SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 24 December 2025

Generated on 24 December 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-2025-67288	An arbitrary file upload vulnerability in Umbraco CMS v16.3.3 allows attackers to execute arbitrary code via uploading a crafted PDF file.	10.0	More Details
CVE-2025-65037	Improper control of generation of code ('code injection') in Azure Container Apps allows an unauthorized attacker to execute code over a network.	10.0	More Details
CVE-2025-44005	An attacker can bypass authorization checks and force a Step CA ACME or SCEP provisioner to create certificates without completing certain protocol authorization checks.	10.0	More Details
CVE-2025-20393	Cisco is aware of a potential vulnerability.&nbsp; Cisco is currently investigating and&nbsp;will update these details as appropriate&nbsp;as more information becomes available.	10.0	More Details
CVE-2025-67108	eProsima Fast-DDS v3.3 was discovered to contain improper validation for ticket revocation, resulting in insecure communications and connections.	10.0	More Details
CVE-2025-65041	Improper authorization in Microsoft Partner Center allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2025-62521	ChurchCRM is an open-source church management system. Prior to version 5.21.0, a pre-authentication remote code execution vulnerability in ChurchCRM's setup wizard allows unauthenticated attackers to inject arbitrary PHP code during the initial installation process, leading to complete server compromise. The vulnerability exists in `setup/routes/setup.php` where user input from the setup form is directly concatenated into a PHP configuration template without any validation or sanitization. Any parameter in the setup form can be used to inject PHP code that gets written to `Include/Config.php`, which is then executed on every page load. This is more severe than typical authenticated RCE vulnerabilities because it requires no credentials and affects the installation process that administrators must complete. Version 5.21.0 patches the issue.	10.0	More Details
CVE-2025-67109	Improper verification of the time certificate in Eclipse Cyclone DDS before v0.10.5 allows attackers to bypass certificate checks and execute commands with System privileges.	10.0	More Details
CVE-2024-57521	SQL Injection vulnerability in RuoYi v.4.7.9 and before allows a remote attacker to execute arbitrary code via the createTable function in SqlUtil.java.	10.0	More Details
CVE-2025-68110	ChurchCRM is an open-source church management system. Versions prior to 6.5.3 may disclose database information in an error message including the host, ip, username, and password. Version 6.5.3 fixes the issue.	9.9	More Details
	n8n is an open source workflow automation platform. Versions starting with 0.211.0 and prior to 1.120.4, 1.121.1, and 1.122.0 contain a critical Remote Code Execution (RCE) vulnerability in their workflow expression evaluation system. Under certain conditions, expressions supplied by authenticated users during workflow configuration may be evaluated in an execution context that is not sufficiently isolated from the underlying runtime. An authenticated attacker could abuse this behavior to execute arbitrary code with the privileges of the n8n process. Successful exploitation may lead to full compromise of the affected instance, including		

CVE-2025-68613	unauthorized access to sensitive data, modification of workflows, and execution of system-level operations. This issue has been fixed in versions 1.120.4, 1.121.1, and 1.122.0. Users are strongly advised to upgrade to a patched version, which introduces additional safeguards to restrict expression evaluation. If upgrading is not immediately possible, administrators should consider the following temporary mitigations: Limit workflow creation and editing permissions to fully trusted users only; and/or deploy n8n in a hardened environment with restricted operating system privileges and network access to reduce the impact of potential exploitation. These workarounds do not fully eliminate the risk and should only be used as short-term measures.	9.9	More Details
CVE-2025-14700	An input neutralization vulnerability in the Webhook Template component of Crafty Controller allows a remote, authenticated attacker to perform remote code execution via Server Side Template Injection.	9.9	More Details
CVE-2025-67164	An authenticated arbitrary file upload vulnerability in the /storage/poc.php component of Pagekit CMS v1.0.18 allows attackers to execute arbitrary code via uploading a crafted PHP file.	9.9	More Details
CVE-2025-67781	An issue was discovered in DriveLock 24.1 before 24.1.6, 24.2 before 24.2.7, and 25.1 before 25.1.5. Local unprivileged users can manipulate privileged processes to gain more privileges on Windows computers.	9.9	More Details
CVE-2025-64663	Custom Question Answering Elevation of Privilege Vulnerability	9.9	More Details
CVE-2025-64374	Unrestricted Upload of File with Dangerous Type vulnerability in StylemixThemes Motors motors allows Using Malicious Files.This issue affects Motors: from n/a through <= 5.6.81.	9.9	More Details
CVE-2023-53951	Ever Gauzy v0.281.9 contains a JWT authentication vulnerability that allows attackers to exploit weak HMAC secret key implementation. Attackers can leverage the exposed JWT token to authenticate and gain unauthorized access with administrative permissions.	9.8	More Details
CVE-2023-53957	Kimai 1.30.10 contains a SameSite cookie vulnerability that allows attackers to steal user session cookies through malicious exploitation. Attackers can trick victims into executing a crafted PHP script that captures and writes session cookie information to a file, enabling potential session hijacking.	9.8	More Details
CVE-2025-67418	ClipBucket 5.5.2 is affected by an improper access control issue where the product is shipped or deployed with hardcoded default administrative credentials. An unauthenticated remote attacker can log in to the administrative panel using these default credentials, resulting in full administrative control of the application.	9.8	More Details
CVE-2025-63665	An issue in GT Edge AI Community Edition Versions before v2.0.12 allows attackers to execute arbitrary code via injecting a crafted JSON payload into the Prompt window.	9.8	More Details
CVE-2025-14733	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS may allow a remote unauthenticated attacker to execute arbitrary code. This vulnerability affects both the Mobile User VPN with IKEv2 and the Branch Office VPN using IKEv2 when configured with a dynamic gateway peer.This vulnerability affects Fireware OS 11.10.2 up to and including 11.12.4_Update1, 12.0 up to and including 12.11.5 and 2025.1 up to and including 2025.1.3.	9.8	More Details
CVE-2023-53948	Lilac-Reloaded for Nagios 2.0.8 contains a remote code execution vulnerability in the autodiscovery feature that allows attackers to inject arbitrary commands. Attackers can exploit the lack of input filtering in the nmap_binary parameter to execute a reverse shell by sending a crafted POST request to the autodiscovery endpoint.	9.8	More Details
CVE-2023-53959	FileZilla Client 3.63.1 contains a DLL hijacking vulnerability that allows attackers to execute malicious code by placing a crafted TextShaping.dll in the application directory. Attackers can generate a reverse shell payload using msfvenom and replace the missing DLL to achieve remote code execution when the application launches.	9.8	More Details
CVE-2023-53950	InnovaStudio WYSIWYG Editor 5.4 contains an unrestricted file upload vulnerability that allows attackers to bypass file extension restrictions through filename manipulation. Attackers can upload malicious ASP shells by using null byte techniques and alternate file extensions to circumvent upload controls in the asset manager.	9.8	More Details
CVE-2025-13329	The File Uploader for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the callback function for the 'add-image-data' REST API endpoint in all versions up to, and including, 1.0.3. This makes it possible for unauthenticated attackers to upload arbitrary files to the Uploadcare service and subsequently download them on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2025-13619	The Flex Store Users plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.1.0. This is due to the 'fsUserHandle::signup' and the 'fsSellerRole::add_role_seller' functions not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site. Note: The vulnerability can be exploited with the 'fs_type' parameter if the Flex Store Seller plugin is also activated.	9.8	More Details
