. This issue affects some unknown processing of the file /admin/getmanagerregion.php. The manipulation of the argument city leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7750	A vulnerability, which was classified as critical, was found in code-projects Online Appointment Booking System 1.0. Affected is an unknown function of the file /admin/adddoctorclinic.php. The manipulation of the argument clinic leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7765	A vulnerability classified as critical was found in code-projects Online Appointment Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/addmanagerclinic.php. The manipulation of the argument clinic leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7764	A vulnerability classified as critical has been found in code-projects Online Appointment Booking System 1.0. Affected is an unknown function of the file /admin/deletedoctorclinic.php. The manipulation of the argument clinic leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7757	A vulnerability classified as critical was found in PHPGurukul Land Record System 1.0. Affected by this vulnerability is an unknown functionality of the file /edit-property.php. The manipulation of the argument editid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-7753	A vulnerability was found in code-projects Online Appointment Booking System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/adddoctor.php. The manipulation of the argument Username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
	A vulnerability was found in code-projects Online Appointment Booking System 1.0 and		

CVE-2025-7752	classified as critical. Affected by this issue is some unknown functionality of the file /admin/deletedoctor.php. The manipulation of the argument did 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-2025-7751	A vulnerability has been found in code-projects Online Appointment Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/addclinic.php. The manipulation of the argument cid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-31512	An issue was discovered in AlertEnterprise Guardian 4.1.14.2.2.1. One can bypass manager approval via isAddedByApprover in a Request%20Building%20Access requestSubmit API call.	7.3	More Details
CVE-2025-44647	In TRENDnet TEW-WLC100P 2.03b03, the i_dont_care_about_security_and_use_aggressive_mode_psk option is enabled in the strongSwan configuration file, so that IKE Responders are allowed to use IKEv1 Aggressive Mode with Pre-Shared Keys to conduct offline attacks on the openly transmitted hash of the PSK.	7.3	More Details
CVE-2025-46118	An issue was discovered in CommScope Ruckus Unleashed prior to 200.15.6.212.14 and 200.17.7.0.139 and in Ruckus ZoneDirector prior to 10.5.1.0.279, where hard-coded credentials for the ftpuser account provide FTP access to the controller, enabling a remote attacker to upload or retrieve arbitrary files from writable firmware directories and thereby expose sensitive information or compromise the controller.	7.3	More Details
CVE-2025-7950	A vulnerability was found in code-projects Public Chat Room 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /login.php. The manipulation of the argument Username 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-2025-53472	WRC-BE36QS-B and WRC-W701-B contain an improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in WebGUI. If exploited, an arbitrary OS command may be executed by a remote attacker who can log in to WebGUI.	7.2	More Details
CVE-2025-41673	A high privileged remote attacker can execute arbitrary system commands via POST requests in the send_sms action due to improper neutralization of special elements used in an OS command.	7.2	More Details
CVE-2025-54450	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Samsung Electronics MagicINFO 9 Server allows Code Injection.This issue affects MagicINFO 9 Server: less than 21.1080.0.	7.2	More Details
CVE-2025-41674	A high privileged remote attacker can execute arbitrary system commands via POST requests in the diagnostic action due to improper neutralization of special elements used in an OS command.	7.2	More Details
CVE-2015-10133	The Subscribe to Comments for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 2.1.2 via the Path to header value. This allows authenticated attackers, with administrative privileges and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included. This same function can also be used to execute arbitrary PHP code.	7.2	More Details
CVE-2025-41675	A high privileged remote attacker can execute arbitrary system commands via GET requests in the cloud server communication script due to improper neutralization of special elements used in an OS command.	7.2	More Details
CVE-2024-53286	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in DDNS Record functionality in Synology Router Manager (SRM) before 1.3.1-9346-11 allows remote authenticated users with administrator privileges to execute arbitrary code via unspecified vectors.	7.2	More Details
CVE-	The Nginx Cache Purge Preload plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.1.1 via the 'nppp_preload_cache_on_update' function. This is due to insufficient sanitization of the $_SERVER['HTTP_REFERERER'] parameter passed from the		More

2025-6213	'nppp_handle_fastcgi_cache_actions_admin_bar' function. This makes it possible for authenticated attackers, with Administrator-level access and above, to execute code on the server.	7.2	Details
CVE-2025-7917	WinMatrix3 Web package developed by Simopro Technology has an Arbitrary File Upload vulnerability, allowing remote attackers with administrator privileges to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	7.2	More Details
CVE-2025-4040	Authorization Bypass Through User-Controlled Key vulnerability in Turpak Automatic Station Monitoring System allows Privilege Escalation.This issue affects Automatic Station Monitoring System: before 5.0.6.51.	7.1	More Details
CVE-2025-46099	In Pluck CMS 4.7.20-dev, an authenticated attacker can upload or create a crafted PHP file under the albums module directory and access it via the module routing logic in albums.site.php, resulting in arbitrary command execution through a GET parameter.	7.1	More Details
CVE-2025-52169	agorum Software GmbH Agorum core open v11.9.2 & v11.10.1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability.	7.1	More Details
CVE-2025-23270	NVIDIA Jetson Linux contains a vulnerability in UEFI Management mode, where an unprivileged local attacker may cause exposure of sensitive information via a side channel vulnerability. A successful exploit of this vulnerability might lead to code execution, data tampering, denial of service, and information disclosure.	7.1	More Details
CVE-2025-53945	apko allows users to build and publish OCI container images built from apk packages. Starting in version 0.27.0 and prior to version 0.29.5, critical files were inadvertently set to 0666, which could likely be abused for root escalation. Version 0.29.5 contains a fix for the issue.	7.0	More Details
CVE-2025-1700	A DLL hijacking vulnerability was reported in the Motorola Software Fix (Rescue and Smart Assistant) installer that could allow a local attacker to escalate privileges during installation of the software.	7.0	More Details
CVE-2025-51463	Path Traversal in restore_run_backup() in AIM 3.28.0 allows remote attackers to write arbitrary files to the server's filesystem via a crafted backup tar file submitted to the run_instruction API, which is extracted without path validation during restoration.	7.0	More Details
CVE-2025-51471	Cross-Domain Token Exposure in server.auth.getAuthorizationToken in Ollama 0.6.7 allows remote attackers to steal authentication tokens and bypass access controls via a malicious realm value in a WWW-Authenticate header returned by the /api/pull endpoint.	6.9	More Details
CVE-2025-7705	: Active Debug Code vulnerability in ABB Switch Actuator 4 DU-83330, ABB Switch actuator, door/light 4 DU -83330-500.This issue affects Switch Actuator 4 DU-83330: All Versions; Switch actuator, door/light 4 DU -83330-500: All Versions.	6.8	More Details
CVE-2025-6233	Mattermost versions 10.8.x <= 10.8.1, 10.7.x <= 10.7.3, 10.5.x <= 10.5.7, 9.11.x <= 9.11.16 fail to sanitize input paths of file attachments in the bulk import JSONL file, which allows a system admin to read arbitrary system files via path traversal.	6.8	More Details
CVE-2025-7371	Okta On-Premises Provisioning (OPP) agents log certain user data during administrator-initiated password resets. This vulnerability allows an attacker with access to the local servers running OPP agents to retrieve user personal information and temporary passwords created during password reset. You are affected by this vulnerability if the following preconditions are met: Local server running OPP agent with versions >=2.2.1 and <= 2.3.0, and User account has had an administrator-initiated password reset while using the affected versions.	6.8	More Details
CVE-2024-13973	A post-auth SQL injection vulnerability in WebAdmin of Sophos Firewall versions older than 21.0 MR1 (21.0.1) can potentially lead to administrators achieving arbitrary code execution.	6.8	More Details
CVE-2025-6249	An authentication bypass vulnerability was reported in FileZ client application that could allow a local attacker with elevated permissions access to application data.	6.7	More Details
CVE-2025-	A buffer overflow vulnerability was reported in the Lenovo Protection Driver, prior to version 5.1.1110.4231, used in Lenovo PC Manager, Lenovo Browser, and Lenovo App Store could allow	6.7	More Details

4657	a local attacker with elevated privileges to execute arbitrary code.		
CVE-2025-1729	A DLL hijacking vulnerability was reported in TrackPoint Quick Menu software that, under certain conditions, could allow a local attacker to escalate privileges.	6.7	More Details
CVE-2024-27779	An insufficient session expiration vulnerability [CWE-613] in FortiSandbox FortiSandbox version 4.4.4 and below, version 4.2.6 and below, 4.0 all versions, 3.2 all versions and FortiIsolator version 2.4 and below, 2.3 all versions, 2.2 all versions, 2.1 all versions, 2.0 all versions, 1.2 all versions may allow a remote attacker in possession of an admin session cookie to keep using that admin's session even after the admin user was deleted.	6.7	More Details
CVE-2025-51481	Local File Inclusion in dagster._grpc.impl.get_notebook_data in Dagster 1.10.14 allows attackers with access to the gRPC server to read arbitrary files by supplying path traversal sequences in the notebook_path field of ExternalNotebookData requests, bypassing the intended extension-based check.	6.6	More Details
CVE-2025-32744	Dell AppSync, version(s) 4.6.0.0, contains an Unrestricted Upload of File with Dangerous Type vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Remote execution.	6.6	More Details
CVE-2025-51867	Insecure Direct Object Reference (IDOR) vulnerability in Deepfiction AI (deepfiction.ai) thru June 3, 2025, allowing attackers to chat with the LLM using other users' credits via sensitive information gained by the /browse/stories endpoint.	6.5	More Details
CVE-2025-51859	Stored Cross-Site Scripting (XSS) vulnerability in Chaindesk thru 2025-05-26 in its agent chat component. An attacker can achieve arbitrary client-side script execution by crafting an AI agent whose system prompt instructs the underlying Large Language Model (LLM) to embed malicious script payloads (e.g., SVG-based XSS) into its chat responses. When a user interacts with such a malicious agent or accesses a direct link to a conversation containing an XSS payload, the script executes in the user's browser. Successful exploitation can lead to the theft of sensitive information, such as JWT session tokens, potentially resulting in account hijacking.	6.5	More Details
CVE-2025-51864	A reflected cross-site scripting (XSS) vulnerability exists in AIBOX LLM chat (chat.aibox365.cn) through 2025-05-27, allowing attackers to hijack accounts through stolen JWT tokens.	6.5	More Details
CVE-2025-7919	WinMatrix3 Web package developed by Simopro Technology has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.	6.5	More Details
CVE-2025-48964	ping in iputils before 20250602 allows a denial of service (application error in adaptive ping mode or incorrect data collection) via a crafted ICMP Echo Reply packet, because a zero timestamp can lead to large intermediate values that have an integer overflow when squared during statistics calculations. NOTE: this issue exists because of an incomplete fix for CVE-2025-47268 (that fix was only about timestamp calculations, and it did not account for a specific scenario where the original timestamp in the ICMP payload is zero).	6.5	More Details
CVE-2025-51459	File Upload vulnerability in agent.hub.controller.refresh_plugins in eosphoros-ai DB-GPT 0.7.0 allows remote attackers to execute arbitrary code via a malicious plugin ZIP file uploaded to the /v1/personal/agent/upload endpoint, interacting with plugin_hub._sanitize_filename and plugins_util.scan_plugins.	6.5	More Details
CVE-2025-51403	A stored cross-site scripting (XSS) vulnerability in the department assignment editing module of of Live Helper Chat v4.60 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Alias Nick parameter.	6.5	More Details
CVE-2025-36106	IBM Cognos Analytics Mobile (iOS) 1.1.0 through 1.1.22 could allow malicious actors to view and modify information coming to and from the application which could then be used to access confidential information on the device or network by using a the deprecated or misconfigured AFNetworking library at runtime.	6.5	More Details
CVE-2025-8033	The JavaScript engine did not handle closed generators correctly and it was possible to resume them leading to a nullptr deref. This vulnerability affects Firefox < 141, Firefox ESR < 115.26, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	6.5	More Details

CVE-2025-31513	An issue was discovered in AlertEnterprise Guardian 4.1.14.2.2.1. One can elevate to administrator privileges via the IsAdminApprover parameter in a Request%20Building%20Access requestSubmit API call.	6.5	More Details
CVE-2025-51458	SQL Injection in editor_sql_run and query_ex in eosphoros-ai DB-GPT 0.7.0 allows remote attackers to execute arbitrary SQL statements via crafted input passed to the /v1/editor/sql/run or /v1/editor/chart/run endpoints, interacting with api_editor_v1.editor_sql_run, editor_chart_run, and datasource.rdbms.base.query_ex.	6.5	More Details
CVE-2025-51472	Code Injection in AgentTemplate.eval_agent_config in TransformerOptimus SuperAGI 0.0.14 allows remote attackers to execute arbitrary Python code via malicious values in agent template configurations such as the goal, constraints, or instruction field, which are evaluated using eval() without validation during template loading or updates.	6.5	More Details
CVE-2025-53771	Improper limitation of a pathname to a restricted directory ('path traversal') in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2025-5681	Authorization Bypass Through User-Controlled Key vulnerability in Turtek Software Eyotek allows Exploitation of Trusted Identifiers.This issue affects Eyotek: before 23.06.2025.	6.5	More Details
CVE-2025-41678	A high privileged remote attacker can alter the configuration database via POST requests due to improper neutralization of special elements used in a SQL statement.	6.5	More Details
CVE-2025-8027	On 64-bit platforms IonMonkey-JIT only wrote 32 bits of the 64-bit return value space on the stack. Baseline-JIT, however, read the entire 64 bits. This vulnerability affects Firefox < 141, Firefox ESR < 115.26, Firefox ESR < 128.13, Firefox ESR < 140.1, Thunderbird < 141, Thunderbird < 128.13, and Thunderbird < 140.1.	6.5	More Details
CVE-2025-52575	EspoCRM is an Open Source CRM (Customer Relationship Management) software. EspoCRM versions 9.1.6 and earlier are vulnerable to blind LDAP Injection when LDAP authentication is enabled. A remote, unauthenticated attacker can manipulate LDAP queries by injecting crafted input containing wildcard characters (e.g., *). This may allow the attacker to bypass authentication controls, enumerate valid usernames, or retrieve sensitive directory information depending on the LDAP server configuration. This was fixed in version 9.1.7.	6.5	More Details
CVE-2025-43720	Headwind MDM before 5.33.1 makes configuration details accessible to unauthorized users. The Configuration profile is exposed to the Observer user role, revealing the password requires to escape out of the MDM controlled device's profile.	6.5	More Details
CVE-2025-54078	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in versions prior to 3.4.6 in the `personalizacao_imagem.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the `err` parameter. Version 3.4.6 fixes the issue.	6.5	More Details
CVE-2025-52166	Incorrect access control in Software GmbH Agorum core open v11.9.2 & v11.10.1 allows authenticated attackers to escalate privileges to Administrator and access sensitive components and information.	6.5	More Details
CVE-2025-6226	Mattermost versions 10.5.x <= 10.5.6, 10.8.x <= 10.8.1, 10.7.x <= 10.7.3, 9.11.x <= 9.11.16 fail to verify authorization when retrieving cached posts by PendingPostID which allows an authenticated user to read posts in private channels they don't have access to via guessing the PendingPostID of recently created posts.	6.5	More Details
CVE-2025-4411	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Dataprom Informatics PACS-ACSS allows Cross-Site Scripting (XSS).This issue affects PACS-ACSS: before 16.05.2025.	6.5	More Details
CVE-2025-7772	The Malcure Malware Scanner — #1 Toolset for WordPress Malware Removal plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 16.8 via the wpmr_inspect_file() function due to a missing capability check. This makes it possible for authenticated attackers, with subscriber-level access and above, to read the contents of	6.5	More Details

	arbitrary files on the server, which can contain sensitive information.		
CVE-2025-40924	Catalyst::Plugin::Session before version 0.44 for Perl generates session ids insecurely. The session id is generated from a (usually SHA-1) hash of a simple counter, the epoch time, the built-in rand function, the PID and the current Catalyst context. This information is of low entropy. The PID will come from a small set of numbers, and the epoch time may be guessed, if it is not leaked from the HTTP Date header. The built-in rand function is unsuitable for cryptographic usage. Predicable session ids could allow an attacker to gain access to systems.	6.5	More Details
CVE-2025-6214	The Omnishop plugin for WordPress is vulnerable to Cross-Site Request Forgery on its /users/delete REST route in all versions up to, and including, 1.0.9. The route's permission_callback only verifies that the requester is logged in, but fails to require any nonce or other proof of intent. This makes it possible for unauthenticated attackers to delete arbitrary user accounts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.5	More Details
CVE-2025-52163	A Server-Side Request Forgery (SSRF) in the component TunnelServlet of agorum Software GmbH Agorum core open v11.9.2 & v11.10.1 allows attackers to forcefully initiate connections to arbitrary internal and external resources via a crafted request. This can lead to sensitive data exposure.	6.5	More Details
CVE-2025-7784	A flaw was found in the Keycloak identity and access management system when Fine-Grained Admin Permissions(FGAPv2) are enabled. An administrative user with the manage-users role can escalate their privileges to realm-admin due to improper privilege enforcement. This vulnerability allows unauthorized elevation of access rights, compromising the intended separation of administrative duties and posing a security risk to the realm.	6.5	More Details
CVE-2025-6717	The B1.lt plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 2.2.56 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2025-52168	Incorrect access control in the dynawebservice component of agorum Software GmbH Agorum core open v11.9.2 & v11.10.1 allows unauthenticated attackers to access arbitrary files on the system.	6.5	More Details
CVE-2025-46002	An issue in Filemanager v2.5.0 and below allows attackers to execute a directory traversal via sending a crafted HTTP request to the filemanager.php endpoint.	6.5	More Details
CVE-2025-50586	StudentManage v1.0 was discovered to contain Cross-Site Request Forgery (CSRF).	6.5	More Details
CVE-2025-54077	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in versions prior to 3.4.6 in the `personalizacao.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the `err` parameter. Version 3.4.6 fixes the issue.	6.5	More Details
CVE-2025-45157	Insecure permissions in Splashin iOS v2.0 allow unauthorized attackers to access location data for specific users.	6.5	More Details
CVE-2025-46000	An arbitrary file upload vulnerability in the component /rsc/filemanager.rsc.class.php of Filemanager commit c75b914 v.2.5.0 allows attackers to execute arbitrary code via uploading a crafted SVG file.	6.5	More Details
CVE-2025-52162	agorum Software GmbH Agorum core open v11.9.2 & v11.10.1 was discovered to contain an XML External Entity (XXE) via the RSSReader endpoint. This vulnerability allows attackers to access sensitive data via providing a crafted XML input.	6.5	More Details
CVE-2025-54076	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A Reflected Cross-Site Scripting (XSS) vulnerability was identified in versions prior to 3.4.6 in the `pre_cadastro_atendido.php` endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts in the `msg_e` parameter. Version 3.4.6	6.5	More Details

	fixes the issue.		
CVE-2025-47995	Weak authentication in Azure Machine Learning allows an authorized attacker to elevate privileges over a network.	6.5	More Details
CVE-2025-5753	The Valuation Calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘link’ parameter in all versions up to, and including, 1.3.2 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-2025-7655	The Live Stream Badger plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'livestream' shortcode in all versions up to, and including, 1.4.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-7658	The Temporarily Hidden Content plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'temphc-start' shortcode in all versions up to, and including, 1.0.6 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-2025-7661	The Partnerský systém Martinus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'martinus' shortcode in all versions up to, and including, 1.7.1 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-2025-27930	Zohocorp ManageEngine Applications Manager versions 176600 and prior are vulnerable to stored cross-site scripting in the File/Directory monitor.	6.4	More Details
CVE-2025-7644	The Pixel Gallery Addons for Elementor – Easy Grid, Creative Gallery, Drag and Drop Grid, Custom Grid Layout, Portfolio Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via URLs in all widgets in all versions up to, and including, 1.6.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-7495	The WP-Members Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpmem_login_link' shortcode in all versions up to, and including, 3.5.4.1 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-2025-6831	The User Registration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's urcr_restrict shortcode in all versions up to, and including, 4.2.4 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-2025-7648	The Ruven Themes: Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ruven_button' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-5240	The CRM and Lead Management by vcita plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘type’ parameter in all versions up to, and including, 2.7.5 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-2025-5800	The Testimonial Post type plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘auto_play’ parameter in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-4685	The Gutentor – Gutenberg Blocks – Page Builder for Gutenberg Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the HTML data attributes of multiple widgets, in all versions up to, and including, 3.4.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-7660	The Map My Locations plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'map_my_locations' shortcode in all versions up to, and including, 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-2025-5752	The Vertical scroll image slideshow gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘width’ parameter in all versions up to, and including, 11.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-8015	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an uploaded image's 'Title' and 'Slide link' fields in all versions up to, and including, 7.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-5754	The Useful Tab Block – Responsive & AMP-Compatible plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘className’ parameter in all versions up to, and including, 1.3.2 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-2025-5767	The Crowdfunding for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘width’ parameter in all versions up to, and including, 3.1.14 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-7653	The EPay.bg Payments plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'epay' shortcode in all versions up to, and including, 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-2025-6261	The Fleetwire Fleet Management plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's fleetwire_list shortcode in all versions up to, and including, 1.0.19 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-2025-7354	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes in all versions up to, and including, 7.4.2 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-	The ThemeREX Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.35.1.1 due to insufficient input sanitization and output escaping. The plugin’s SVG rendering routine calls the trx_addons_get_svg_from_file() function on an unvalidated 'svg' parameter supplied via the shortcode or Elementor widget settings, then outputs it via the trx_addons_show_layout()	6.4	More Details

6997	function. Because there is no check on the URL’s origin, scheme, or the SVG content itself, authenticated attackers, with Contributor-level access and above, can supply a remote SVG and inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.		
CVE-2025-7787	A vulnerability, which was classified as critical, was found in Xuxueli xxl-job up to 3.1.1. Affected is the function httpJobHandler of the file src\main\java\com\xxl\job\executor\service\jobhandler\SampleXxlJob.java. The manipulation leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-8018	A vulnerability was found in code-projects Food Ordering Review System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /user/reservation_page.php. The manipulation of the argument reg_Id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	6.3	More Details
CVE-2025-7927	A vulnerability has been found in PHPGurukul Online Banquet Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/view-user-queries.php. The manipulation of the argument viewid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-36117	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 does not disallow the session id after use which could allow an authenticated user to impersonate another user on the system.	6.3	More Details
CVE-2025-46119	An issue was discovered in CommScope Ruckus Unleashed prior to 200.15.6.212.27 and 200.18.7.1.323, and in Ruckus ZoneDirector prior to 10.5.1.0.282, where an authenticated request to the management endpoint `/admin/_cmdstat.jsp` discloses the administrator password in a trivially reversible obfuscated form. The same obfuscation method persists in configuration prior to 200.18.7.1.302, allowing anyone who obtains the system configuration to recover the plaintext credentials.	6.3	More Details
CVE-2025-36116	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 GUI is affected by cross-site WebSocket hijacking vulnerability. By sending a specially crafted request, an unauthenticated malicious actor could exploit this vulnerability to sniff an existing WebSocket connection to then remotely perform operations that the user is not allowed to perform.	6.3	More Details
CVE-2025-7873	A vulnerability was found in Metasoft 美特软件 MetaCRM up to 6.4.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file mcc_login.jsp. The manipulation of the argument workerid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-7798	A vulnerability classified as critical has been found in Beijing Shenzhou Shihan Technology Multimedia Integrated Business Display System up to 8.2. This affects an unknown part of the file /admin/system/structure/getdirectorydata/web/baseinfo/companyManage. The manipulation of the argument Struccture_ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7788	A vulnerability has been found in Xuxueli xxl-job up to 3.1.1 and classified as critical. Affected by this vulnerability is the function commandJobHandler of the file src\main\java\com\xxl\job\executor\service\jobhandler\SampleXxlJob.java. The manipulation leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7864	A vulnerability was found in thinkgem JeeSite up to 5.12.0. It has been classified as critical. This affects the function Upload of the file src/main/java/com/jeesite/modules/file/web/FileUploadController.java. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 3585737d21fe490ff6948d913fcbd8d99c41fc08. It is recommended to apply a patch to fix this issue.	6.3	More Details
CVE-2025-	A bug in Apache HTTP Server 2.4.64 results in all "RewriteCond expr ..." tests evaluating as "true". Users are recommended to upgrade to version 2.4.65, which fixes the issue.	6.3	More Details

54090			
CVE-2025-7754	A vulnerability was found in code-projects Patient Record Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /xray_form.php. The manipulation of the argument itr_no leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7935	A vulnerability, which was classified as critical, was found in fuyang_lipengjun platform up to ca9aceff6902feb7b0b6bf510842aea88430796a. Affected is the function SysLogController of the file platform-admin/src/main/java/com/platform/controller/SysLogController.java. The manipulation of the argument key leads to sql injection. It is possible to launch 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.	6.3	More Details
CVE-2025-7936	A vulnerability has been found in fuyang_lipengjun platform up to ca9aceff6902feb7b0b6bf510842aea88430796a and classified as critical. Affected by this vulnerability is the function queryPage of the file com/platform/controller/ScheduleJobLogController.java. The manipulation of the argument beanName/methodName leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may 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.	6.3	More Details
CVE-2025-7876	A vulnerability classified as critical was found in Metasoft 美特软件 MetaCRM up to 6.4.2. This vulnerability affects the function AnalyzeParam of the file download.jsp. The manipulation of the argument p leads to deserialization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-7877	A vulnerability, which was classified as critical, has been found in Metasoft 美特软件 MetaCRM up to 6.4.2. This issue affects some unknown processing of the file sendfile.jsp. The manipulation of the argument File leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-7878	A vulnerability, which was classified as critical, was found in Metasoft 美特软件 MetaCRM up to 6.4.2. Affected is an unknown function of the file /common/jsp/upload2.jsp. The manipulation of the argument File leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-7879	A vulnerability has been found in Metasoft 美特软件 MetaCRM up to 6.4.2 and classified as critical. Affected by this vulnerability is an unknown functionality of the file mobileupload.jsp. The manipulation of the argument File leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-7880	A vulnerability was found in Metasoft 美特软件 MetaCRM up to 6.4.2 and classified as critical. Affected by this issue is some unknown functionality of the file /business/common/sms/sendsms.jsp. The manipulation of the argument File leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-7836	A vulnerability has been found in D-Link DIR-816L up to 2.06B01 and classified as critical. Affected by this vulnerability is the function lxmldbc_system of the file /htdocs/cgibin of the component Environment Variable Handler. The manipulation leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2025-7934	A vulnerability, which was classified as critical, has been found in fuyang_lipengjun platform up to ca9aceff6902feb7b0b6bf510842aea88430796a. This issue affects the function queryPage of the file platform-schedule/src/main/java/com/platform/controller/ScheduleJobController.java. The manipulation of the argument beanName leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product does not	6.3	More Details

	use versioning. This is why information about affected and unaffected releases are unavailable.		
CVE-2025-7939	A vulnerability was found in jerryshensjf JPACookieShop 蛋糕商城JPA版 1.0. It has been classified as critical. Affected is the function addGoods of the file GoodsController.java. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely.	6.3	More Details
CVE-2025-7888	A vulnerability was found in TDuckCloud tduck-platform 5.1 and classified as critical. This issue affects the function UserFormDataMapper of the file src/main/java/com/tduck/cloud/form/mapper/UserFormDataMapper.java. The manipulation of the argument formKey leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-7932	A vulnerability classified as critical has been found in D-Link DIR-817L up to 1.04B01. This affects the function lxmldbc_system of the file ssdpcgi. The manipulation leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7894	A vulnerability, which was classified as critical, has been found in Onyx up to 0.29.1. This issue affects the function generate_simple_sql of the file backend/onyx/agents/agent_search/kb_search/nodes/a3_generate_simple_sql.py of the component Chat Interface. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2025-7906	A vulnerability was found in yangzongzhuan RuoYi up to 4.8.1 and classified as critical. This issue affects the function uploadFile of the file ruoyi-admin/src/main/java/com/ruoyi/web/controller/common/CommonController.java. The manipulation of the argument File leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7895	A vulnerability, which was classified as critical, was found in harry0703 MoneyPrinterTurbo up to 1.2.6. Affected is the function upload_bgm_file of the file app/controllers/v1/video.py of the component File Extension Handler. The manipulation of the argument File leads to unrestricted upload. It is possible to launch the attack remotely.	6.3	More Details
CVE-2025-7896	A vulnerability has been found in harry0703 MoneyPrinterTurbo up to 1.2.6 and classified as critical. Affected by this vulnerability is the function download_video/delete_video of the file app/controllers/v1/video.py. The manipulation leads to path traversal. The attack can be launched remotely.	6.3	More Details
CVE-2025-7759	A vulnerability, which was classified as critical, was found in thinkgem JeeSite up to 5.12.0. This affects an unknown part of the file modules/core/src/main/java/com/jeesite/common/ueditor/ActionEnter.java of the component UEditor Image Grabber. The manipulation of the argument Source leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 1c5e49b0818037452148e0f8ff69ed04cb8fefdc. It is recommended to apply a patch to fix this issue.	6.3	More Details
CVE-2025-7904	A vulnerability, which was classified as critical, was found in itsourcecode Insurance Management System 1.0. This affects an unknown part of the file /insertNominee.php. The manipulation of the argument nominee_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7952	A vulnerability classified as critical was found in TOTOLINK T6 4.1.5cu.748. This vulnerability affects the function ckeckKeepAlive of the file wireless.so of the component MQTT Packet Handler. The manipulation leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2025-7905	A vulnerability has been found in itsourcecode Insurance Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /insertPayment.php. The manipulation of the argument recipt_no leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-	An issue was discovered in Westermo WeOS 5 (5.24 through 5.24.4). A threat actor potentially		More