CVE-2025-15006	A weakness has been identified in Tenda WH450 1.0.0.18. Affected by this vulnerability is an unknown functionality of the file /goform/CheckTools of the component HTTP Request Handler. This manipulation of the argument ipaddress causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	9.8	More Details
CVE-2025-15007	A security vulnerability has been detected in Tenda WH450 1.0.0.18. Affected by this issue is some unknown functionality of the file /goform/L7Im of the component HTTP Request Handler. Such manipulation of the argument page leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	9.8	More Details

CVE-2025-15010	A vulnerability has been found in Tenda WH450 1.0.0.18. This issue affects some unknown processing of the file /goform/SafeUrlFilter. The manipulation of the argument page leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	9.8	More Details
CVE-2025-15016	Enterprise Cloud Database developed by Ragic has a Hard-coded Cryptographic Key vulnerability, allowing unauthenticated remote attackers to exploit the fixed key to generate verification information and log into the system as any user.	9.8	More Details
CVE-2025-14964	A vulnerability has been found in TOTOLINK T10 4.1.8cu.5083_B20200521. This affects the function sprintf of the file /cgi-bin/cstecgi.cgi. Such manipulation of the argument loginAuthUrl leads to stack-based buffer overflow. The attack may be performed from remote.	9.8	More Details
CVE-2023-53980	ProjectSend r1605 contains a remote code execution vulnerability that allows attackers to upload malicious files by manipulating file extensions. Attackers can upload shell scripts with disguised extensions through the upload.process.php endpoint to execute arbitrary commands on the server.	9.8	More Details
CVE-2023-53955	SOUND4 IMPACT/FIRST/PULSE/Eco v2.x contains an insecure direct object reference vulnerability that allows attackers to bypass authorization and access hidden system resources. Attackers can exploit the vulnerability by manipulating user-supplied input to execute privileged functionalities without proper authentication.	9.8	More Details
CVE-2025-33222	NVIDIA Isaac Launchable contains a vulnerability where an attacker could exploit a hard-coded credential issue. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, and data tampering.	9.8	More Details
CVE-2025-15047	A vulnerability was found in Tenda WH450 1.0.0.18. This affects an unknown function of the file /goform/PPTPDClient of the component HTTP Request Handler. Performing manipulation of the argument Username results in stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made public and could be used.	9.8	More Details
CVE-2025-15046	A vulnerability has been found in Tenda WH450 1.0.0.18. The impacted element is an unknown function of the file /goform/PPTPClient of the component HTTP Request Handler. Such manipulation of the argument netmsk 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.	9.8	More Details
CVE-2025-15045	A flaw has been found in Tenda WH450 1.0.0.18. The affected element is an unknown function of the file /goform/Natlimit of the component HTTP Request Handler. This manipulation of the argument page causes stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been published and may be used.	9.8	More Details
CVE-2025-15044	A vulnerability was detected in Tenda WH450 1.0.0.18. Impacted is an unknown function of the file /goform/NatStaticSetting. The manipulation of the argument page results in stack-based buffer overflow. The attack may be performed from remote. The exploit is now public and may be used.	9.8	More Details
CVE-2025-65354	Improper input handling in /Grocery/search_products_itname.php inPuneethReddyHC event-management 1.0 permits SQL injection via the sitem_name POST parameter. Crafted payloads can alter query logic and disclose database contents. Exploitation may result in sensitive data disclosure and backend compromise.	9.8	More Details
CVE-2025-51511	Cadmium CMS v.0.4.9 has a background arbitrary file upload vulnerability in /admin/content/filemanager/uploads.	9.8	More Details
CVE-2025-33224	NVIDIA Isaac Launchable contains a vulnerability where an attacker could cause an execution with unnecessary privileges. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, information disclosure and data tampering.	9.8	More Details
CVE-2025-33223	NVIDIA Isaac Launchable contains a vulnerability where an attacker could cause an execution with unnecessary privileges. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, denial of service, information disclosure and data tampering.	9.8	More Details
CVE-2025-29229	linksys E5600 V1.1.0.26 is vulnerable to command injection in the function ddnsStatus.	9.8	More Details
CVE-2023-53963	SOUND4 IMPACT/FIRST/PULSE/Eco v2.x contains an unauthenticated OS command injection vulnerability that allows remote attackers to execute arbitrary shell commands through the 'password' parameter. Attackers can exploit the login.php and index.php scripts by injecting shell commands via the 'password' POST parameter to execute commands with web server privileges.	9.8	More Details
CVE-2025-29228	Linksys E5600 V1.1.0.26 is vulnerable to command injection in the runtime.macClone function via the mc.ip parameter.	9.8	More Details
CVE-2025-50526	Netgear EX8000 V1.0.0.126 was discovered to contain a command injection vulnerability via the switch_status function.	9.8	More Details
CVE-2025-14388	The PhastPress plugin for WordPress is vulnerable to Unauthenticated Arbitrary File Read via null byte injection in all versions up to, and including, 3.7. This is due to a discrepancy between the extension validation in `getExtensionForURL()` which operates on URL-decoded paths, and `appendNormalized()` which strips everything after a null byte before constructing the filesystem path. This makes it possible for unauthenticated attackers to read arbitrary files from the webroot, including wp-config.php, by appending a double URL-encoded null byte (%2500) followed by an allowed extension (.txt) to the file path.	9.8	More Details

CVE-2025-68615	net-snmp is a SNMP application library, tools and daemon. Prior to versions 5.9.5 and 5.10.pre2, a specially crafted packet to an net-snmp snmptrapd daemon can cause a buffer overflow and the daemon to crash. This issue has been patched in versions 5.9.5 and 5.10.pre2.	9.8	More Details
CVE-2025-65856	Authentication bypass vulnerability in Xiongmai XM530 IP cameras on Firmware V5.00.R02.000807D8.10010.346624.S.ONVIF 21.06 allows unauthenticated remote attackers to access sensitive device information and live video streams. The ONVIF implementation fails to enforce authentication on 31 critical endpoints, enabling direct unauthorized video stream access.	9.8	More Details
CVE-2025-59374	"UNSUPPORTED WHEN ASSIGNED" Certain versions of the ASUS Live Update client were distributed with unauthorized modifications introduced through a supply chain compromise. The modified builds could cause devices meeting specific targeting conditions to perform unintended actions. Only devices that met these conditions and installed the compromised versions were affected. The Live Update client has already reached End-of-Support (EOS) in October 2021, and no currently supported devices or products are affected by this issue.	9.8	More Details
CVE-2023-53968	Screen SFT DAB 600/C Firmware 1.9.3 contains a session management vulnerability that allows attackers to bypass authentication controls by exploiting IP address session binding. Attackers can reuse the same IP address and issue unauthorized requests to the userManager API to remove user accounts without proper authentication.	9.8	More Details
CVE-2023-53966	SOUND4 LinkAndShare Transmitter 1.1.2 contains a format string vulnerability that allows attackers to trigger memory stack overflows through maliciously crafted environment variables. Attackers can manipulate the username environment variable with format string payloads to potentially execute arbitrary code and crash the application.	9.8	More Details
CVE-2023-53941	EasyPHP Webserver 14.1 contains an OS command injection vulnerability that allows unauthenticated attackers to execute arbitrary system commands by injecting malicious payloads through the app_service_control parameter. Attackers can send POST requests to /index.php?zone=settings with crafted app_service_control values to execute commands with administrative privileges.	9.8	More Details
CVE-2025-56157	Default credentials in Dify thru 1.5.1. PostgreSQL username and password specified in the docker-compose.yaml file included in its source code.	9.8	More Details
CVE-2025-64236	Authentication Bypass Using an Alternate Path or Channel vulnerability in AmentoTech Tuturn allows Authentication Abuse.This issue affects Tuturn: from n/a before 3.6.	9.8	More Details
CVE-2023-53923	UliCMS 2023.1 contains a privilege escalation vulnerability that allows unauthenticated attackers to create administrative accounts through the UserController endpoint. Attackers can send a crafted POST request to /dist/admin/index.php with specific parameters to generate a new admin user with full system access.	9.8	More Details
CVE-2023-53930	ProjectSend r1605 contains an insecure direct object reference vulnerability that allows unauthenticated attackers to download private files by manipulating the download ID parameter. Attackers can access any user's private files by changing the 'id' parameter in the download request to process.php.	9.8	More Details
CVE-2023-53922	TinyWebGallery v2.5 contains a remote code execution vulnerability in the admin upload functionality that allows unauthenticated attackers to upload malicious PHP files. Attackers can upload .phar files with embedded system commands to execute arbitrary code on the server by accessing the uploaded file's URL.	9.8	More Details
CVE-2023-53921	SitemagicCMS 4.4.3 contains a remote code execution vulnerability that allows attackers to upload malicious PHP files to the files/images directory. Attackers can upload a .phar file with system command execution payload to compromise the web application and execute arbitrary system commands.	9.8	More Details
CVE-2025-53433	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes EasyEat easyeat allows PHP Local File Inclusion.This issue affects EasyEat: from n/a through <= 1.9.0.	9.8	More Details
CVE-2025-54723	Deserialization of Untrusted Data vulnerability in BoldThemes DentiCare denticare allows Object Injection.This issue affects DentiCare: from n/a through < 1.4.3.	9.8	More Details
CVE-2023-53914	UliCMS 2023.1 contains an authentication bypass vulnerability that allows unauthenticated attackers to create admin users through mass assignment in the UserController. Attackers can send a crafted POST request to the admin index.php endpoint with specific parameters to generate an administrative account with full system access.	9.8	More Details
CVE-2025-14879	A weakness has been identified in Tenda WH450 1.0.0.18. Affected is an unknown function of the file /goform/onSSIDChange of the component HTTP Request Handler. This manipulation of the argument ssid_index causes stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	9.8	More Details
CVE-2025-60089	Deserialization of Untrusted Data vulnerability in CRM Perks WP Gravity Forms FreshDesk Plugin gf-freshdesk allows Object Injection.This issue affects WP Gravity Forms FreshDesk Plugin: from n/a through <= 1.3.5.	9.8	More Details
CVE-2025-67791	An issue was discovered in DriveLock 24.1 through 24.1.*, 24.2 through 24.2.*, and 25.1 through 25.1.*. An incomplete configuration (agent authentication) in DriveLock tenant allows attackers to impersonate any DriveLock agent on the network against the DES (DriveLock Enterprise Service).	9.8	More Details
CVE-2025-60090	Deserialization of Untrusted Data vulnerability in CRM Perks WP Gravity Forms Insightly gf-insightly allows Object Injection.This issue affects WP Gravity Forms Insightly: from n/a through <= 1.1.6.	9.8	More Details

CVE-2025-60091	Deserialization of Untrusted Data vulnerability in CRM Perks WP Gravity Forms Zoho CRM and Bigin gf-zoho allows Object Injection.This issue affects WP Gravity Forms Zoho CRM and Bigin: from n/a through <= 1.2.9.	9.8	More Details
CVE-2025-60174	Deserialization of Untrusted Data vulnerability in CRM Perks WP Gravity Forms Constant Contact Plugin gf-constant-contact allows Object Injection.This issue affects WP Gravity Forms Constant Contact Plugin: from n/a through <= 1.1.2.	9.8	More Details
CVE-2025-60178	Deserialization of Untrusted Data vulnerability in CRM Perks WP Gravity Forms HubSpot gf-hubspot allows Object Injection.This issue affects WP Gravity Forms HubSpot: from n/a through <= 1.2.6.	9.8	More Details
CVE-2025-60180	Deserialization of Untrusted Data vulnerability in CRM Perks WP Gravity Forms Salesforce gf-salesforce-crmperks allows Object Injection.This issue affects WP Gravity Forms Salesforce: from n/a through <= 1.5.1.	9.8	More Details
CVE-2025-64188	Incorrect Privilege Assignment vulnerability in PenciDesign Soledad soledad allows Privilege Escalation.This issue affects Soledad: from n/a through <= 8.6.9.	9.8	More Details
CVE-2025-64206	Deserialization of Untrusted Data vulnerability in TieLabs Jannah jannah allows Object Injection.This issue affects Jannah: from n/a through <= 7.6.0.	9.8	More Details
CVE-2025-64227	Deserialization of Untrusted Data vulnerability in BoldGrid Client Invoicing by Sprout Invoices sprout-invoices allows Object Injection.This issue affects Client Invoicing by Sprout Invoices: from n/a through <= 20.8.7.	9.8	More Details
CVE-2025-63389	A critical authentication bypass vulnerability exists in Ollama platform's API endpoints in versions prior to and including v0.12.3. The platform exposes multiple API endpoints without requiring authentication, enabling remote attackers to perform unauthorized model management operations.	9.8	More Details
CVE-2025-67895	Edge3 Worker RPC RCE on Airflow 2. This issue affects Apache Airflow Providers Edge3: before 2.0.0 - and only if you installed and configured it on Airflow 2. The Edge3 provider support in Airflow 2 has been always development-only and not officially released, however if you installed and configured Edge3 provider in Airflow 2, it implicitly enabled non-public (normally) API which was used to test Edge Provider in Airflow 2 during the development. This API allowed Dag author to perform Remote Code Execution in the webserver context, which Dag Author was not supposed to be able to do. If you installed and configured Edge3 provider for Airflow 2, you should uninstall it and migrate to Airflow 3. The new Edge3 provider versions (>=2.0.0) has minimum version of Airflow set to 3 and the RCE-prone Airflow 2 code is removed, so it should no longer be possible to use the Edge3 provider 2.0.0+ on Airflow 2. If you used Edge Provider in Airflow 3, you are not affected.	9.8	More Details
CVE-2022-23851	Netaxis API Orchestrator (APIO) before 0.19.3 allows server side template injection (SSTI).	9.8	More Details
CVE-2025-67165	An Insecure Direct Object Reference (IDOR) in Pagekit CMS v1.0.18 allows attackers to escalate privileges.	9.8	More Details
CVE-2025-67073	A Buffer overflow vulnerability in function fromAdvSetMacMtuWan of bin httpd in Tenda AC10V4.0 V16.03.10.20 allows remote attackers to cause denial of service and possibly code execution by sending a post request with a crafted payload (field `serviceName`) to /goform/AdvSetMacMtuWan.	9.8	More Details
CVE-2025-14878	A security flaw has been discovered in Tenda WH450 1.0.0.18. This impacts an unknown function of the file /goform/wirelessRestart of the component HTTP Request Handler. The manipulation of the argument GO results in stack-based buffer overflow. The attack may be performed from remote. The exploit has been released to the public and may be exploited.	9.8	More Details
CVE-2023-53926	PHPJabbers Simple CMS 5.0 contains a SQL injection vulnerability in the 'column' parameter that allows remote attackers to manipulate database queries. Attackers can inject crafted SQL payloads through the 'column' parameter in the index.php endpoint to potentially extract or modify database information.	9.8	More Details
CVE-2025-43428	A configuration issue was addressed with additional restrictions. This issue is fixed in visionOS 26.2, iOS 26.2 and iPadOS 26.2, macOS Tahoe 26.2. Photos in the Hidden Photos Album may be viewed without authentication.	9.8	More Details
CVE-2025-14860	Use-after-free in the Disability Access APIs component. This vulnerability affects Firefox < 146.0.1.	9.8	More Details
CVE-2025-43526	This issue was addressed with improved URL validation. This issue is fixed in macOS Tahoe 26.2, Safari 26.2. On a Mac with Lockdown Mode enabled, web content opened via a file URL may be able to use Web APIs that should be restricted.	9.8	More Details