2025-54319	can gain unauthorized access to sensitive information via system logging information (syslog verbose logging that includes credentials).	6.3	Details
CVE-2025-7755	A vulnerability was found in code-projects Online Ordering System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/edit_product.php. The manipulation of the argument image leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-40682	IBM SmartCloud Analytics - Log Analysis 1.3.7.0, 1.3.7.1, 1.3.7.2, 1.3.8.0, 1.3.8.1, and 1.3.8.2 could allow a local user to cause a denial of service due to improper validation of specified type of input.	6.2	More Details
CVE-2025-7715	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Block Attributes allows Cross-Site Scripting (XSS).This issue affects Block Attributes: from 0.0.0 before 1.1.0, from 2.0.0 before 2.0.1.	6.1	More Details
CVE-2025-7392	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Cookies Addons allows Cross-Site Scripting (XSS).This issue affects Cookies Addons: from 1.0.0 before 1.2.4.	6.1	More Details
CVE-2025-6174	The Qwizcards | online quizzes and flashcards WordPress plugin through 3.9.4 does not sanitise and escape the "_stylesheet" parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin or any other user.	6.1	More Details
CVE-2024-55040	Cross Site Scripting vulnerability in Sensaphone WEB600 Monitoring System v.1.6.5.H and before allows a remote attacker to execute arbitrary code via a crafted GET requests to /@.xml, placing payloads in the g7200, g7300, g4601, and g1F02 parameters.	6.1	More Details
CVE-2025-51863	Self Cross Site Scripting (XSS) vulnerability in ChatGPT Unli (ChatGPTUnli.com) thru 2025-05-26 allows attackers to execute arbitrary code via a crafted SVG file to the chat interface.	6.1	More Details
CVE-2025-40598	A Reflected cross-site scripting (XSS) vulnerability exists in the SMA100 series web interface, allowing a remote unauthenticated attacker to potentially execute arbitrary JavaScript code.	6.1	More Details
CVE-2025-7716	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Real-time SEO for Drupal allows Cross-Site Scripting (XSS).This issue affects Real-time SEO for Drupal: from 2.0.0 before 2.2.0.	6.1	More Details
CVE-2025-51858	Self Cross-Site Scripting (XSS) vulnerability in ChatPlayground.ai through 2025-05-24, allows attackers to execute arbitrary code and gain sensitive information via a crafted SVG file contents sent through the chat component.	6.1	More Details
CVE-2025-51862	Insecure Direct Object Reference (IDOR) vulnerability in TelegAI (telegai.com) thru 2025-05-26 in its chat component. An attacker can exploit this IDOR to tamper other users' conversation. Additionally, malicious contents and XSS payloads can be injected, leading to phishing attack, user spoofing and account hijacking via XSS.	6.1	More Details
CVE-2025-7369	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 7.4.2. This is due to missing or incorrect nonce validation on the preview function. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link. In combination with CVE-2025-7354, it leads to Reflected Cross-Site Scripting.	6.1	More Details
CVE-2025-46383	CWE-79 Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')	6.1	More Details
CVE-2025-6054	The YANewsflash plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.3. This is due to missing or incorrect nonce validation on the 'yanewsflash/yanewsflash.php' page. 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-2025-51860	Stored Cross-Site Scripting (XSS) in TelegAI (telegai.com) 2025-05-26 in its chat component and character container component. An attacker can achieve arbitrary client-side script execution by crafting an AI Character with SVG XSS payloads in either description, greeting, example dialog, or system prompt(instructing the LLM to embed XSS payload in its chat response). When a user interacts with such a malicious AI Character or just browse its profile, the script executes in the user's browser. Successful exploitation can lead to the theft of sensitive information, such as session tokens, potentially resulting in account hijacking.	6.1	More Details
CVE-2025-7669	The Avishi WP PayPal Payment Button plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0. This is due to missing or incorrect nonce validation on the 'avishi-wp-paypal-payment-button/index.php' page. 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-2025-7685	The Like & Share My Site plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.2. This is due to missing or incorrect nonce validation on the 'lsms_admin' page. 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-2025-7687	The Latest Post Accordian Slider plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3. This is due to missing or incorrect nonce validation on the 'lpaccordian' page. 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-2025-47189	Netwrix Directory Manager (formerly Imanami GroupID) 11.0.0.0 before 11.1.25162.02 allows XSS for authentication error data of certain user flows, a different vulnerability than CVE-2025-54392.	6.1	More Details
CVE-2025-7920	WinMatrix3 Web package developed by Simopro Technology has a Reflected Cross-site Scripting vulnerability, allowing unauthenticated remote attackers to execute arbitrary JavaScript codes in user's browser through phishing attacks.	6.1	More Details
CVE-2025-4284	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Rolantis Information Technologies Agentis allows Reflected XSS, DOM-Based XSS.This issue affects Agentis: before 4.32.	6.1	More Details
CVE-2025-53941	Hollo is a federated single-user microblogging software designed to be federated through ActivityPub. Versions prior to 0.6.5 allow HTML form elements to be submitted, making the software vulnerable to HTML injection. Version 0.6.5 fixes the issue.	6.1	More Details
CVE-2025-6053	The Zuppler Online Ordering plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1.0. This is due to missing or incorrect nonce validation on the 'zuppler-online-ordering-options' page. 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-2025-51462	Stored Cross-site Scripting (XSS) vulnerability in api.apps.dialog_app.set_dialog in RAGFlow 0.17.2 allows remote attackers to execute arbitrary JavaScript via crafted input to the assistant greeting field, which is stored unsanitised and rendered using a markdown component with rehype-raw.	6.1	More Details
CVE-2025-36107	IBM Cognos Analytics Mobile (iOS) 1.1.0 through 1.1.22 could allow malicious actors to obtain sensitive information due to the cleartext transmission of data.	5.9	More Details
CVE-2024-53288	Improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in NTP Region functionality in Synology Router Manager (SRM) before 1.3.1-9346-11 allows remote authenticated users with administrator privileges to inject arbitrary web script or HTML via unspecified vectors.	5.9	More Details
CVE-2025-	IBM Cognos Analytics Mobile (iOS) 1.1.0 through 1.1.22 could be vulnerable to information exposure due to the use of unencrypted network traffic.	5.9	More Details

36062			
CVE-2025-7427	Uncontrolled Search Path Element in Arm Development Studio before 2025 may allow an attacker to perform a DLL hijacking attack. Successful exploitation could lead to local arbitrary code execution in the context of the user running Arm Development Studio.	5.9	More Details
CVE-2024-53287	Improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in VPN Setting functionality in Synology Router Manager (SRM) before 1.3.1-9346-11 allows remote authenticated users with administrator privileges to inject arbitrary web script or HTML via unspecified vectors.	5.9	More Details
CVE-2025-33020	IBM Engineering Systems Design Rhapsody 9.0.2, 10.0, and 10.0.1 transmits sensitive information without encryption that could allow an attacker to obtain highly sensitive information.	5.9	More Details
CVE-2024-13175	Authorization Bypass Through User-Controlled Key vulnerability in Vidco Software VOC TESTER allows Forceful Browsing.This issue affects VOC TESTER: before 12.41.0.	5.5	More Details
CVE-2024-41750	IBM SmartCloud Analytics - Log Analysis 1.3.7.0, 1.3.7.1, 1.3.7.2, 1.3.8.0, 1.3.8.1, and 1.3.8.2 could allow a local, authenticated attacker to bypass client-side enforcement of security to manipulate data.	5.5	More Details
CVE-2025-5818	The Featured Image Plus – Quick & Bulk Edit with Unsplash plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.6.4 via the fip_get_image_options() function. This makes it possible for authenticated attackers, with administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	5.5	More Details
CVE-2025-41458	Unencrypted storage in the database in Two App Studio Journey v5.5.9 for iOS allows local attackers to extract sensitive data via direct access to the app’s filesystem.	5.5	More Details
CVE-2025-42947	SAP FICA ODN framework allows a high privileged user to inject value inside the local variable which can then be executed by the application. An attacker could thereby control the behaviour of the application causing high impact on integrity, low impact on availability and no impact on confidentiality of the application.	5.5	More Details
CVE-2024-41751	IBM SmartCloud Analytics - Log Analysis 1.3.7.0, 1.3.7.1, 1.3.7.2, 1.3.8.0, 1.3.8.1, and 1.3.8.2 could allow a local, authenticated attacker to bypass client-side enforcement of security to manipulate data.	5.5	More Details
CVE-2025-33014	IBM Sterling B2B Integrator and IBM Sterling File Gateway 6.0.0.0 through 6.1.2.7 and 6.2.0.0 through 6.2.0.4 uses a web link with untrusted references to an external site. A remote attacker could exploit this vulnerability to expose sensitive information or perform unauthorized actions on the victims’ web browser.	5.4	More Details
CVE-2025-51479	Authorization bypass in update_user_group in onyx-dot-app Onyx Enterprise Edition 0.27.0 allows remote authenticated attackers to modify arbitrary user groups via crafted PATCH requests to the /api/manage/admin/user-group/id endpoint, bypassing intended curator-group assignment checks.	5.4	More Details
CVE-2025-51396	A stored cross-site scripting (XSS) vulnerability in Live Helper Chat v4.60 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Telegram Bot Username parameter.	5.4	More Details
CVE-2025-51397	A stored cross-site scripting (XSS) vulnerability in the Facebook Chat module of Live Helper Chat v4.60 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Surname parameter under the Recipient' Lists.	5.4	More Details
CVE-2025-51400	A stored cross-site scripting (XSS) vulnerability in the Personal Canned Messages of Live Helper Chat v4.60 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload.	5.4	More Details
CVE-2025-	A stored cross-site scripting (XSS) vulnerability in the Facebook registration page of Live Helper Chat v4.60 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted	5.4	More

51398	payload into the Name parameter.		Details
CVE-2024-40686	IBM SmartCloud Analytics - Log Analysis 1.3.7.0, 1.3.7.1, 1.3.7.2, 1.3.8.0, 1.3.8.1, and 1.3.8.2 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking.	5.4	More Details
CVE-2025-51401	A stored cross-site scripting (XSS) vulnerability in the chat transfer function of Live Helper Chat v4.60 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the operator name parameter.	5.4	More Details
CVE-2025-46102	Cross Site Scripting vulnerability in Beakon Software Beakon Learning Management System Sharable Content Object Reference Model (SCORM) version V.5.4.3 allows a remote attacker to obtain sensitive information via the URL parameter	5.4	More Details
CVE-2025-44109	A URL redirection in Pinokio v3.6.23 allows attackers to redirect victim users to attacker-controlled pages.	5.4	More Details
CVE-2025-46171	vBulletin 3.8.7 is vulnerable to a denial-of-service condition via the misc.php?do=buddylist endpoint. If an authenticated user has a sufficiently large buddy list, processing the list can consume excessive memory, exhausting system resources and crashing the forum.	5.4	More Details
CVE-2025-46732	OpenCTI is an open source platform for managing cyber threat intelligence knowledge and observables. Prior to version 6.6.6, an IDOR vulnerability in the GrapQL `NotificationLineNotificationMarkReadMutation` and `NotificationLineNotificationDeleteMutation` mutations of OpenCTI allows an authenticated user to change the read status of a notification or delete a notification of another user in case he has knowledge of the UUID of the notification. When changing the read status of a notification, the user also receives the content of the notification they changed the read status of. Authenticated Users in OpenCTI can read, modify and delete notification of other users if they know the UUID of the notification. Version 6.6.6 fixes the issue.	5.4	More Details
CVE-2025-50477	A URL redirection in lbry-desktop v0.53.9 allows attackers to redirect victim users to attacker-controlled pages.	5.4	More Details
CVE-2025-7947	A vulnerability classified as critical has been found in jshERP up to 3.5. Affected is an unknown function of the file /user/delete of the component Account Handler. The manipulation of the argument ID leads to improper authorization. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	5.4	More Details
CVE-2025-7889	A vulnerability was found in CallApp Caller ID App up to 2.0.4 on Android. It has been classified as problematic. Affected is an unknown function of the file AndroidManifest.xml of the component caller.id.phone.number.block. The manipulation leads to improper export of android application components. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-7940	A vulnerability was found in Genshin Albedo Cat House App 1.0.2 on Android. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file AndroidManifest.xml of the component com.house.auscat. The manipulation leads to improper export of android application components. 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-2025-4302	The Stop User Enumeration WordPress plugin before version 1.7.3 blocks REST API /wp-json/wp/v2/users/ requests for non-authorized users. However, this can be bypassed by URL-encoding the API path.	5.3	More Details
CVE-2025-7874	A vulnerability was found in Metasoft 美特软件 MetaCRM up to 6.4.2. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /env.jsp. The manipulation leads to information disclosure. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-			

2025-45156	Splashin iOS v2.0 fails to enforce server-side interval restrictions for location updates for free-tier users.	5.3	More Details
CVE-2025-7890	A vulnerability was found in Dunamu StockPlus App up to 7.62.10 on Android. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file AndroidManifest.xml of the component com.dunamu.stockplus. The manipulation leads to improper export of android application components. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-7891	A vulnerability was found in InstantBits Web Video Cast App up to 5.12.4 on Android. It has been rated as problematic. Affected by this issue is some unknown functionality of the file AndroidManifest.xml of the component com.instantbits.cast.webvideo. The manipulation leads to improper export of android application components. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-7892	A vulnerability classified as problematic has been found in IDnow App up to 9.6.0 on Android. This affects an unknown part of the file AndroidManifest.xml of the component de.idnow. The manipulation leads to improper export of android application components. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-5811	The Listly: Listicles For WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the Init() function in all versions up to, and including, 2.7. This makes it possible for unauthenticated attackers to delete arbitrary transient values on the WordPress site.	5.3	More Details
CVE-2025-7893	A vulnerability classified as problematic was found in Foresight News App up to 2.6.4 on Android. This vulnerability affects unknown code of the file AndroidManifest.xml of the component pro.foresightnews.appa. The manipulation leads to improper export of android application components. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2025-46382	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	5.3	More Details
CVE-2025-7797	A vulnerability was found in GPAC up to 2.4. It has been rated as problematic. Affected by this issue is the function gf_dash_download_init_segment of the file src/media_tools/dash_client.c. The manipulation of the argument base_init_url leads to null pointer dereference. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The patch is identified as 153ea314b6b053db17164f8bc3c7e1e460938eaa. It is recommended to apply a patch to fix this issue.	5.3	More Details
CVE-2025-6721	The Vchasno Kasa plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the mrkv_vchasno_kasa_wc_do_metabox_action() function in all versions up to, and including, 1.0.3. This makes it possible for unauthenticated attackers to generate invoices for arbitrary orders.	5.3	More Details
CVE-2025-6720	The Vchasno Kasa plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the clear_all_log() function in all versions up to, and including, 1.0.3. This makes it possible for unauthenticated attackers to clear log files.	5.3	More Details
CVE-2025-6215	The Omnishop plugin for WordPress is vulnerable to Unauthenticated Registration Bypass in all versions up to, and including, 1.0.9. Its /users/register endpoint is exposed to the public (permission_callback always returns true) and invokes wp_create_user() unconditionally, ignoring the site's users_can_register option and any nonce or CAPTCHA checks. This makes it possible for unauthenticated attackers to create arbitrary user accounts (customer) on sites where registrations should be closed.	5.3	More Details
CVE-2025-6230	A SQL injection vulnerability was reported in Lenovo Vantage that could allow a local attacker to modify the local SQLite database and execute code with elevated permissions.	5.3	More Details