CVE-2025-67793	An issue was discovered in DriveLock 24.1 through 24.1.*, 24.2 through 24.2.*, and 25.1 before 25.1.6. Users with the "Manage roles and permissions" privilege can promote themselves or other DOC users to the Supervisor role through an API call. This privilege is included by default in the Administrator role. This issue mainly affects cloud multi-tenant deployments; on-prem single-tenant installations are typically not impacted because local admins usually already have Supervisor privileges.	9.8	More Details
CVE-2025-64233	Deserialization of Untrusted Data vulnerability in BoldThemes Codiqa codiqa allows Object Injection.This issue affects Codiqa: from n/a through < 1.2.8.	9.8	More Details
CVE-2025-64231	Unrestricted Upload of File with Dangerous Type vulnerability in RedefiningTheWeb WordPress Contact Form 7 PDF, Google Sheet & Database rtwwcfp-wordpress-contact-form-7-pdf allows Using Malicious Files.This issue affects WordPress Contact Form 7 PDF, Google Sheet & Database: from n/a through <= 3.0.0.	9.8	More Details
CVE-2025-	An issue was discovered in 25.1.2 before 25.1.5. A Cross Site Scripting (XSS) issue in DriveLock Operations		More Details

67787	Center allows for session takeover over a network.	9.6	
CVE-2025-68112	ChurchCRM is an open-source church management system. In versions prior to 6.5.3, a SQL injection vulnerability in ChurchCRM's Event Attendee Editor allows authenticated users to execute arbitrary SQL commands, leading to complete database compromise, administrative credential theft, and potential system takeover. The vulnerability enables attackers to extract sensitive member data, authentication credentials, and financial information from the church management system. Version 6.5.3 contains a patch for the issue.	9.6	More Details
CVE-2025-68669	5ire is a cross-platform desktop artificial intelligence assistant and model context protocol client. In versions 0.15.2 and prior, an RCE vulnerability exists in useMarkdown.ts, where the markdown-it-mermaid plugin is initialized with securityLevel: 'loose'. This configuration explicitly permits the rendering of HTML tags within Mermaid diagram nodes. This issue has not been patched at time of publication.	9.6	More Details
CVE-2025-66580	Dive is an open-source MCP Host Desktop Application that enables integration with function-calling LLMs. A critical Stored Cross-Site Scripting (XSS) vulnerability exists in versions prior to 0.11.1 in the Mermaid diagram rendering component. The application allows the execution of arbitrary JavaScript via `javascript:`. An attacker can exploit this to inject a malicious Model Context Protocol (MCP) server configuration, leading to Remote Code Execution (RCE) on the victim's machine when the node is clicked. Version 0.11.1 fixes the issue.	9.6	More Details
CVE-2024-27708	Iframe injection vulnerability in aircpt/solucoes-servicos.solucoes MyNET v.26.06 and before allows a remote attacker to execute arbitrary code via the src parameter.	9.6	More Details
CVE-2025-67289	An arbitrary file upload vulnerability in the Attachments module of Frappe Framework v15.89.0 allows attackers to execute arbitrary code via uploading a crafted XML file.	9.6	More Details
CVE-2025-60062	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in mmetrodw tPlayer tplayer-html5-audio-player-with-playlist allows SQL Injection.This issue affects tPlayer: from n/a through <= 1.2.1.6.	9.4	More Details
CVE-2025-58951	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in smartcms Advance Seat Reservation Management for WooCommerce scw-seat-reservation allows SQL Injection.This issue affects Advance Seat Reservation Management for WooCommerce: from n/a through <= 3.1.	9.3	More Details
CVE-2025-68664	LangChain is a framework for building agents and LLM-powered applications. Prior to versions 0.3.81 and 1.2.5, a serialization injection vulnerability exists in LangChain's dumps() and dumpd() functions. The functions do not escape dictionaries with 'lc' keys when serializing free-form dictionaries. The 'lc' key is used internally by LangChain to mark serialized objects. When user-controlled data contains this key structure, it is treated as a legitimate LangChain object during deserialization rather than plain user data. This issue has been patched in versions 0.3.81 and 1.2.5.	9.3	More Details
CVE-2025-68109	ChurchCRM is an open-source church management system. In versions prior to 6.5.3, the Database Restore functionality does not validate the content or file extension of uploaded files. As a result, an attacker can upload a web shell file and subsequently upload a .htaccess file to enable direct access to it. Once accessed, the uploaded web shell allows remote code execution (RCE) on the server. Version 6.5.3 fixes the issue.	9.1	More Details
CVE-2025-66078	Improper Control of Generation of Code ('Code Injection') vulnerability in jetmonsters Hotel Booking Lite motopress-hotel-booking-lite allows Remote Code Inclusion.This issue affects Hotel Booking Lite: from n/a through <= 5.2.3.	9.1	More Details
CVE-2024-49587	Glutton V1 service endpoints were exposed without any authentication on Gotham stacks, this could have allowed users that did not have any permission to hit glutton backend directly and read/update/delete data. The affected service has been patched and automatically deployed to all Apollo-managed Gotham Instances	9.1	More Details
CVE-2025-1928	Improper Restriction of Excessive Authentication Attempts vulnerability in Restajet Information Technologies Inc. Online Food Delivery System allows Password Recovery Exploitation.This issue affects Online Food Delivery System: through 19122025.	9.1	More Details
CVE-2025-34434	AVideo versions prior to 20.1 with the ImageGallery plugin enabled is vulnerable to unauthenticated file upload and deletion. Plugin endpoints responsible for managing gallery images fail to enforce authentication checks and do not validate ownership, allowing unauthenticated attackers to upload or delete images associated with any image-based video.	9.1	More Details
CVE-2025-63386	A Cross-Origin Resource Sharing (CORS) misconfiguration vulnerability exists in Dify v1.9.1 in the /console/api/setup endpoint. The endpoint implements an insecure CORS policy that reflects any Origin header and enables Access-Control-Allow-Credentials: true, permitting arbitrary external domains to make authenticated requests.	9.1	More Details
CVE-2025-68398	Weblate is a web based localization tool. In versions prior to 5.15.1, it was possible to overwrite Git configuration remotely and override some of its behavior. Version 5.15.1 fixes the issue.	9.1	More Details
CVE-2025-63388	A Cross-Origin Resource Sharing (CORS) misconfiguration vulnerability exists in Dify v1.9.1 in the /console/api/system-features endpoint. The endpoint implements an overly permissive CORS policy that reflects arbitrary Origin headers and sets Access-Control-Allow-Credentials: true, allowing any external domain to make authenticated cross-origin requests.	9.1	More Details
	Zerobyte is a backup automation tool Zerobyte versions prior to 0.18.5 and 0.19.0 contain an authentication bypass vulnerability where authentication middleware is not properly applied to API endpoints. This results in certain API endpoints being accessible without valid session credentials. This is dangerous for those who have		

CVE-2025-68435	exposed Zerobyte to be used outside of their internal network. A fix has been applied in both version 0.19.0 and 0.18.5. If immediate upgrade is not possible, restrict network access to the Zerobyte instance to trusted networks only using firewall rules or network segmentation. This is only a temporary mitigation; upgrading is strongly recommended.	9.1	More Details
CVE-2025-66074	Unrestricted Upload of File with Dangerous Type vulnerability in Cozmoslabs WP Webhooks wp-webhooks allows Path Traversal.This issue affects WP Webhooks: from n/a through <= 3.3.8.	9.0	More Details
CVE-2025-47372	Memory Corruption when a corrupted ELF image with an oversized file size is read into a buffer without authentication.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2025-40892	A Stored Cross-Site Scripting vulnerability was discovered in the Reports functionality due to improper validation of an input parameter. An authenticated user with report privileges can define a malicious report containing a JavaScript payload, or a victim can be socially engineered to import a malicious report template. When the victim views or imports the report, the XSS executes in their browser context, allowing the attacker to perform unauthorized actions as the victim, such as modify application data, disrupt application availability, and access limited sensitive information.	8.9	More Details