CVE-2025-6082	The Birth Chart Compatibility plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 2.0. This is due to insufficient protection against directly accessing the plugin's index.php file, which causes an error exposing the full path. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2025-41679	An unauthenticated remote attacker could exploit a buffer overflow vulnerability in the device causing a denial of service that affects only the network initializing wizard (Conftool) service.	5.3	More Details
CVE-2025-54121	Starlette is a lightweight ASGI (Asynchronous Server Gateway Interface) framework/toolkit, designed for building async web services in Python. In versions 0.47.1 and below, when parsing a multi-part form with large files (greater than the default max spool size) starlette will block the main thread to roll the file over to disk. This blocks the event thread which means the application can't accept new connections. The UploadFile code has a minor bug where instead of just checking for self._in_memory, the logic should also check if the additional bytes will cause a rollover. The vulnerability is fixed in version 0.47.2.	5.3	More Details
CVE-2025-36057	IBM Cognos Analytics Mobile (iOS) 1.1.0 through 1.1.22 is vulnerable to authentication bypass by using the Local Authentication Framework library which is not needed as biometric authentication is not used in the application.	5.2	More Details
CVE-2025-52372	An issue in hMailServer v.5.8.6 allows a local attacker to obtain sensitive information via the hmailserver/installation/hMailServerInnoExtension.iss and hMailServer.ini components.	5.1	More Details
CVE-2025-51475	Arbitrary File Overwrite (AFO) in superagi.controllers.resources.upload in TransformerOptimus SuperAGI 0.0.14 allows remote attackers to overwrite arbitrary files via unsanitised filenames submitted to the file upload endpoint, due to improper handling of directory traversal in os.path.join() and lack of path validation in get_root_input_dir().	5.0	More Details
CVE-2025-46686	Redis through 7.4.3 allows memory consumption via a multi-bulk command composed of many bulks, sent by an authenticated user. This occurs because the server allocates memory for the command arguments of every bulk, even when the command is skipped because of insufficient permissions.	4.9	More Details
CVE-2025-46267	Hidden functionality issue exists in WRC-BE36QS-B and WRC-W701-B. If exploited, the product's hidden debug function may be enabled by a remote attacker who can log in to WebGUI.	4.9	More Details
CVE-2025-54316	An issue was discovered in Logpoint before 7.6.0. When creating reports, attackers can create custom Jinja templates that chained built-in filter functions to generate XSS payloads. These payloads can be rendered by the Logpoint Report Template engine, making it vulnerable to cross-site scripting (XSS) attacks.	4.9	More Details
CVE-2025-41677	A high privileged remote attacker can exhaust critical system resources by sending specifically crafted POST requests to the send-mail action in fast succession.	4.9	More Details
CVE-2025-7638	The Forminator Forms – Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to time-based SQL Injection via the `order_by` parameter in all versions up to, and including, 1.45.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with 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-2025-41676	A high privileged remote attacker can exhaust critical system resources by sending specifically crafted POST requests to the send-sms action in fast succession.	4.9	More Details
CVE-2025-41681	A high privileged remote attacker can gain persistent XSS via POST requests due to improper neutralization of special elements used to create dynamic content.	4.8	More Details
CVE-	A cross-site scripting (XSS) vulnerability in the component /blog/blogpost/add of Mezzanine CMS		

2025-50481	v6.1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into a blog post.	4.8	More Details
CVE-2025-4294	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in HotelRunner B2B allows Cross-Site Scripting (XSS).This issue affects B2B: before 04.06.2025.	4.8	More Details
CVE-2025-50584	StudentManage v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the Add A New Teacher module.	4.8	More Details
CVE-2025-50581	MRCMS v3.1.2 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /admin/group/save.do.	4.8	More Details
CVE-2025-50582	StudentManage v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the Add A New Course module.	4.8	More Details
CVE-2025-50583	StudentManage v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the Add A New Student module.	4.8	More Details
CVE-2025-4296	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in HotelRunner B2B allows Forceful Browsing.This issue affects B2B: before 04.06.2025.	4.7	More Details
CVE-2025-23269	NVIDIA Jetson Linux contains a vulnerability in the kernel where an attacker may cause an exposure of sensitive information due to a shared microarchitectural predictor state that influences transient execution. A successful exploit of this vulnerability may lead to information disclosure.	4.7	More Details
CVE-2025-54066	DiracX-Web is a web application that provides an interface to interact with the DiracX services. Prior to version 0.1.0-a8, an attacker can forge a request that they can pass to redirect an authenticated user to another arbitrary website. In the login page, DiracX-Web has a `redirect` field which is the location where the server will redirect the user. This URI is not verified, and can be an arbitrary URI. Paired with a parameter pollution, an attacker can hide their malicious URI. This could be used for phishing, and extract new data (such as redirecting to a new "log in" page, and asking another time credentials). Version 0.1.0-a8 fixes this vulnerability.	4.7	More Details
CVE-2025-7898	A vulnerability was found in Codecanyon iDentSoft 2.0. It has been classified as critical. This affects an unknown part of the file /clinica/profile/updateSetting of the component Account Setting Page. The manipulation of the argument photo leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2025-4295	Improper Validation of Certificate with Host Mismatch vulnerability in HotelRunner B2B allows HTTP Response Splitting.This issue affects B2B: before 04.06.2025.	4.6	More Details
CVE-2025-53927	MaxKB is an open-source AI assistant for enterprise. Prior to version 2.0.0, the sandbox design rules can be bypassed because MaxKB only restricts the execution permissions of files in a specific directory. Therefore, an attacker can use the `shutil.copy2` method in Python to copy the command they want to execute to the executable directory. This bypasses directory restrictions and reverse shell. Version 2.0.0 fixes the issue.	4.6	More Details
CVE-2025-53928	MaxKB is an open-source AI assistant for enterprise. Prior to versions 1.10.9-lts and 2.0.0, a Remote Command Execution vulnerability exists in the MCP call. Versions 1.10.9-lts and 2.0.0 fix the issue.	4.6	More Details
CVE-2025-52374	Use of hardcoded cryptographic key in Encryption.cs in hMailServer 5.8.6 and 5.6.9-beta allows attacker to decrypt passwords to other servers from hMailAdmin.exe.config file to access other hMailServer admin consoles with configured connections.	4.6	More Details
CVE-	Use of hardcoded cryptographic key in BlowFish.cpp in hMailServer 5.8.6 and 5.6.9-beta allows		More

2025-52373	attacker to decrypt passwords used in database connections from hMailServer.ini config file.	4.6	Details
CVE-2024-38335	IBM Security QRadar Network Threat Analytics 1.0.0 through 1.3.1 could allow a privileged user to cause a denial of service due to improper allocation of resources.	4.5	More Details
CVE-2025-30477	Dell PowerScale OneFS, versions prior to 9.11.0.0, contains a use of a broken or risky cryptographic algorithm vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	4.4	More Details
CVE-2025-7431	The Knowledge Base plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin slug setting in all versions up to, and including, 2.3.1 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.	4.4	More Details
CVE-2025-6719	The Terms descriptions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.4.8 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-2025-7486	The Ebook Store plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Order Details in all versions up to, and including, 5.8012 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.	4.4	More Details
CVE-2025-54059	melange allows users to build apk packages using declarative pipelines. Starting in version 0.23.0 and prior to version 0.29.5, SBOM files generated by melange in apks had file system permissions mode 666. This potentially allows an unprivileged user to tamper with apk SBOMs on a running image, potentially confusing security scanners. An attacker could also perform a DoS under special circumstances. Version 0.29.5 fixes the issue.	4.4	More Details
CVE-2025-2301	Authorization Bypass Through User-Controlled Key vulnerability in Akbim Software Online Exam Registration allows Exploitation of Trusted Identifiers.This issue affects Online Exam Registration: before 14.03.2025.	4.4	More Details
CVE-2025-7903	A vulnerability classified as problematic was found in yangzongzhuan RuoYi up to 4.8.1. Affected by this vulnerability is an unknown functionality of the component Image Source Handler. The manipulation leads to improper restriction of rendered ui layers. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-7943	A vulnerability was found in PHPGurukul Taxi Stand Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/search-autoortaxi.php. The manipulation of the argument searchdata leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-7887	A vulnerability has been found in Zavy86 WikiDocs up to 1.0.78 and classified as problematic. This vulnerability affects unknown code of the file template.inc.php. The manipulation of the argument path leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-7944	A vulnerability was found in PHPGurukul Taxi Stand Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /search.php. The manipulation of the argument searchdata leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-	A vulnerability, which was classified as problematic, has been found in Huashengdun WebSSH up to 1.6.2. Affected by this issue is some unknown functionality of the component Login Page. The manipulation of the argument hostname/port leads to cross site scripting. The attack may	4.3	More

7885	be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		Details
CVE-2025-54139	HAX CMS allows users to manage their microsite universe with a NodeJS or PHP backend. In haxcms-nodejs versions 11.0.12 and below and in haxcms-php versions 11.0.7 and below, all pages within the HAX CMS application do not contain headers to prevent other websites from loading the site within an iframe. This applies to both the CMS and generated sites. An unauthenticated attacker can load the standalone login page or other sensitive functionality within an iframe, performing a UI redressing attack (clickjacking). This can be used to perform social engineering attacks to attempt to coerce users into performing unintended actions within the HAX CMS application. This is fixed in haxcms-nodejs version 11.0.13 and haxcms-php 11.0.8.	4.3	More Details
CVE-2025-54129	HAXiam is a packaging wrapper for HAXcms which allows anyone to spawn their own microsite management platform. In versions 11.0.4 and below, the application returns a 200 response when requesting the data of a valid user and a 404 response when requesting the data of an invalid user. This can be used to infer the existence of valid user accounts. An authenticated attacker can use automated tooling to brute force potential usernames and use the application's response to identify valid accounts. This can be used in conjunction with other vulnerabilities, such as the lack of authorization checks, to enumerate and deface another user's sites. This is fixed in version 11.0.5.	4.3	More Details
CVE-2025-3415	Grafana is an open-source platform for monitoring and observability. The Grafana Alerting DingDing integration was not properly protected and could be exposed to users with Viewer permission. Fixed in versions 10.4.19+security-01, 11.2.10+security-01, 11.3.7+security-01, 11.4.5+security-01, 11.5.5+security-01, 11.6.2+security-01 and 12.0.1+security-01	4.3	More Details
CVE-2025-7901	A vulnerability was found in yangzongzhuan RuoYi up to 4.8.1. It has been rated as problematic. This issue affects some unknown processing of the file /swagger-ui/index.html of the component Swagger UI. The manipulation of the argument configUrl leads to cross site scripting. The attack may be initiated remotely.	4.3	More Details
CVE-2025-7946	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /search-visitor.php of the component HTTP POST Request Handler. The manipulation of the argument searchdata leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-7834	A vulnerability, which was classified as problematic, was found in PHPGurukul Complaint Management System 2.0. Affected is an unknown function. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-7948	A vulnerability classified as problematic was found in jshERP up to 3.5. Affected by this vulnerability is an unknown functionality of the file /jshERP-boot/user/updatePwd. The manipulation leads to weak password recovery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-6781	The Copymatic – AI Content Writer & Generator plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1. This is due to missing or incorrect nonce validation on the 'copymatic-menu' page. This makes it possible for unauthenticated attackers to update the copymatic_apikey option 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-2025-7907	A vulnerability was found in yangzongzhuan RuoYi up to 4.8.1. It has been classified as problematic. Affected is an unknown function of the file ruoyi-admin/src/main/resources/application-druid.yml of the component Druid. The manipulation leads to use of default credentials. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-7925	A vulnerability, which was classified as problematic, has been found in PHPGurukul Online Banquet Booking System 1.0. Affected by this issue is some unknown functionality of the file /admin/login.php. The manipulation of the argument user_login/userpassword leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details

CVE-2025-5816	The Plugin Pengiriman WooCommerce Kurir Reguler, Instan, Kargo – Biteship plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.2.0 via the get_order_detail() due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view other user's orders.	4.3	More Details
CVE-2025-7763	A vulnerability, which was classified as problematic, was found in thinkgem JeeSite up to 5.12.0. Affected is the function select of the file src/main/java/com/jeesite/modules/cms/web/SiteController.java of the component Site Controller. The manipulation of the argument redirect leads to open redirect. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The patch is identified as 3d06b8d009d0267f0255acc87ea19d29d07cedc3. It is recommended to apply a patch to fix this issue.	4.3	More Details
CVE-2025-6726	The Block Editor Gallery Slider plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the classic_gallery_slider_options() function in all versions up to, and including, 1.1.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update limited post meta for arbitrary posts.	4.3	More Details
CVE-2025-7756	A vulnerability classified as problematic has been found in code-projects E-Commerce Site 1.0. Affected is an unknown function. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2024-32124	An improper access control vulnerability [CWE-284] in FortiIsolator version 2.4.4, version 2.4.3, 2.3 all versions logging component may allow a remote authenticated read-only attacker to alter logs via a crafted HTTP request.	4.3	More Details
CVE-2025-7785	A vulnerability classified as problematic was found in thinkgem JeeSite up to 5.12.0. This vulnerability affects the function sso of the file src/main/java/com/jeesite/modules/sys/web/SsoController.java. The manipulation of the argument redirect leads to open redirect. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The patch is identified as 3d06b8d009d0267f0255acc87ea19d29d07cedc3. It is recommended to apply a patch to fix this issue.	4.3	More Details
CVE-2025-43976	The com.enflick.android.tn2ndLine application through 24.17.1.0 for Android enables any installed application (with no permissions) to place phone calls without user interaction by sending a crafted intent via the com.enflick.android.TextNow.activities.DialerActivity component.	4.3	More Details
CVE-2025-43977	The com.skt.prod.dialer application through 12.5.0 for Android enables any installed application (with no permissions) to place phone calls without user interaction by sending a crafted intent via the com.skt.prod.dialer.activities.outgoingcall.OutgoingCallInternalBroadcaster component.	4.3	More Details
CVE-2025-7938	A vulnerability was found in jerryshensjf JPACookieShop 蛋糕商城JPA版 1.0 and classified as critical. This issue affects the function updateGoods of the file GoodsController.java. The manipulation leads to authorization bypass. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2025-6197	An open redirect vulnerability has been identified in Grafana OSS organization switching functionality. Prerequisites for exploitation: - Multiple organizations must exist in the Grafana instance - Victim must be on a different organization than the one specified in the URL	4.2	More Details
CVE-2025-36603	Dell AppSync, version(s) 4.6.0.0, contains an Improper Restriction of XML External Entity Reference vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure and Information tampering.	4.2	More Details
CVE-2025-32019	Harbor is an open source trusted cloud native registry project that stores, signs, and scans content. Versions 2.11.2 and below, as well as versions 2.12.0-rc1 and 2.13.0-rc1, contain a vulnerability where the markdown field in the info tab page can be exploited to inject XSS code. This is fixed in versions 2.11.3 and 2.12.3.	4.1	More Details
CVE-2025-	In Mbed TLS 3.6.1 through 3.6.3 before 3.6.4, a timing discrepancy in block cipher padding removal allows an attacker to recover the plaintext when PKCS#7 padding mode is used.	4.0	More Details