CVE-2019-25229	An unrestricted file upload vulnerability in Kentico Xperience allows authenticated users with 'Read data' permissions to upload arbitrary file types via MVC form file uploader components. Attackers can manipulate file names and upload potentially malicious files to the system, enabling unauthorized file uploads.	8.8	More Details
CVE-2023-53942	File Thingie 2.5.7 contains an authenticated file upload vulnerability that allows remote attackers to upload malicious PHP zip archives to the web server. Attackers can create a custom PHP payload, upload and unzip it, and then execute arbitrary system commands through a crafted PHP script with a command parameter.	8.8	More Details
CVE-2025-14994	A flaw has been found in Tenda FH1201 and FH1206 1.2.0.14(408)/1.2.0.8(8155). This impacts the function strcat of the file /goform/webtypelibrary of the component HTTP Request Handler. This manipulation of the argument webSiteId causes stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2025-60083	Deserialization of Untrusted Data vulnerability in add-ons.org PDF Invoice Builder for WooCommerce pdf-for-woocommerce allows Object Injection.This issue affects PDF Invoice Builder for WooCommerce: from n/a through <= 6.3.2.	8.8	More Details
CVE-2023-53981	PhotoShow 3.0 contains a remote code execution vulnerability that allows authenticated administrators to inject malicious commands through the exiftran path configuration. Attackers can exploit the ffmpeg configuration settings by base64 encoding a reverse shell command and executing it through a crafted video upload process.	8.8	More Details
CVE-2025-60082	Deserialization of Untrusted Data vulnerability in add-ons.org PDF for WPForms pdf-for-wpforms allows Object Injection.This issue affects PDF for WPForms: from n/a through <= 6.3.1.	8.8	More Details
CVE-2025-14995	A vulnerability has been found in Tenda FH1201 1.2.0.14(408). Affected is the function sprintf of the file /goform/SetIpBind. Such manipulation of the argument page leads to stack-based buffer overflow. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2023-53979	MyBB 1.8.32 contains a chained vulnerability that allows authenticated administrators to bypass avatar upload restrictions and execute arbitrary code. Attackers can modify upload path settings, upload a malicious PHP-embedded image file, and execute commands through the language configuration editing interface.	8.8	More Details
CVE-2025-43529	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 26.2, Safari 26.2, iOS 18.7.3 and iPadOS 18.7.3, iOS 26.2 and iPadOS 26.2, macOS Tahoe 26.2, visionOS 26.2, tvOS 26.2. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 26. CVE-2025-14174 was also issued in response to this report.	8.8	More Details
CVE-2025-60081	Deserialization of Untrusted Data vulnerability in add-ons.org PDF for Contact Form 7 pdf-for-contact-form-7 allows Object Injection.This issue affects PDF for Contact Form 7: from n/a through <= 6.3.4.	8.8	More Details
CVE-2025-59134	Incorrect Privilege Assignment vulnerability in Jthemes Sale! Immigration law, Visa services support, Migration Agent Consulting immiex allows Privilege Escalation.This issue affects Sale! Immigration law, Visa services support, Migration Agent Consulting: from n/a through <= 1.5.8.	8.8	More Details
CVE-2025-62001	BullWall Ransomware Containment contains excluded file paths, such as '$recycle.bin' that are not monitored. An attacker with file write permissions could bypass detection by renaming a directory. Versions 4.6.0.0, 4.6.0.6, 4.6.0.7, and 4.6.1.4 were confirmed to be affected; other versions before and after may also be affected.	8.8	More Details
CVE-2025-68645	A Local File Inclusion (LFI) vulnerability exists in the Webmail Classic UI of Zimbra Collaboration (ZCS) 10.0 and 10.1 because of improper handling of user-supplied request parameters in the RestFilter servlet. An unauthenticated remote attacker can craft requests to the /h/rest endpoint to influence internal request dispatching, allowing inclusion of arbitrary files from the WebRoot directory.	8.8	More Details

CVE-2025-14993	A vulnerability was detected in Tenda AC18 15.03.05.05. This affects the function sprintf of the file /goform/SetDlnaCfg of the component HTTP Request Handler. The manipulation of the argument scanList results in stack-based buffer overflow. The attack can be executed remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2025-68400	ChurchCRM is an open-source church management system. A SQL Injection vulnerability exists in the legacy endpoint `/Reports/ConfirmReportEmail.php` in ChurchCRM prior to version 6.5.3. Although the feature was removed from the UI, the file remains deployed and reachable directly via URL. This is a classic case of *dead but reachable code*. Any authenticated user - including one with zero assigned permissions - can exploit SQL injection through the `familyId` parameter. Version 6.5.3 fixes the issue.	8.8	More Details
CVE-2025-14849	Advantech WebAccess/SCADA is vulnerable to unrestricted file upload, which may allow an attacker to remotely execute arbitrary code.	8.8	More Details
CVE-2023-53971	WebTareas 2.4 contains a file upload vulnerability that allows authenticated users to upload malicious PHP files through the chat photo upload functionality. Attackers can upload a PHP file with arbitrary code to the /files/Messages/ directory and execute it directly through the generated file path.	8.8	More Details
CVE-2023-53933	Serendipity 2.4.0 contains a remote code execution vulnerability that allows authenticated attackers to upload malicious PHP files with .phar extension. Attackers can upload files with system command payloads to the media upload endpoint and execute arbitrary commands on the server.	8.8	More Details
CVE-2025-13941	A local privilege escalation vulnerability exists in the Foxit PDF Reader/Editor Update Service. During plugin installation, incorrect file system permissions are assigned to resources used by the update service. A local attacker with low privileges could modify or replace these resources, which are later executed by the service, resulting in execution of arbitrary code with SYSTEM privileges.	8.8	More Details
CVE-2025-34437	AVideo versions prior to 20.1 permit any authenticated user to upload comment images to videos owned by other users. The endpoint validates authentication but omits ownership checks, allowing attackers to perform unauthorized uploads to arbitrary video objects.	8.8	More Details
CVE-2025-34436	AVideo versions prior to 20.1 allow any authenticated user to upload files into directories belonging to other users due to an insecure direct object reference. The upload functionality verifies authentication but does not enforce ownership checks.	8.8	More Details
CVE-2025-65817	LSC Smart Connect Indoor IP Camera 1.4.13 contains a RCE vulnerability in start_app.sh.	8.8	More Details
CVE-2025-66953	CSRF vulnerability in narda miteq Uplink Power Contril Unit UPC2 v.1.17 allows a remote attacker to execute arbitrary code via the Web-based management interface and specifically the /system_setup.htm, /set_clock.htm, /receiver_setup.htm, /cal.htm?..., and /channel_setup.htm endpoints	8.8	More Details
CVE-2025-66395	ChurchCRM is an open-source church management system. Prior to version 6.5.3, a SQL injection vulnerability exists in the `src/ListEvents.php` file. When filtering events by type, the `WhichType` POST parameter is not properly sanitized or type-casted before being used in multiple SQL queries. This allows any authenticated user to execute arbitrary SQL commands, including time-based blind SQL injection attacks. Any authenticated user, regardless of their privilege level, can execute arbitrary queries on the database. This could allow them to exfiltrate, modify, or delete any data in the database, including user credentials, financial data, and personal information, leading to a full compromise of the application's data. Version 6.5.3 fixes the issue.	8.8	More Details
CVE-2023-53913	Rukovoditel 3.3.1 contains a CSV injection vulnerability that allows authenticated users to inject malicious formulas into the firstname field. Attackers can craft payloads like =calc|a!z| to trigger code execution when an admin exports customer data as a CSV file.	8.8	More Details