49087			
CVE-2025-54310	qBittorrent before 5.1.2 does not prevent access to a local file that is referenced in a link URL. This affects rsswidget.cpp and searchjobwidget.cpp.	4.0	More Details
CVE-2025-48965	Mbed TLS before 3.6.4 has a NULL pointer dereference because mbedtls_asn1_store_named_data can trigger conflicting data with val.p of NULL but val.len greater than zero.	4.0	More Details
CVE-2025-52924	In One Identity OneLogin before 2025.2.0, the SQL connection "application name" is set based on the value of an untrusted X-RequestId HTTP request header.	4.0	More Details
CVE-2025-44657	In Linksys EA6350 V2.1.2, the chroot_local_user option is enabled in the dynamically generated vsftpd configuration file. This could lead to unauthorized access to system files, privilege escalation, or use of the compromised server as a pivot point for internal network attacks.	3.9	More Details
CVE-2025-54352	WordPress 3.5 through 6.8.2 allows remote attackers to guess titles of private and draft posts via pingback.ping XML-RPC requests. NOTE: the Supplier is not changing this behavior.	3.7	More Details
CVE-2025-7789	A vulnerability was found in Xuxueli xxl-job up to 3.1.1 and classified as problematic. Affected by this issue is the function makeToken of the file src/main/java/com/xxl/job/admin/controller/IndexController.java of the component Token Generation. The manipulation leads to password hash with insufficient computational effort. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used.	3.7	More Details
CVE-2025-4878	A vulnerability was found in libssh, where an uninitialized variable exists under certain conditions in the privatekey_from_file() function. This flaw can be triggered if the file specified by the filename doesn't exist and may lead to possible signing failures or heap corruption.	3.6	More Details
CVE-2025-7949	A vulnerability was found in Sanluan PublicCMS up to 5.202506.a. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file publiccms-parent/publiccms/src/main/resources/templates/admin/cmsDiy/preview.html. The manipulation of the argument url leads to open redirect. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The patch is named c1e79f124e3f4c458315d908ed7dee06f9f12a76/f1af17af004ca9345c6fe4d5936d87d008d26e75. It is recommended to apply a patch to fix this issue.	3.5	More Details
CVE-2025-7942	A vulnerability has been found in PHPGurukul Taxi Stand Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/admin-profile.php. The manipulation of the argument adminname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7941	A vulnerability, which was classified as problematic, was found in PHPGurukul Time Table Generator System 1.0. Affected is an unknown function of the file /admin/profile.php. The manipulation of the argument adminname leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7953	A vulnerability, which was classified as problematic, has been found in Sanluan PublicCMS up to 5.202506.a. This issue affects some unknown processing of the file publiccms-parent/publiccms/src/main/webapp/resource/plugins/pdfjs/viewer.html. The manipulation of the argument File leads to open redirect. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The patch is named f1af17af004ca9345c6fe4d5936d87d008d26e75. It is recommended to apply a patch to fix this issue.	3.5	More Details
CVE-2025-7951	A vulnerability classified as problematic has been found in code-projects Public Chat Room 1.0. This affects an unknown part of the file /send_message.php. The manipulation of the argument chat_msg/your_name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
	A vulnerability classified as problematic has been found in Scada-LTS up to 2.7.8.1. Affected is		

CVE-2025-7728	an unknown function of the file users.shtm. The manipulation of the argument Username leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this issue and confirmed that it will be fixed in the upcoming release 2.8.0.	3.5	More Details
CVE-2025-7729	A vulnerability classified as problematic was found in Scada-LTS up to 2.7.8.1. Affected by this vulnerability is an unknown functionality of the file usersProfiles.shtm. The manipulation of the argument Username leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this issue and confirmed that it will be fixed in the upcoming release 2.8.0.	3.5	More Details
CVE-2025-7802	A vulnerability was found in PHPGurukul Complaint Management System 2.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/complaint-search.php. The manipulation of the argument Search leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7748	A vulnerability classified as problematic was found in ZCMS 3.6.0. This vulnerability affects unknown code of the component Create Article Page. The manipulation of the argument Title leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7866	A vulnerability was found in Portabilis i-Educar 2.9.0. It has been rated as problematic. This issue affects some unknown processing of the file /intranet/educar_deficiencia_lst.php of the component Disabilities Module. The manipulation of the argument Deficiência ou Transtorno leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-7865	A vulnerability was found in thinkgem JeeSite up to 5.12.0. It has been declared as problematic. This vulnerability affects the function xssFilter of the file src/main/java/com/jeesite/common/codec/EncodeUtils.java of the component XSS Filter. The manipulation of the argument text leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The patch is identified as 3585737d21fe490ff6948d913fcbd8d99c41fc08. It is recommended to apply a patch to fix this issue.	3.5	More Details
CVE-2025-7863	A vulnerability was found in thinkgem JeeSite up to 5.12.0 and classified as problematic. Affected by this issue is the function redirectUrl of the file src/main/java/com/jeesite/common/web/http/ServletUtils.java. The manipulation of the argument url leads to open redirect. The attack may be launched remotely. The name of the patch is 3d06b8d009d0267f0255acc87ea19d29d07cedc3. It is recommended to apply a patch to fix this issue.	3.5	More Details
CVE-2024-42209	HCL Connections is vulnerable to an information disclosure vulnerability that could allow a user to obtain sensitive information they are not entitled to, which is caused by improper handling of request data.	3.5	More Details
CVE-2025-2818	A vulnerability was reported in version 1.0 of the Bluetooth Transmission Alliance protocol adopted by Motorola Smart Connect Android Application that could allow a nearby attacker within the Bluetooth interaction range to intercept files when transferred to a device not paired in Smart Connect.	3.5	More Details
CVE-2025-7858	A vulnerability classified as problematic has been found in PHPGurukul Apartment Visitors Management System 1.0. This affects an unknown part of the file /admin-profile.php of the component HTTP POST Request Handler. The manipulation of the argument adminname leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7857	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file bwdates-passreports-details.php of the component HTTP POST Request Handler. The manipulation of the argument visname leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
	A vulnerability was found in Campcodes Online Movie Theater Seat Reservation System 1.0. It		

CVE-2025-7840	has been classified as problematic. This affects an unknown part of the file /index.php?page=reserve of the component Reserve Your Seat Page. The manipulation of the argument Firstname/Lastname leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7868	A vulnerability classified as problematic was found in Portabilis i-Educar 2.9.0. Affected by this vulnerability is an unknown functionality of the file /intranet/educar_calendario_dia_motivo_cad.php of the component Calendar Module. The manipulation of the argument Motivo leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-7767	A vulnerability, which was classified as problematic, has been found in PHPGurukul Art Gallery Management System 1.1. Affected by this issue is some unknown functionality of the file /admin/edit-art-medium-detail.php. The manipulation of the argument artmed leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7818	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /category.php of the component HTTP POST Request Handler. The manipulation of the argument categoryname leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7817	A vulnerability has been found in PHPGurukul Apartment Visitors Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /bwdates-reports.php of the component HTTP POST Request Handler. The manipulation of the argument visname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7816	A vulnerability, which was classified as problematic, was found in PHPGurukul Apartment Visitors Management System 1.0. Affected is an unknown function of the file /visitor-detail.php of the component HTTP POST Request Handler. The manipulation of the argument visname leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7786	A vulnerability, which was classified as problematic, has been found in Gnuboard g6 up to 6.0.10. This issue affects some unknown processing of the file /bbs/scrap_popin_update/qa/ of the component Post Reply 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.	3.5	More Details
CVE-2025-7803	A vulnerability was found in descreekert wx-discuz up to 12bd4745c63ec203cb32119bf77ead4a923bf277. It has been classified as problematic. This affects the function validToken of the file /wx.php. The manipulation of the argument echostr leads to cross site scripting. It is possible to initiate the attack remotely. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	3.5	More Details
CVE-2025-7791	A vulnerability was found in PHPGurukul Online Security Guards Hiring System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/search.php. The manipulation of the argument searchdata leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-53901	Wasmtime is a runtime for WebAssembly. Prior to versions 24.0.4, 33.0.2, and 34.0.2, a bug in Wasmtime's implementation of the WASIp1 set of import functions can lead to a WebAssembly guest inducing a panic in the host (embedder). The specific bug is triggered by calling `path_open` after calling `fd_renumber` with either two equal argument values or a second argument being equal to a previously-closed file descriptor number value. The corrupt state introduced in `fd_renumber` will lead to the subsequent opening of a file descriptor to panic. This panic cannot introduce memory unsafety or allow WebAssembly to break outside of its sandbox, however. There is no possible heap corruption or memory unsafety from this panic. This bug is in the implementation of Wasmtime's `wasmtime-wasi` crate which provides an implementation of WASIp1. The bug requires a specially crafted call to `fd_renumber` in addition to the ability to open a subsequent file descriptor. Opening a second file descriptor is only possible when a preopened directory was provided to the guest, and this is common amongst embeddings. A panic in the host is considered a denial-of-service vector for	3.5	More Details

	WebAssembly embedders and is thus a security issue in Wasmtime. This bug does not affect WASIp2 and embedders using components. In accordance with Wasmtime's release process, patch releases are available as 24.0.4, 33.0.2, and 34.0.2. Users of other release of Wasmtime are recommended to move to a supported release of Wasmtime. Embedders who are using components or are not providing guest access to create more file descriptors (e.g. via a preopened filesystem directory) are not affected by this issue. Otherwise, there is no workaround at this time, and affected embeddings are recommended to update to a patched version which will not cause a panic in the host.		
CVE-2025-7867	A vulnerability classified as problematic has been found in Portabilis i-Educar 2.9.0. Affected is an unknown function of the file /intranet/agenda.php of the component Agenda Module. The manipulation of the argument novo_titulo leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-7856	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file pass-details.php of the component HTTP POST Request Handler. The manipulation of the argument visname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7869	A vulnerability, which was classified as problematic, has been found in Portabilis i-Educar 2.9.0. Affected by this issue is some unknown functionality of the file intranet/educar_turma_tipo_det.php?cod_turma_tipo=ID of the component Turma Module. The manipulation of the argument nm_tipo leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-7902	A vulnerability classified as problematic has been found in yangzongzhuan RuoYi up to 4.8.1. Affected is the function addSave of the file com/ruoyi/web/controller/system/SysNoticeController.java. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7926	A vulnerability, which was classified as problematic, was found in PHPGurukul Online Banquet Booking System 1.0. This affects an unknown part of the file /admin/booking-search.php. The manipulation of the argument searchdata leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7924	A vulnerability classified as problematic was found in PHPGurukul Online Banquet Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/admin-profile.php. The manipulation of the argument adminname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2025-7870	A vulnerability, which was classified as problematic, was found in Portabilis i-Diario 1.5.0. This affects an unknown part of the component justificativas-de-falta Endpoint. The manipulation of the argument Anexo leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-7800	A vulnerability classified as problematic was found in cgpandey hotelmis up to c572198e6c4780fccc63b1d3e8f3f72f825fc94e. This vulnerability affects unknown code of the file admin.php of the component HTTP GET Request Handler. The manipulation of the argument Search leads to cross site scripting. The attack can be initiated remotely. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	3.5	More Details
CVE-2025-7871	A vulnerability has been found in Portabilis i-Diario 1.5.0 and classified as problematic. This vulnerability affects unknown code of the file /conteudos. The manipulation of the argument filter[by_description] leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2025-	A vulnerability was found in Portabilis i-Diario 1.5.0 and classified as problematic. This issue affects some unknown processing of the file /justificativas-de-falta. The manipulation of the argument Justificativa leads to cross site scripting. The attack may be initiated remotely. The	3.5	More

7872	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.		Details
CVE-2025-7339	on-headers is a node.js middleware for listening to when a response writes headers. A bug in on-headers versions `<1.1.0` may result in response headers being inadvertently modified when an array is passed to `response.writeHead()`. Users should upgrade to version 1.1.0 to receive a patch. Uses are strongly encouraged to upgrade to `1.1.0`, but this issue can be worked around by passing an object to `response.writeHead()` rather than an array.	3.4	More Details
CVE-2025-7884	A vulnerability classified as problematic was found in Eluktronics Control Center 5.23.51.41. Affected by this vulnerability is an unknown functionality of the component REG File Handler. The manipulation leads to insufficient verification of data authenticity. It is possible to launch the attack on the local host. 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.	3.3	More Details
CVE-2025-7882	A vulnerability was found in Mercusys MW301R 1.0.2 Build 190726 Rel.59423n. It has been rated as problematic. This issue affects some unknown processing of the component Login. The manipulation leads to improper restriction of excessive authentication attempts. The attack can only be initiated within the local network. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2025-54314	Thor before 1.4.0 can construct an unsafe shell command from library input.	2.8	More Details
CVE-2025-7881	A vulnerability was found in Mercusys MW301R 1.0.2 Build 190726 Rel.59423n. It has been declared as problematic. This vulnerability affects unknown code of the component Web Interface. The manipulation of the argument code leads to weak password recovery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.7	More Details
CVE-2025-7819	A vulnerability was found in PHPGurukul Apartment Visitors Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /create-pass.php of the component HTTP POST Request Handler. The manipulation of the argument visname leads to cross site scripting. It is possible to initiate the attack remotely.	2.4	More Details
CVE-2025-7815	A vulnerability, which was classified as problematic, has been found in PHPGurukul Apartment Visitors Management System 1.0. This issue affects some unknown processing of the file /manage-newvisitors.php of the component HTTP POST Request Handler. The manipulation of the argument visname leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	2.4	More Details
CVE-2025-6227	Mattermost versions 10.5.x <= 10.5.7, 9.11.x <= 9.11.16 fail to negotiate a new token when accepting the invite which allows a user that intercepts both invite and password to send synchronization payloads to the server that originally created the invite via the REST API.	2.2	More Details
CVE-2025-43881	Improper validation of specified quantity in input issue exists in Real-time Bus Tracking System versions prior to 1.1. If exploited, a denial of service (DoS) condition may be caused by an attacker who can log in to the administrative page of the affected product.	N/A	More Details
CVE-2025-6235	In ExtremeControl before 25.5.12, a cross-site scripting (XSS) vulnerability was discovered in a login interface of the affected application. The issue stems from improper handling of user-supplied input within HTML attributes, allowing an attacker to inject script code that may execute in a user's browser under specific interaction conditions. Successful exploitation could lead to exposure of user data or unauthorized actions within the browser context.	N/A	More Details
CVE-2025-27209	The V8 release used in Node.js v24.0.0 has changed how string hashes are computed using rapidhash. This implementation re-introduces the HashDoS vulnerability as an attacker who can control the strings to be hashed can generate many hash collisions - an attacker can generate collisions even without knowing the hash-seed. * This vulnerability affects Node.js v24.x users.	N/A	More Details
CVE-2025-41100	Incorrect authentication vulnerability in ParkingDoor. Through this vulnerability it is possible to operate the device without the access being logged in the application and even if the access permissions have been revoked.	N/A	More Details