CVE-2025-13641	The Photo Gallery, Sliders, Proofing and Themes – NextGEN Gallery plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.59.12 via the 'template' shortcode parameter. This is due to insufficient path validation that allows absolute paths to be provided. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary PHP files on the server, bypassing web server restrictions like .htaccess. Successful exploitation could lead to information disclosure, code execution in the WordPress context, and potential remote code execution if combined with arbitrary file upload capabilities.	8.8	More Details
CVE-2025-14992	A security vulnerability has been detected in Tenda AC18 15.03.05.05. The impacted element is the function strcpy of the file /goform/GetParentControlInfo of the component HTTP Request Handler. The manipulation of the argument mac leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	8.8	More Details
CVE-2025-52692	Successful exploitation of the vulnerability could allow an attacker with local network access to send a specially crafted URL to access certain administration functions without login credentials.	8.8	More Details
CVE-2025-14364	The Demo Importer Plus plugin for WordPress is vulnerable to unauthorized modification of data, loss of data, and privilege escalation due to a missing capability check on the Ajax::handle_request() function in all versions up to, and including, 2.0.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to trigger a full site reset, dropping all database tables except users/usermeta and re-running wp_install(), which also assigns the Administrator role to the attacking subscriber account.	8.8	More Details
CVE-	Dotclear 2.25.3 contains a remote code execution vulnerability that allows authenticated attackers to upload malicious		More

2023-53952	PHP files with .phar extension through the blog post creation interface. Attackers can upload files containing PHP system commands that execute when the uploaded file is accessed, enabling arbitrary code execution on the server.	8.8	Details
CVE-2023-53956	Flatnux 2021-03.25 contains an authenticated file upload vulnerability that allows administrative users to upload arbitrary PHP files through the file manager. Attackers with admin credentials can upload malicious PHP scripts to the web root directory, enabling remote code execution on the server.	8.8	More Details
CVE-2021-47736	CMSimple_XH 1.7.4 contains an authenticated remote code execution vulnerability in the content editing functionality that allows administrative users to upload malicious PHP files. Attackers with valid credentials can exploit the CSRF token mechanism to create a PHP shell file that enables arbitrary command execution on the server.	8.8	More Details
CVE-2025-14861	Memory safety bugs present in Firefox 146. 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 < 146.0.1.	8.8	More Details
CVE-2021-47735	CMSimple 5.4 contains an authenticated remote code execution vulnerability that allows logged-in attackers to inject malicious PHP code into template files. Attackers can exploit the template editing functionality by crafting a reverse shell payload and saving it through the template editing endpoint with a valid CSRF token.	8.8	More Details
CVE-2023-53929	phpMyFAQ 3.1.12 contains a CSV injection vulnerability that allows authenticated users to inject malicious formulas into their profile names. Attackers can modify their user profile name with a payload like 'calc|a!z|' to trigger code execution when an administrator exports user data as a CSV file.	8.8	More Details
CVE-2021-47721	Orangescrum 1.8.0 contains a privilege escalation vulnerability that allows authenticated users to take over other project-assigned accounts by manipulating session cookies. Attackers can extract the victim's unique ID from the page source and replace their own session cookie to gain unauthorized access to another user's account.	8.8	More Details
CVE-2023-53945	BrainyCP 1.0 contains an authenticated remote code execution vulnerability that allows logged-in users to inject arbitrary commands through the crontab configuration interface. Attackers can exploit the crontab endpoint by adding a malicious command that spawns a reverse shell to a specified IP and port.	8.8	More Details
CVE-2023-53927	PHPJabbers Simple CMS 5.0 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through section name parameters. Attackers can create sections with embedded JavaScript payloads that will execute when administrators view the sections, potentially enabling client-side code execution.	8.8	More Details
CVE-2025-67877	ChurchCRM is an open-source church management system. Versions prior to 6.5.3 have a SQL injection vulnerability in the `src/CartToFamily.php` file, specifically in how the `PersonAddress` POST parameter is handled. Unlike other parameters in the same file which are correctly cast to integers using the `InputUtils` class, the `PersonAddress` parameter is missing the type definition. This allows an attacker to inject arbitrary SQL commands directly into the query. Version 6.5.3 fixes the issue.	8.8	More Details
CVE-2025-64266	Deserialization of Untrusted Data vulnerability in magepeopleteam Booking and Rental Manager booking-and-rental-manager-for-woocommerce allows Object Injection.This issue affects Booking and Rental Manager: from n/a through <= 2.5.4.	8.8	More Details
CVE-2025-59886	Improper input validation at one of the endpoints of Eaton xComfort ECI's web interface, could lead into an attacker with network access to the device executing privileged user commands. As cybersecurity standards continue to evolve and to meet our requirements today, Eaton has decided to discontinue the product. Upon retirement or end of support, there will be no new security updates, non-security updates, or paid assisted support options, or online technical content updates.	8.8	More Details
CVE-2025-46281	A logic issue was addressed with improved checks. This issue is fixed in macOS Tahoe 26.2. An app may be able to break out of its sandbox.	8.8	More Details
CVE-2021-47711	A SQL injection vulnerability in Kentico Xperience allows authenticated editors to inject malicious SQL queries via online marketing macro method parameters. This enables unauthorized database access and potential data manipulation by exploiting macro method input validation weaknesses.	8.8	More Details
CVE-2025-68434	Open Source Point of Sale (opensourcepos) is a web based point of sale application written in PHP using CodeIgniter framework. Starting in version 3.4.0 and prior to version 3.4.2, a Cross-Site Request Forgery (CSRF) vulnerability exists in the application's filter configuration. The CSRF protection mechanism was **explicitly disabled**, allowing the application to process state-changing requests (POST) without verifying a valid CSRF token. An unauthenticated remote attacker can exploit this by hosting a malicious web page. If a logged-in administrator visits this page, their browser is forced to send unauthorized requests to the application. A successful exploit allows the attacker to silently create a new Administrator account with full privileges, leading to a complete takeover of the system and loss of confidentiality, integrity, and availability. The vulnerability has been patched in version 3.4.2. The fix re-enables the CSRF filter in `app/Config/Filters.php` and resolves associated AJAX race conditions by adjusting token regeneration settings. As a workaround, administrators can manually re-enable the CSRF filter in `app/Config/Filters.php` by uncommenting the protection line. However, this is not recommended without applying the full patch, as it may cause functionality breakage in the Sales module due to token synchronization issues.	8.8	More Details
CVE-2023-53905	ProjectSend r1605 contains a CSV injection vulnerability that allows authenticated users to inject malicious formulas into user profile names. Attackers can craft payloads like =calc|a!z| in the name field to trigger code execution when administrators export action logs as CSV files.	8.8	More Details
CVE-2023-	UliCMS 2023.1-sniffing-vicuna contains a remote code execution vulnerability that allows authenticated attackers to upload PHP files with .phar extension during profile avatar upload. Attackers can trigger code execution by visiting the	8.8	More Details

53924	uploaded file's location, enabling system command execution through maliciously crafted avatar uploads.		