CVE-2025-38351	In the Linux kernel, the following vulnerability has been resolved: KVM: x86/hyper-v: Skip non-canonical addresses during PV TLB flush In KVM guests with Hyper-V hypercalls enabled, the hypercalls HVCALL_FLUSH_VIRTUAL_ADDRESS_LIST and HVCALL_FLUSH_VIRTUAL_ADDRESS_LIST_EX allow a guest to request invalidation of portions of a virtual TLB. For this, the hypercall parameter includes a list of GVAs that are supposed to be invalidated. However, when non-canonical GVAs are passed, there is currently no filtering in place and they are eventually passed to checked invocations of INVVPID on Intel / INVLPGA on AMD. While AMD's INVLPGA silently ignores non-canonical addresses (effectively a no-op), Intel's INVVPID explicitly signals VM-Fail and ultimately triggers the WARN_ONCE in invvpid_error(): invvpid failed: ext=0x0 vpid=1 gva=0xaaaaaaaaaaaaa000 WARNING: CPU: 6 PID: 326 at arch/x86/kvm/vmx/vmx.c:482 invvpid_error+0x91/0xa0 [kvm_intel] Modules linked in: kvm_intel kvm 9pnet_virtio irqbypass fuse CPU: 6 UID: 0 PID: 326 Comm: kvm-vm Not tainted 6.15.0 #14 PREEMPT(voluntary) RIP: 0010:invvpid_error+0x91/0xa0 [kvm_intel] Call Trace: vmx_flush_tlb_gva+0x320/0x490 [kvm_intel] kvm_hv_vcpu_flush_tlb+0x24f/0x4f0 [kvm] kvm_arch_vcpu_ioctl_run+0x3013/0x5810 [kvm] Hyper-V documents that invalid GVAs (those that are beyond a partition's GVA space) are to be ignored. While not completely clear whether this ruling also applies to non-canonical GVAs, it is likely fine to make that assumption, and manual testing on Azure confirms "real" Hyper-V interprets the specification in the same way. Skip non-canonical GVAs when processing the list of address to avoid tripping the INVVPID failure. Alternatively, KVM could filter out "bad" GVAs before inserting into the FIFO, but practically speaking the only downside of pushing validation to the final processing is that doing so is suboptimal for the guest, and no well-behaved guest will request TLB flushes for non-canonical addresses.	N/A	More Details
CVE-2025-7394	In the OpenSSL compatibility layer implementation, the function RAND_poll() was not behaving as expected and leading to the potential for predictable values returned from RAND_bytes() after fork() is called. This can lead to weak or predictable random numbers generated in applications that are both using RAND_bytes() and doing fork() operations. This only affects applications explicitly calling RAND_bytes() after fork() and does not affect any internal TLS operations. Although RAND_bytes() documentation in OpenSSL calls out not being safe for use with fork() without first calling RAND_poll(), an additional code change was also made in wolfSSL to make RAND_bytes() behave similar to OpenSSL after a fork() call without calling RAND_poll(). Now the Hash-DRBG used gets reseeded after detecting running in a new process. If making use of RAND_bytes() and calling fork() we recommend updating to the latest version of wolfSSL. Thanks to Per Allansson from Appgate for the report.	N/A	More Details
CVE-2025-7395	A certificate verification error in wolfSSL when building with the WOLFSSL_SYS_CA_CERTS and WOLFSSL_APPLE_NATIVE_CERT_VALIDATION options results in the wolfSSL client failing to properly verify the server certificate's domain name, allowing any certificate issued by a trusted CA to be accepted regardless of the hostname.	N/A	More Details
CVE-2025-7396	In wolfSSL release 5.8.2 blinding support is turned on by default for Curve25519 in applicable builds. The blinding configure option is only for the base C implementation of Curve25519. It is not needed, or available with; ARM assembly builds, Intel assembly builds, and the small Curve25519 feature. While the side-channel attack on extracting a private key would be very difficult to execute in practice, enabling blinding provides an additional layer of protection for devices that may be more susceptible to physical access or side-channel observation.	N/A	More Details
CVE-2025-29757	An incorrect authorisation check in the the 'plant transfer' function of the Growatt cloud service allowed a malicous attacker with a valid account to transfer any plant into his/her account.	N/A	More Details
CVE-2025-46121	An issue was discovered in CommScope Ruckus Unleashed prior to 200.15.6.212.14 and 200.17.7.0.139, where the functions `stamgr_cfg_adpt_addStaFavourite` and `stamgr_cfg_adpt_addStalot` pass a client hostname directly to snprintf as the format string. A remote attacker can exploit this flaw either by sending a crafted request to the authenticated endpoint `/admin/_conf.jsp`, or without authentication and without direct network access to the controller by spoofing the MAC address of a favourite station and embedding malicious format specifiers in the DHCP hostname field, resulting in unauthenticated format-string processing and arbitrary code execution on the controller.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net/sched: Always pass notifications when child class becomes empty Certain classful qdiscs may invoke their classes' dequeue handler on an enqueue operation. This may unexpectedly empty the child qdisc and		

CVE-2025-38350	thus make an in-flight class passive via qlen_notify(). Most qdiscs do not expect such behaviour at this point in time and may re-activate the class eventually anyways which will lead to a use-after-free. The referenced fix commit attempted to fix this behavior for the HFSC case by moving the backlog accounting around, though this turned out to be incomplete since the parent's parent may run into the issue too. The following reproducer demonstrates this use-after-free: tc qdisc add dev lo root handle 1: drr tc filter add dev lo parent 1: basic classid 1:1 tc class add dev lo parent 1: classid 1:1 drr tc qdisc add dev lo parent 1:1 handle 2: hfsc def 1 tc class add dev lo parent 2: classid 2:1 hfsc rt m1 8 d 1 m2 0 tc qdisc add dev lo parent 2:1 handle 3: netem tc qdisc add dev lo parent 3:1 handle 4: blackhole echo 1 | socat -u STDIN UDP4-DATAGRAM:127.0.0.1:8888 tc class delete dev lo classid 1:1 echo 1 | socat -u STDIN UDP4-DATAGRAM:127.0.0.1:8888 Since backlog accounting issues leading to a use-after-frees on stale class pointers is a recurring pattern at this point, this patch takes a different approach. Instead of trying to fix the accounting, the patch ensures that qdisc_tree_reduce_backlog always calls qlen_notify when the child qdisc is empty. This solves the problem because deletion of qdiscs always involves a call to qdisc_reset() and / or qdisc_purge_queue() which ultimately resets its qlen to 0 thus causing the following qdisc_tree_reduce_backlog() to report to the parent. Note that this may call qlen_notify on passive classes multiple times. This is not a problem after the recent patch series that made all the classful qdiscs qlen_notify() handlers idempotent.	N/A	More Details
CVE-2025-27210	An incomplete fix has been identified for CVE-2025-23084 in Node.js, specifically affecting Windows device names like CON, PRN, and AUX. This vulnerability affects Windows users of `path.join` API.	N/A	More Details
CVE-2025-54120	PCL (Plain Craft Launcher) Community Edition is a Minecraft launcher. In PCL CE versions 2.12.0-beta.5 to 2.12.0-beta.9, the login credentials used during the third-party login process are accidentally recorded in the local log file. Although the log file is not automatically uploaded or shared, if the user manually sends the log file, there is a risk of leakage. This is fixed in version 2.12.0-beta.10.	N/A	More Details
CVE-2025-7723	A command injection vulnerability exists that can be exploited after authentication in VIGI NVR1104H-4P V1 and VIGI NVR2016H-16MP V2.This issue affects VIGI NVR1104H-4P V1: before 1.1.5 Build 250518; VIGI NVR2016H-16MP V2: before 1.3.1 Build 250407.	N/A	More Details
CVE-2025-7724	An unauthenticated OS command injection vulnerability exists in VIGI NVR1104H-4P V1 and VIGI NVR2016H-16MP V2.This issue affects VIGI NVR1104H-4P V1: before 1.1.5 Build 250518; VIGI NVR2016H-16MP V2: before 1.3.1 Build 250407.	N/A	More Details
CVE-2025-4570	An insecure sensitive key storage issue was found in MyASUS. potentially allowing unauthorized actor to obtain a token that could be used to communicate with certain services. Refer to the 'Security Update for for MyASUS' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-43488	A potential security vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.2. The vulnerability could allow a bypass of the application's XSS filter by submitting untrusted characters. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-43487	A potential privilege escalation through Sudo vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.2. The firmware flaw does not properly implement access controls. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-43486	A potential stored cross-site scripting vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.1. The website allows user input to be stored and rendered without proper sanitization. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-43485	A potential security vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.2. The vulnerability could potentially allow a privileged user to retrieve credentials from the log files. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-43484	A potential reflected cross-site scripting vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.1. The website does not validate or sanitize the user input before rendering it in the response. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-43483	A potential security vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.1. The vulnerability could allow the retrieval of hardcoded cryptographic keys. HP has addressed the issue in the latest software update.	N/A	More Details

CVE-2025-43022	A potential SQL injection vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.1. The vulnerability could allow a privileged user to execute SQL commands. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-43021	A potential security vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.1. The vulnerability could allow the use and retrieval of the default password. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-43020	A potential command injection vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.2. The vulnerability could allow a privileged user to submit arbitrary input. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-4569	An insecure sensitive key storage issue was found in MyASUS. potentially allowing unauthorized actor to obtain a token that could be used to communicate with certain services. Refer to the 'Security Update for for MyASUS' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-4049	Use of hard-coded, the same among all vulnerable installations SQLite credentials vulnerability in SIGNUM-NET FARA allows to read and manipulate local-stored database.This issue affects FARA: through 5.0.80.34.	N/A	More Details
CVE-2025-0664	A locally authenticated, privileged user can craft a malicious OpenSSL configuration file, potentially leading the agent to load an arbitrary local library. This may impair endpoint defenses and allow the attacker to achieve code execution with SYSTEM-level privileges.	N/A	More Details
CVE-2025-43489	A potential security vulnerability has been identified in the Poly Clariti Manager for versions prior to 10.12.1. The vulnerability could deserialize untrusted data without validation. HP has addressed the issue in the latest software update.	N/A	More Details
CVE-2025-54079	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.4.6 in the endpoint `/html/atendido/Profile_Atendido.php`, in the `idatendido` parameter. This vulnerability allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. Version 3.4.6 fixes the issue.	N/A	More Details
CVE-2025-7783	Use of Insufficiently Random Values vulnerability in form-data allows HTTP Parameter Pollution (HPP). This vulnerability is associated with program files lib/form_data.Js. This issue affects form-data: < 2.5.4, 3.0.0 - 3.0.3, 4.0.0 - 4.0.3.	N/A	More Details
CVE-2025-7295	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26242.	N/A	More Details
CVE-2025-54070	OpenZeppelin Contracts is a library for secure smart contract development. Starting in version 5.2.0 and prior to version 5.4.0, the `lastIndexOf(bytes,byte,uint256)` function of the `Bytes.sol` library may access uninitialized memory when the following two conditions hold: 1) the provided buffer length is empty (i.e. `buffer.length == 0`) and position is not `2**256 - 1` (i.e. `pos != type(uint256).max`). The `pos` argument could be used to access arbitrary data outside of the buffer bounds. This could lead to the operation running out of gas, or returning an invalid index (outside of the empty buffer). Processing this invalid result for accessing the `buffer` would cause a revert under normal conditions. When triggered, the function reads memory at offset `buffer + 0x20 + pos`. If memory at that location (outside the `buffer`) matches the search pattern, the function would return an out of bound index instead of the expected `type(uint256).max`. This creates unexpected behavior where callers receive a valid-looking index pointing outside buffer bounds. Subsequent memory accesses that don't check bounds and use the returned index must carefully review the potential impact depending on their setup. Code relying on this function returning `type(uint256).max` for empty buffers or using the returned index without bounds checking could exhibit undefined behavior. Users should upgrade to version 5.4.0 to receive a patch.	N/A	More Details
	Livewire is a full-stack framework for Laravel. In Livewire v3 up to and including v3.6.3, a vulnerability allows unauthenticated attackers to achieve remote command execution in specific		

CVE-2025-54068	scenarios. The issue stems from how certain component property updates are hydrated. This vulnerability is unique to Livewire v3 and does not affect prior major versions. Exploitation requires a component to be mounted and configured in a particular way, but does not require authentication or user interaction. This issue has been patched in Livewire v3.6.4. All users are strongly encouraged to upgrade to this version or later as soon as possible. No known workarounds are available.	N/A	More Details
CVE-2025-53817	7-Zip is a file archiver with a high compression ratio. 7-Zip supports extracting from Compound Documents. Prior to version 25.0.0, a null pointer dereference in the Compound handler may lead to denial of service. Version 25.0.0 contains a fix cor the issue.	N/A	More Details
CVE-2025-53816	7-Zip is a file archiver with a high compression ratio. Zeroes written outside heap buffer in RAR5 handler may lead to memory corruption and denial of service in versions of 7-Zip prior to 25.0.0. Version 25.0.0 contains a fix for the issue.	N/A	More Details
CVE-2025-53644	OpenCV is an Open Source Computer Vision Library. Versions prior to 4.12.0 have an uninitialized pointer variable on stack that may lead to arbitrary heap buffer write when reading crafted JPEG images. Version 4.12.0 fixes the vulnerability.	N/A	More Details
CVE-2025-53638	Solady is software that provides Solidity snippets with APIs. Starting in version 0.0.125 and prior to version 0.1.24, when an account is deployed via a proxy, using regular Solidity to call its initialization function may result in a silent failure, if the initialization function does not return a `bool` or some other return data. This is because regular Solidity uses `extcodesize(proxy)` to decide if call succeeds. This is insufficient in the case when the proxy points to an empty implementation. Users should upgrade to Solady v0.1.24 or later to receive a patch. Deploy any affected implementations and their factories on new EVM chains as soon as possible.	N/A	More Details
CVE-2025-51497	An issue was discovered in AdGuard plugin before 1.11.22 for Safari on MacOS. AdGaurd verbosely logged each url that Safari accessed when the plugin was active. These logs went into the MacOS general logs for any unsandboxed process to read. This may be disabled in version 1.11.22.	N/A	More Details
CVE-2024-32323	SQL Injection vulnerability in cnhcit.com Haichang OA v.1.0.0 allows a remote attacker to obtain sensitive information via the if parameter in hcit.project.rte.agents.UploadImages.class.	N/A	More Details
CVE-2025-53867	Island Lake WebBatch before 2025C allows Remote Code Execution via a crafted URL.	N/A	More Details
CVE-2023-47356	Mingyu Security Gateway before v3.0-5.3p was discovered to contain a remote command execution (RCE) vulnerability via the log_type parameter at /log/fw_security.mds.	N/A	More Details
CVE-2023-41566	OA EKP v16 was discovered to contain an arbitrary download vulnerability via the component /ui/sys_ui_extend/sysUiExtend.do. This vulnerability allows attackers to obtain the password of the background administrator and further obtain database permissions.	N/A	More Details
CVE-2025-54064	Rucio is a software framework that provides functionality to organize, manage, and access large volumes of scientific data using customizable policies. The common Rucio helm-charts for the `rucio-server`, `rucio-ui`, and `rucio-webui` define the log format for the apache access log of these components. The `X-Rucio-Auth-Token`, which is part of each request header sent to Rucio, is part of this log format. Thus, each access log line potentially exposes the credentials (Internal Rucio token, or JWT in case of OIDC authentication) of the user. Due to the length of the token (Especially for a JWT) the tokens are often truncated, and thus not usable as credential; nevertheless, the (partial) credential should not be part of the logfile. The impact of this issue is amplified if the access logs are made available to a larger group of people than the instance administrators themselves. An updated release has been supplied for the `rucio-server`, `rucio-ui` and `rucio-webui` helm-chart. The change was also retrofitted for the currently supported Rucio LTS releases. The patched versions are rucio-server 37.0.2, 35.0.1, and 32.0.1; rucio-ui 37.0.4, 35.0.1, and 32.0.2; and rucio-webui 37.0.2, 35.1.1, and 32.0.1. As a workaround, one may update the `logFormat` variable and remove the `X-Rucio-Auth-Token`.	N/A	More Details
CVE-	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.4.6 in		