CVE-2025-58710	Incorrect Privilege Assignment vulnerability in e-plugins Hotel Listing hotel-listing allows Privilege Escalation.This issue affects Hotel Listing: from n/a through <= 1.4.0.	8.6	More Details
CVE-2025-54741	Missing Authorization vulnerability in Tyler Moore Super Blank super-blank allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Super Blank: from n/a through <= 1.2.0.	8.6	More Details
CVE-2025-60084	Deserialization of Untrusted Data vulnerability in add-ons.org PDF for Elementor Forms + Drag And Drop Template Builder pdf-for-elementor-forms allows Object Injection.This issue affects PDF for Elementor Forms + Drag And Drop Template Builder: from n/a through <= 6.3.1.	8.6	More Details
CVE-2025-68665	LangChain is a framework for building LLM-powered applications. Prior to @langchain/core versions 0.3.80 and 1.1.8, and prior to langchain versions 0.3.37 and 1.2.3, a serialization injection vulnerability exists in LangChain JS's toJSON() method (and subsequently when string-ifying objects using JSON.stringify(). The method did not escape objects with 'lc' keys when serializing free-form data in kwargs. The 'lc' key is used internally by LangChain to mark serialized objects. When user-controlled data contains this key structure, it is treated as a legitimate LangChain object during deserialization rather than plain user data. This issue has been patched in @langchain/core versions 0.3.80 and 1.1.8, and langchain versions 0.3.37 and 1.2.3	8.6	More Details
CVE-2025-14314	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Roxnor PopupKit popup-builder-block allows Blind SQL Injection.This issue affects PopupKit: from n/a through <= 2.1.5.	8.5	More Details
CVE-2025-64371	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in shinetheme Traveler traveler allows Blind SQL Injection.This issue affects Traveler: from n/a through < 3.2.6.	8.5	More Details
CVE-2023-53946	Arcsoft PhotoStudio 6.0.0.172 contains an unquoted service path vulnerability in the ArcSoft Exchange Service that allows local attackers to escalate privileges. Attackers can place a malicious executable in the unquoted path and trigger the service to execute arbitrary code with system-level permissions.	8.4	More Details
CVE-2022-50688	Cobian Backup Gravity 11.2.0.582 contains an unquoted service path vulnerability that allows local users to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted service path in the CobianBackup11 service to inject malicious code that would execute with LocalSystem privileges during service startup.	8.4	More Details
CVE-2022-50690	Wondershare MirrorGo 2.0.11.346 contains a local privilege escalation vulnerability due to incorrect file permissions on executable files. Unprivileged local users can replace the ElevationService.exe with a malicious file to execute arbitrary code with LocalSystem privileges.	8.4	More Details
CVE-2023-53949	AspEmail 5.6.0.2 contains a binary permission vulnerability that allows local users to escalate privileges through the Persits Software EmailAgent service. Attackers can exploit full write permissions in the BIN directory to replace the service executable and gain elevated system access.	8.4	More Details
CVE-2023-53947	OCS Inventory NG 2.3.0.0 contains an unquoted service path vulnerability that allows local attackers to escalate privileges to system level. Attackers can place a malicious executable in the unquoted service path and trigger the service restart to execute code with elevated system privileges.	8.4	More Details
CVE-2021-47739	Epic Games Easy Anti-Cheat 4.0 contains an unquoted service path vulnerability that allows local non-privileged users to execute arbitrary code with elevated system privileges. Attackers can exploit the service configuration by inserting malicious code in the system root path that would execute with LocalSystem privileges during application startup.	8.4	More Details
CVE-2023-53965	SOUND4 Server Service 4.1.102 contains an unquoted service path vulnerability that allows local non-privileged users to potentially execute code with elevated system privileges. Attackers can exploit the unquoted binary path by inserting malicious code in the system root path that could execute with LocalSystem privileges during service startup.	8.4	More Details
CVE-2025-14096	A vulnerability exists in multiple Radiometer products that allow an attacker with physical access to the analyzer possibility to extract credential information. The vulnerability is due to a weakness in the design and insufficient credential protection in operating system. Other related CVE's are CVE-2025-14095 & CVE-2025-14097. Affected customers have been informed about this vulnerability. This CVE is being published to provide transparency. Required Configuration for Exposure: Attacker requires physical access to the analyzer. Temporary work Around: Only authorized people can physically access the analyzer. Permanent solution: Local Radiometer representatives will contact all affected customers to discuss a permanent solution. Exploit Status: Researchers have provided a working proof-of-concept (PoC). Radiometer is not aware of any public exploit code at the time of this publication.	8.4	More Details
CVE-2023-53973	Zillya Total Security 3.0.2367.0 contains a privilege escalation vulnerability that allows low-privileged users to copy files to unauthorized system locations using the quarantine module. Attackers can leverage symbolic link techniques to restore quarantined files to restricted directories, potentially enabling system-level access through techniques like DLL hijacking.	8.4	More Details
CVE-2025-25364	A command injection vulnerability in the me.connectify.SMJobBlessHelper XPC service of Speedify VPN up to v15.0.0 allows attackers to execute arbitrary commands with root-level privileges.	8.4	More Details
CVE-2025-64675	Improper neutralization of input during web page generation ('cross-site scripting') in Azure Cosmos DB allows an unauthorized attacker to perform spoofing over a network.	8.3	More Details

CVE-2025-66397	ChurchCRM is an open-source church management system. Prior to version 6.5.3, the allowRegistration, acceptKiosk, reloadKiosk, and identifyKiosk functions in the Kiosk Manager feature suffers from broken access control, allowing any authenticated user to allow and accept kiosk registrations, and perform other Kiosk Manager actions such as reload and identify. Version 6.5.3 fixes the issue.	8.3	More Details
CVE-2025-14727	A vulnerability exists in NGINX Ingress Controller's nginx.org/rewrite-target annotation validation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.3	More Details
CVE-2025-67843	A Server-Side Template Injection (SSTI) vulnerability in the MDX Rendering Engine in Mintlify Platform before 2025-11-15 allows remote attackers to execute arbitrary code via inline JSX expressions in an MDX file.	8.3	More Details
CVE-2025-58932	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Prisma prisma allows PHP Local File Inclusion.This issue affects Prisma: from n/a through <= 1.10.	8.2	More Details
CVE-2025-58931	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Palatio palatio allows PHP Local File Inclusion.This issue affects Palatio: from n/a through <= 1.6.	8.2	More Details