2025-54062	the `/html/funcionario/profile_dependente.php` endpoint, specifically in the `id_dependente` parameter. This vulnerability allows attackers to execute arbitrary SQL commands, compromising the confidentiality, integrity, and availability of the database. Version 3.4.6 fixes the issue.	N/A	More Details
CVE-2025-54061	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.4.6 in the `idatendido_familiares` parameter of the `/html/funcionario/dependente_editarDoc.php` endpoint. This vulnerability allows attacker to manipulate SQL queries and access sensitive database information, such as table names and sensitive data. Version 3.4.6 fixes the issue.	N/A	More Details
CVE-2025-54060	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.4.6 in the `idatendido_familiares` parameter of the `/html/funcionario/dependente_editarInfoPessoal.php` endpoint. This vulnerability allows attacker to manipulate SQL queries and access sensitive database information, such as table names and sensitive data. Version 3.4.6 fixes the issue.	N/A	More Details
CVE-2025-54058	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.4.6 in the `idatendido_familiares` parameter of the `/html/funcionario/dependente_editarEndereco.php` endpoint. This vulnerability allows attacker to manipulate SQL queries and access sensitive database information, such as table names and sensitive data. Version 3.4.6 fixes the issue.	N/A	More Details
CVE-2025-53946	WeGIA is an open source web manager with a focus on the Portuguese language and charitable institutions. A SQL Injection vulnerability was identified in versions prior to 3.4.5 in the `id_funcionario` parameter of the `/html/saude/profile_paciente.php` endpoint. This vulnerability allows attacker to manipulate SQL queries and access sensitive database information, such as table names and sensitive data. Version 3.4.5 fixes the issue.	N/A	More Details
CVE-2025-8058	The regcomp function in the GNU C library version from 2.4 to 2.41 is subject to a double free if some previous allocation fails. It can be accomplished either by a malloc failure or by using an interposed malloc that injects random malloc failures. The double free can allow buffer manipulation depending of how the regex is constructed. This issue affects all architectures and ABIs supported by the GNU C library.	N/A	More Details
CVE-2025-5346	Bluebird devices contain a pre-loaded barcode scanner application. This application exposes an unsecured broadcast receiver "kr.co.bluebird.android.bbsettings.BootReceiver". A local attacker can call the receiver to overwrite file containing ".json" keyword with default barcode config file. It is possible to overwrite file in any location due to lack of protection against path traversal in name of the file. This issue affects all versions before 1.3.3.	N/A	More Details
CVE-2025-5345	Bluebird devices contain a pre-loaded file manager application. This application exposes an unsecured service provider "com.bluebird.system.koreanpost.IsdcardRemoteService". A local attacker can bind to the AIDL-type service to copy and delete arbitrary files from device's storage with system-level permissions. Version 1.4.4 is vulnerable, vendor reverted vulnerable versions to older version: 1.3.6	N/A	More Details
CVE-2025-5344	Bluebird devices contain a pre-loaded kiosk application. This application exposes an unsecured service provider "com.bluebird.kiosk.launcher.IpartnerKioskRemoteService". A local attacker can bind to the AIDL-type service to modify device's global settings and wallpaper image. This issue affects all versions before 1.1.2.	N/A	More Details
CVE-2025-53942	authentik is an open-source Identity Provider that emphasizes flexibility and versatility, with support for a wide set of protocols. In versions 2025.4.4 and earlier, as well as versions 2025.6.0-rc1 through 2025.6.3, deactivated users who registered through OAuth/SAML or linked their accounts to OAuth/SAML providers can still retain partial access to the system despite their accounts being deactivated. They end up in a half-authenticated state where they cannot access the API but crucially they can authorize applications if they know the URL of the application. To workaround this issue, developers can add an expression policy to the user login stage on the respective authentication flow with the expression of return request.context["pending_user"].is_active. This modification ensures that the return statement only activates the user login stage when the user is active. This issue is fixed in versions authentik 2025.4.4 and 2025.6.4.	N/A	More Details

CVE-2025-54371	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2025-52933	Rejected reason: 3rd party vulnerability	N/A	More Details
CVE-2016-15044	A remote code execution vulnerability exists in Kaltura versions prior to 11.1.0-2 due to unsafe deserialization of user-controlled data within the keditorservices module. An unauthenticated remote attacker can exploit this issue by sending a specially crafted serialized PHP object in the kdata GET parameter to the redirectWidgetCmd endpoint. Successful exploitation leads to execution of arbitrary PHP code in the context of the web server process.	N/A	More Details
CVE-2025-6391	Brocade ASCG before 3.3.0 logs JSON Web Tokens (JWT) in log files. An attacker with access to the log files can withdraw the unencrypted tokens with security implications, such as unauthorized access, session hijacking, and information disclosure.	N/A	More Details
CVE-2022-4978	Remote Control Server, maintained by Steppschuh, 3.1.1.12 allows unauthenticated remote code execution when authentication is disabled, which is the default configuration. The server exposes a custom UDP-based control protocol that accepts remote keyboard input events without verification. An attacker on the same network can issue a sequence of keystroke commands to launch a system shell and execute arbitrary commands, resulting in full system compromise.	N/A	More Details
CVE-2018-25114	A remote code execution vulnerability exists within osCommerce Online Merchant version 2.3.4.1 due to insecure default configuration and missing authentication in the installer workflow. By default, the /install/ directory remains accessible after installation. An unauthenticated attacker can invoke install_4.php, submit crafted POST data, and inject arbitrary PHP code into the configure.php file. When the application later includes this file, the injected payload is executed, resulting in full server-side compromise.	N/A	More Details
CVE-2025-38349	In the Linux kernel, the following vulnerability has been resolved: eventpoll: don't decrement ep refcount while still holding the ep mutex Jann Horn points out that epoll is decrementing the ep refcount and then doing a mutex_unlock(&ep->mtx); afterwards. That's very wrong, because it can lead to a use-after-free. That pattern is actually fine for the very last reference, because the code in question will delay the actual call to "ep_free(ep)" until after it has unlocked the mutex. But it's wrong for the much subtler "next to last" case when somebody *else* may also be dropping their reference and free the ep while we're still using the mutex. Note that this is true even if that other user is also using the same ep mutex: mutexes, unlike spinlocks, can not be used for object ownership, even if they guarantee mutual exclusion. A mutex "unlock" operation is not atomic, and as one user is still accessing the mutex as part of unlocking it, another user can come in and get the now released mutex and free the data structure while the first user is still cleaning up. See our mutex documentation in Documentation/locking/mutex-design.rst, in particular the section [1] about semantics: "mutex_unlock() may access the mutex structure even after it has internally released the lock already - so it's not safe for another context to acquire the mutex and assume that the mutex_unlock() context is not using the structure anymore" So if we drop our ep ref before the mutex unlock, but we weren't the last one, we may then unlock the mutex, another user comes in, drops _their_ reference and releases the 'ep' as it now has no users - all while the mutex_unlock() is still accessing it. Fix this by simply moving the ep refcount dropping to outside the mutex: the refcount itself is atomic, and doesn't need mutex protection (that's the whole _point_ of refcounts: unlike mutexes, they are inherently about object lifetimes).	N/A	More Details
CVE-2025-53888	RIOT-OS, an operating system that supports Internet of Things devices, has an ineffective size check implemented with `assert()` can lead to buffer overflow in versions up to and including 2025.04. Assertions are usually compiled out in production builds. If assertions are the only defense against untrusted inputs, the software may be exposed to attacks that utilize the lack of proper input checks. In the `l2filter_add()` function shown below, `addr_len` is checked using an assertion and is subsequently used as an argument in a `memcpy()` call. When assertions are disabled, there would be no size check for `addr_len`. As a consequence, if an attacker were to provide an `addr_len` value larger than `CONFIG_L2FILTER_ADDR_MAXLEN`, they can trigger a buffer overflow and write past the `list[i].addr` buffer. If the unchecked input is attacker-controlled, the impact of the buffer overflow can range from a denial of service to arbitrary code	N/A	More Details

	execution. Commit f6f7de4ccc107c018630e4c15500825caf02e1c2 contains a patch for the vulnerability.		
CVE-2025-50126	A stored XSS vulnerability in the RSBlog! component 1.11.6-1.14.5 Joomla was discovered. The issue allows remote authenticated users to inject arbitrary web script or HTML via the jform[tags_text] parameter.	N/A	More Details
CVE-2025-50058	A stored XSS vulnerability in the RSDirectory! component 1.0.0-2.2.8 Joomla was discovered. The issue allows remote authenticated attackers to inject arbitrary web script or HTML via the review reply component.	N/A	More Details
CVE-2025-50057	A DOS vulnerability in RSFiles! component 1.16.3-1.17.7 Joomla was discovered. The issue allows unauthenticated remote attackers to deny access to service via the search feature.	N/A	More Details
CVE-2025-50056	A reflected XSS vulnerability in RSMail! component 1.19.20 - 1.22.26 28 Joomla was discovered. The issue allows remote attackers to inject arbitrary web script or HTML via the crafted parameter.	N/A	More Details
CVE-2025-8070	The Windows service configuration of ABP and AES contains an unquoted ImagePath registry value vulnerability. This allows a local attacker to execute arbitrary code by placing a malicious executable in a predictable location such as C:\Program.exe. If the service runs with elevated privileges, exploitation results in privilege escalation to SYSTEM level. This vulnerability arises from an unquoted service path affecting systems where the executable resides in a path containing spaces. Affected products and versions include: ABP 2.0.7.6130 and earlier as well as AES 1.0.6.6133 and earlier.	N/A	More Details
CVE-2025-49486	A stored XSS vulnerability in the Balbooa Gallery plugin 1.0.0-2.4.0 for Joomla allows privileged users to store malicious scripts in gallery items.	N/A	More Details
CVE-2025-49485	A SQL injection vulnerability in the Balbooa Forms plugin 1.0.0-2.3.1.1 for Joomla allows privileged users to execute arbitrary SQL commands via the 'id' parameter.	N/A	More Details
CVE-2025-49484	A SQL injection vulnerability in the JS Jobs plugin versions 1.0.0-1.4.1 for Joomla allows low-privilege users to execute arbitrary SQL commands via the 'cvid' parameter in the employee application feature.	N/A	More Details
CVE-2024-12310	A vulnerability in Imprivata Enterprise Access Management (formerly Imprivata OneSign) allows bypassing the login screen of the shared kiosk workstation and allows unauthorized access to the underlying Windows system through the already logged-in autologon account due to insufficient handling of keyboard shortcuts. This issue affects Imprivata Enterprise Access Management versions 5.3 through 24.2.	N/A	More Details
CVE-2025-2425	Time-of-check to time-of-use race condition vulnerability potentially allowed an attacker to use the installed ESET security software to clear the content of an arbitrary file on the file system.	N/A	More Details
CVE-2025-29572	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2018-25113	An unauthenticated path traversal vulnerability exists in Dicoogle PACS Web Server version 2.5.0 and possibly earlier. The vulnerability allows remote attackers to read arbitrary files on the underlying system by sending a crafted request to the /exportFile endpoint using the UID parameter. Successful exploitation can reveal sensitive files accessible by the web server user.	N/A	More Details
CVE-2025-7398	Brocade ASCG before 3.3.0 allows for the use of medium strength cryptography algorithms on internal ports ports 9000 and 8036.	N/A	More Details
CVE-2025-50127	A SQLi vulnerability in DJ-Flyer component 1.0-3.2 for Joomla was discovered. The issue allows privileged users to execute arbitrary SQL commands.	N/A	More Details
CVE-			

2025-54294	A SQLi vulnerability in Komento component 4.0.0-4.0.7for Joomla was discovered. The issue allows unprivileged users to execute arbitrary SQL commands.	N/A	More Details
CVE-2025-54295	A Reflected XSS vulnerability in DJ-Reviews component 1.0-1.3.6 for Joomla was discovered.	N/A	More Details
CVE-2025-54296	A stored XSS vulnerability in ProFiles component 1.0-1.5.0 for Joomla was discovered.	N/A	More Details
CVE-2025-54297	A stored XSS vulnerability in CComment component 5.0.0-6.1.14 for Joomla was discovered.	N/A	More Details
CVE-2025-7397	A vulnerability in the ascgshell, of Brocade ASCG before 3.3.0 stores any command executed in the Command Line Interface (CLI) in plain text within the command history. A local authenticated user that can access sensitive information like passwords within the CLI history leading to unauthorized access and potential data breaches.	N/A	More Details
CVE-2010-10012	A path traversal vulnerability exists in httpdasm version 0.92, a lightweight Windows HTTP server, that allows unauthenticated attackers to read arbitrary files on the host system. By sending a specially crafted GET request containing a sequence of URL-encoded backslashes and directory traversal patterns, an attacker can escape the web root and access sensitive files outside of the intended directory.	N/A	More Details
CVE-2015-10141	An unauthenticated OS command injection vulnerability exists within Xdebug versions 2.5.5 and earlier, a PHP debugging extension developed by Derick Rethans. When remote debugging is enabled, Xdebug listens on port 9000 and accepts debugger protocol commands without authentication. An attacker can send a crafted eval command over this interface to execute arbitrary PHP code, which may invoke system-level functions such as system() or passthru(). This results in full compromise of the host under the privileges of the web server user.	N/A	More Details
CVE-2016-15045	A local privilege escalation vulnerability exists in lastore-daemon, the system package manager daemon used in Deepin Linux (developed by Wuhan Deepin Technology Co., Ltd.). In versions 0.9.53-1 (Deepin 15.5) and 0.9.66-1 (Deepin 15.7), the D-Bus configuration permits any user in the sudo group to invoke the InstallPackage method without password authentication. By default, the first user created on Deepin is in the sudo group. An attacker with shell access can craft a .deb package containing a malicious post-install script and use dbus-send to install it via lastore-daemon, resulting in arbitrary code execution as root.	N/A	More Details
CVE-2017-20198	The Marathon UI in DC/OS < 1.9.0 allows unauthenticated users to deploy arbitrary Docker containers. Due to improper restriction of volume mount configurations, attackers can deploy a container that mounts the host's root filesystem (/) with read/write privileges. When using a malicious Docker image, the attacker can write to /etc/cron.d/ on the host, achieving arbitrary code execution with root privileges. This impacts any system where the Docker daemon honors Marathon container configurations without policy enforcement.	N/A	More Details
CVE-2025-46123	An issue was discovered in CommScope Ruckus Unleashed prior to 200.15.6.212.14 and 200.17.7.0.139, and in Ruckus ZoneDirector prior to 10.5.1.0.279, where the authenticated configuration endpoint `/admin/_conf.jsp` writes the Wi-Fi guest password to memory with snprintf using the attacker-supplied value as the format string; a crafted password therefore triggers uncontrolled format-string processing and enables remote code execution on the controller.	N/A	More Details
CVE-2025-7294	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26230.	N/A	More Details
	marshmallow-packages/nova-tiptap is a rich text editor for Laravel Nova based on tiptap. Prior to 5.7.0, a vulnerability was discovered in the marshmallow-packages/nova-tiptap Laravel Nova		

CVE-2025-54082	package that allows unauthenticated users to upload arbitrary files to any Laravel disk configured in the application. The vulnerability is due to missing authentication middleware (Nova and Nova.Auth) on the /nova-tiptap/api/file upload endpoint, the lack of validation on uploaded files (no MIME/type or extension restrictions), and the ability for an attacker to choose the disk parameter dynamically. This means an attacker can craft a custom form and send a POST request to /nova-tiptap/api/file, supplying a valid CSRF token, and upload executable or malicious files (e.g., .php, binaries) to public disks such as local, public, or s3. If a publicly accessible storage path is used (e.g. S3 with public access, or Laravel's public disk), the attacker may gain the ability to execute or distribute arbitrary files — amounting to a potential Remote Code Execution (RCE) vector in some environments. This vulnerability was fixed in 5.7.0.	N/A	More Details
CVE-2025-7325	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26434.	N/A	More Details
CVE-2025-7292	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26228.	N/A	More Details
CVE-2025-7291	IrfanView CADImage Plugin DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26227.	N/A	More Details
CVE-2025-7290	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26226.	N/A	More Details
CVE-2025-54127	HAXcms with nodejs backend allows users to start the server in any HAXsite or HAXcms instance. In versions 11.0.6 and below, the NodeJS version of HAXcms uses an insecure default configuration designed for local development. The default configuration does not perform authorization or authentication checks. If a user were to deploy haxcms-nodejs without modifying the default settings, 'HAXCMS_DISABLE_JWT_CHECKS' would be set to 'true' and their deployment would lack session authentication. This is fixed in version 11.0.7.	N/A	More Details
CVE-2025-54128	HAX CMS NodeJs allows users to manage their microsite universe with a NodeJs backend. In versions 11.0.7 and below, the NodeJS version of HAX CMS has a disabled Content Security Policy (CSP). This configuration is insecure for a production application because it does not protect against cross-site-scripting attacks. The contentSecurityPolicy value is explicitly disabled in the application's Helmet configuration in app.js. This is fixed in version 11.0.8.	N/A	More Details
CVE-2025-7289	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26225.	N/A	More Details

CVE-2025-54134	HAX CMS NodeJs allows users to manage their microsite universe with a NodeJs backend. In versions 11.0.8 and below, the HAX CMS NodeJS application crashes when an authenticated attacker provides an API request lacking required URL parameters. This vulnerability affects the listFiles and saveFiles endpoints. This vulnerability exists because the application does not properly handle exceptions which occur as a result of changes to user-modifiable URL parameters. This is fixed in version 11.0.9.	N/A	More Details
CVE-2025-7288	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26224.	N/A	More Details
CVE-2025-7287	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26223.	N/A	More Details
CVE-2025-7286	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26222.	N/A	More Details
CVE-2025-7285	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26221.	N/A	More Details
CVE-2025-7284	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26220.	N/A	More Details
CVE-2025-7283	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26219.	N/A	More Details
CVE-2025-7282	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26216.	N/A	More Details
	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected		

CVE-2025-7281	installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26215.	N/A	More Details
CVE-2025-7280	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26214.	N/A	More Details
CVE-2025-7279	IrfanView CADImage Plugin CGM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26213.	N/A	More Details
CVE-2025-7278	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26211.	N/A	More Details
CVE-2025-7277	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26209.	N/A	More Details
CVE-2025-7276	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26208.	N/A	More Details
CVE-2025-7275	IrfanView CADImage Plugin CGM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26204.	N/A	More Details
CVE-2025-54354	Rejected reason: Not used	N/A	More Details
CVE-2025-54355	Rejected reason: Not used	N/A	More Details
CVE-2025-	Rejected reason: Not used	N/A	More

54356			Details
CVE-2025-54357	Rejected reason: Not used	N/A	More Details
CVE-2025-54358	Rejected reason: Not used	N/A	More Details
CVE-2025-54359	Rejected reason: Not used	N/A	More Details
CVE-2025-7293	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26229.	N/A	More Details
CVE-2025-7324	IrfanView CADImage Plugin DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26430.	N/A	More Details
CVE-2025-54361	Rejected reason: Not used	N/A	More Details
CVE-2025-7323	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26428.	N/A	More Details
CVE-2025-7296	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26243.	N/A	More Details
CVE-2025-7297	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26244.	N/A	More Details
CVE-2025-7298	IrfanView CADImage Plugin DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker	N/A	More Details

	can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26246.		
CVE-2025-7299	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26376.	N/A	More Details
CVE-2025-7300	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26377.	N/A	More Details
CVE-2025-7301	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26380.	N/A	More Details
CVE-2025-7302	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26381.	N/A	More Details
CVE-2025-7303	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26384.	N/A	More Details
CVE-2025-7304	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26385.	N/A	More Details
CVE-2025-7305	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26386.	N/A	More Details
CVE-2025-7306	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage	N/A	More Details

	this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26387.		
CVE-2025-7307	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26388.	N/A	More Details
CVE-2025-7308	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26389.	N/A	More Details
CVE-2025-7309	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26391.	N/A	More Details
CVE-2025-7310	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26393.	N/A	More Details
CVE-2025-7311	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26395.	N/A	More Details
CVE-2025-7312	IrfanView CADImage Plugin DWG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26398.	N/A	More Details
CVE-2025-7313	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26399.	N/A	More Details
CVE-2025-7314	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage	N/A	More Details

	this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26400.		
CVE-2025-7315	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26408.	N/A	More Details
CVE-2025-7316	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26410.	N/A	More Details
CVE-2025-7317	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26411.	N/A	More Details
CVE-2025-7318	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26412.	N/A	More Details
CVE-2025-7319	IrfanView CADImage Plugin DWG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26413.	N/A	More Details
CVE-2025-7320	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26418.	N/A	More Details
CVE-2025-7321	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26421.	N/A	More Details
CVE-2025-7322	IrfanView CADImage Plugin DWG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker	N/A	More Details

	can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26423.		
CVE-2025-54360	Rejected reason: Not used	N/A	More Details
CVE-2025-54362	Rejected reason: Not used	N/A	More Details
CVE-2025-7962	In Jakarta Mail 2.2 it is possible to preform a SMTP Injection by utilizing the \r and \n UTF-8 characters to separate different messages.	N/A	More Details
CVE-2025-7251	IrfanView CADImage Plugin DWG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26108.	N/A	More Details
CVE-2025-7249	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26100.	N/A	More Details
CVE-2025-7248	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26098.	N/A	More Details
CVE-2025-7247	IrfanView CADImage Plugin DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26096.	N/A	More Details
CVE-2025-7246	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26095.	N/A	More Details
CVE-2025-7244	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26093.	N/A	More Details
	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution		

CVE-2025-7243	Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26091.	N/A	More Details
CVE-2025-7242	IrfanView CADImage Plugin DWG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26088.	N/A	More Details
CVE-2025-7241	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26087.	N/A	More Details
CVE-2025-7240	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26086.	N/A	More Details
CVE-2025-7239	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26085.	N/A	More Details
CVE-2025-7238	IrfanView CADImage Plugin DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26084.	N/A	More Details
CVE-2025-7237	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26083.	N/A	More Details
CVE-2025-7236	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26080.	N/A	More Details

CVE-2025-7235	IrfanView CADImage Plugin DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26075.	N/A	More Details
CVE-2025-7234	IrfanView CADImage Plugin CGM File Parsing Out-of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26074.	N/A	More Details
CVE-2025-7233	IrfanView CADImage Plugin DWG File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-26072.	N/A	More Details
CVE-2025-7231	INVT VT-Designer PM3 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of INVT VT-Designer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PM3 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25724.	N/A	More Details
CVE-2025-7230	INVT VT-Designer PM3 File Parsing Type Confusion Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of INVT VT-Designer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PM3 files. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25723.	N/A	More Details
CVE-2025-7229	INVT VT-Designer PM3 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of INVT VT-Designer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PM3 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25722.	N/A	More Details
CVE-2025-7228	INVT VT-Designer PM3 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of INVT VT-Designer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PM3 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25571.	N/A	More Details
CVE-2025-7227	INVT VT-Designer PM3 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of INVT VT-Designer. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PM3 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability	N/A	More Details

	to execute code in the context of the current process. Was ZDI-CAN-25550.		
CVE-2025-7226	INVT HMITool VPM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of INVT HMITool. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VPM files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25048.	N/A	More Details
CVE-2025-7225	INVT HMITool VPM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of INVT HMITool. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VPM files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25047.	N/A	More Details
CVE-2025-7224	INVT HMITool VPM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of INVT HMITool. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VPM files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25045.	N/A	More Details
CVE-2025-7223	INVT HMITool VPM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of INVT HMITool. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of VPM files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25044.	N/A	More Details
CVE-2025-7222	Luxion KeyShot 3DM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Luxion KeyShot. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DM files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26473.	N/A	More Details
CVE-2025-54071	RomM (ROM Manager) allows users to scan, enrich, browse and play their game collections with a clean and responsive interface. In versions 4.0.0-beta.3 and below, an authenticated arbitrary file write vulnerability exists in the /api/saves endpoint. This can lead to Remote Code Execution on the system. The vulnerability permits arbitrary file write operations, allowing attackers to create or modify files at any filesystem location with user-supplied content. A user with viewer role or Scope.ASSETS_WRITE permission or above is required to pass authentication checks. The vulnerability is fixed in version 4.0.0-beta.4.	N/A	More Details
CVE-2025-7250	IrfanView CADImage Plugin DWG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26107.	N/A	More Details
CVE-2025-7252	IrfanView CADImage Plugin DWG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker	N/A	More Details

	can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26109.		
CVE-2025-7274	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26203.	N/A	More Details
CVE-2025-7253	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26112.	N/A	More Details
CVE-2025-7273	IrfanView CADImage Plugin DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26202.	N/A	More Details
CVE-2025-7272	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26198.	N/A	More Details
CVE-2025-7271	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26193.	N/A	More Details
CVE-2025-52580	Insertion of sensitive information into log file issue exists in "region PAY" App for Android prior to 1.5.28. If exploited, sensitive user information may be exposed to an attacker who has access to the application logs.	N/A	More Details
CVE-2025-7270	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26189.	N/A	More Details
CVE-2025-7269	IrfanView CADImage Plugin DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26188.	N/A	More Details
	IrfanView CADImage Plugin DXF File Parsing Out-Of-Bounds Read Remote Code Execution		

CVE-2025-7268	Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26182.	N/A	More Details
CVE-2025-7267	IrfanView CADImage Plugin DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26179.	N/A	More Details
CVE-2025-38352	In the Linux kernel, the following vulnerability has been resolved: posix-cpu-timers: fix race between handle_posix_cpu_timers() and posix_cpu_timer_del() If an exiting non-autoreaping task has already passed exit_notify() and calls handle_posix_cpu_timers() from IRQ, it can be reaped by its parent or debugger right after unlock_task_sighand(). If a concurrent posix_cpu_timer_del() runs at that moment, it won't be able to detect timer->it.cpu.firing != 0: cpu_timer_task_rcu() and/or lock_task_sighand() will fail. Add the tsk->exit_state check into run_posix_cpu_timers() to fix this. This fix is not needed if CONFIG_POSIX_CPU_TIMERS_TASK_WORK=y, because exit_task_work() is called before exit_notify(). But the check still makes sense, task_work_add(&tsk->posix_cputimers_work.work) will fail anyway in this case.	N/A	More Details
CVE-2025-7266	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26174.	N/A	More Details
CVE-2025-7265	IrfanView CADImage Plugin CGM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26173.	N/A	More Details
CVE-2025-7264	IrfanView CADImage Plugin CGM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26171.	N/A	More Details
CVE-2025-7263	IrfanView CADImage Plugin CGM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26170.	N/A	More Details
	IrfanView CADImage Plugin DWG File Parsing Out-Of-Bounds Read Remote Code Execution		

CVE-2025-7262	Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26132.	N/A	More Details
CVE-2025-7261	IrfanView CADImage Plugin DWG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26130.	N/A	More Details
CVE-2025-7260	IrfanView CADImage Plugin DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26129.	N/A	More Details
CVE-2025-7258	IrfanView CADImage Plugin DWG File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26127.	N/A	More Details
CVE-2025-7899	The powermail extension for TYPO3 allows Insecure Direct Object Reference resulting in download of arbitrary files from the webserver. This issue affects powermail version 12.0.0 up to 12.5.2 and version 13.0.0	N/A	More Details
CVE-2025-7900	The femanager extension for TYPO3 allows Insecure Direct Object Reference resulting in unauthorized modification of userdata. This issue affects femanager version 6.4.1 and below, 7.0.0 to 7.5.2 and 8.0.0 to 8.3.0	N/A	More Details
CVE-2025-7257	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26126.	N/A	More Details
CVE-2025-7256	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26119.	N/A	More Details
CVE-2025-34140	An authorization bypass vulnerability exists in ETQ Reliance (legacy CG and NXG SaaS platforms). By appending a specific URI suffix to certain API endpoints, an unauthenticated attacker can bypass access control checks and retrieve limited sensitive resources. The root cause was a misconfiguration in API authorization logic, which has since been corrected in SE.2025.1 and 2025.1.2.	N/A	More Details

CVE-2025-34141	A reflected cross-site scripting (XSS) vulnerability exists in ETQ Reliance CG (legacy) platform within the `SQLConverterServlet` component. This vulnerability requires user interaction, such as clicking a crafted link, and may result in execution of unauthorized scripts in the user's context. The affected servlet was unnecessarily exposed to authenticated users and has since been disabled in version SE.2025.1.	N/A	More Details
CVE-2025-34142	An XML External Entity (XXE) injection vulnerability exists in ETQ Reliance on the CG (legacy) platform within the `/resources/sessions/sso` endpoint. The SAML authentication handler processes XML input without disabling external entity resolution, allowing crafted SAML responses to invoke external entity references. This could enable attackers to retrieve sensitive files or perform server-side request forgery (SSRF). The issue was addressed by disabling external entity processing for the affected XML parser in versions SE.2025.1 and 2025.1.2.	N/A	More Details
CVE-2025-34143	An authentication bypass vulnerability exists in ETQ Reliance on the CG (legacy) platform. The application allowed login as the privileged internal SYSTEM user by manipulating the username field. The SYSTEM account does not require a password, enabling attackers with network access to the login page to obtain elevated access. Once authenticated, an attacker could achieve remote code execution by modifying Jython scripts within the application. This issue was resolved by introducing stricter validation logic to exclude internal accounts from public authentication workflows in version MP-4583.	N/A	More Details
CVE-2025-7255	IrfanView CADImage Plugin DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26118.	N/A	More Details
CVE-2025-7254	IrfanView CADImage Plugin DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView CADImage Plugin. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-26113.	N/A	More Details
CVE-2025-54365	fastapi-guard is a security library for FastAPI that provides middleware to control IPs, log requests, detect penetration attempts and more. In version 3.0.1, the regular expression patched to mitigate the ReDoS vulnerability by limiting the length of string fails to catch inputs that exceed this limit. This type of patch fails to detect cases in which the string representing the attributes of a <script> tag exceeds 100 characters. As a result, most of the regex patterns present in version 3.0.1 can be bypassed. This is fixed in version 3.0.2.	N/A	More Details