CVE-2025-64205	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in TieLabs Jannah jannah allows PHP Local File Inclusion.This issue affects Jannah: from n/a through <= 7.6.0.	8.2	More Details
CVE-2025-58945	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes EcoGrow ecogrow allows PHP Local File Inclusion.This issue affects EcoGrow: from n/a through <= 1.7.	8.2	More Details
CVE-2025-64677	Improper neutralization of input during web page generation ('cross-site scripting') in Office Out-of-Box Experience allows an unauthorized attacker to perform spoofing over a network.	8.2	More Details
CVE-2025-58929	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Pantry pantry allows PHP Local File Inclusion.This issue affects Pantry: from n/a through <= 1.4.	8.2	More Details
CVE-2025-58944	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Manufactory manufactory allows PHP Local File Inclusion.This issue affects Manufactory: from n/a through <= 1.4.	8.2	More Details
CVE-2025-58943	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Agricola agricola allows PHP Local File Inclusion.This issue affects Agricola: from n/a through <= 1.1.0.	8.2	More Details
CVE-2025-58930	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes FitFlex fitflex allows PHP Local File Inclusion.This issue affects FitFlex: from n/a through <= 1.6.	8.2	More Details
CVE-2023-53982	PMB 7.4.6 contains a SQL injection vulnerability in the storage parameter of the ajax.php endpoint that allows remote attackers to manipulate database queries. Attackers can exploit the unsanitized 'id' parameter by injecting conditional sleep statements to extract information or perform time-based blind SQL injection attacks.	8.2	More Details
CVE-2025-58889	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Towny towny allows PHP Local File Inclusion.This issue affects Towny: from n/a through <= 1.16.	8.2	More Details
CVE-2025-58888	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes The Flash theflash allows PHP Local File Inclusion.This issue affects The Flash: from n/a through <= 1.15.	8.2	More Details
CVE-2025-58942	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Dwell dwell allows PHP Local File Inclusion.This issue affects Dwell: from n/a through <= 1.7.0.	8.2	More Details
CVE-2025-58941	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Fabric fabric allows PHP Local File Inclusion.This issue affects Fabric: from n/a through <= 1.5.0.	8.2	More Details
CVE-2023-53975	Atom CMS 2.0 contains an unauthenticated SQL injection vulnerability that allows remote attackers to manipulate database queries through unvalidated parameters. Attackers can inject malicious SQL code in the 'id' parameter of the admin index page to execute time-based blind SQL injection attacks.	8.2	More Details
CVE-2025-58885	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Pathfinder pathfinder allows PHP Local File Inclusion.This issue affects Pathfinder: from n/a through <= 1.16.	8.2	More Details
CVE-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability		More

2025-58879	in AncoraThemes Festy festy allows PHP Local File Inclusion.This issue affects Festy: from n/a through <= 1.13.0.	8.2	Details
CVE-2025-58803	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Algenix algenix allows PHP Local File Inclusion.This issue affects Algenix: from n/a through <= 1.0.	8.2	More Details
CVE-2025-58940	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Basil basil allows PHP Local File Inclusion.This issue affects Basil: from n/a through <= 1.3.12.	8.2	More Details
CVE-2023-53960	SOUND4 IMPACT/FIRST/PULSE/Eco version 2.x contains an SQL injection vulnerability in the 'index.php' authentication mechanism that allows attackers to manipulate login credentials. Attackers can inject malicious SQL code through the 'password' POST parameter to bypass authentication and potentially gain unauthorized access to the system.	8.2	More Details
CVE-2025-58946	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Vocal vocal allows PHP Local File Inclusion.This issue affects Vocal: from n/a through <= 1.12.	8.2	More Details
CVE-2025-58892	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Tourimo tourimo allows PHP Local File Inclusion.This issue affects Tourimo: from n/a through <= 1.2.3.	8.2	More Details
CVE-2025-58895	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Integro integro allows PHP Local File Inclusion.This issue affects Integro: from n/a through <= 1.8.0.	8.2	More Details
CVE-2025-58898	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes HealthHub healthhub allows PHP Local File Inclusion.This issue affects HealthHub: from n/a through <= 1.3.0.	8.2	More Details
CVE-2025-60055	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Fabrica fabrica allows PHP Local File Inclusion.This issue affects Fabrica: from n/a through <= 1.8.1.	8.2	More Details
CVE-2025-60054	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes OnLeash onleash allows PHP Local File Inclusion.This issue affects OnLeash: from n/a through <= 1.5.2.	8.2	More Details
CVE-2025-60053	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes MaxCube maxcube allows PHP Local File Inclusion.This issue affects MaxCube: from n/a through <= 1.3.1.	8.2	More Details
CVE-2025-60052	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes W&D wd allows PHP Local File Inclusion.This issue affects W&D: from n/a through <= 1.0.	8.2	More Details
CVE-2025-58894	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Good Mood good-mood allows PHP Local File Inclusion.This issue affects Good Mood: from n/a through <= 1.16.	8.2	More Details
CVE-2025-60051	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Rare Radio rareradio allows PHP Local File Inclusion.This issue affects Rare Radio: from n/a through <= 1.0.15.1.	8.2	More Details
CVE-2025-58893	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Alright alright allows PHP Local File Inclusion.This issue affects Alright: from n/a through <= 1.6.1.	8.2	More Details
CVE-2025-60063	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Rosalinda rosalinda allows PHP Local File Inclusion.This issue affects Rosalinda: from n/a through <= 1.2.3.	8.2	More Details
CVE-2025-60050	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Panda panda allows PHP Local File Inclusion.This issue affects Panda: from n/a through <= 1.21.	8.2	More Details
CVE-2025-58947	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Athos athos allows PHP Local File Inclusion.This issue affects Athos: from n/a through <= 1.9.	8.2	More Details
CVE-2025-60049	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Soleil soleil allows PHP Local File Inclusion.This issue affects Soleil: from n/a through <= 1.17.	8.2	More Details
CVE-2025-58891	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Sanger sanger allows PHP Local File Inclusion.This issue affects Sanger: from n/a through <= 1.24.0.	8.2	More Details

CVE-2023-53972	WebTareas 2.4 contains a SQL injection vulnerability in the webTareasSID cookie parameter that allows unauthenticated attackers to manipulate database queries. Attackers can exploit error-based and time-based blind SQL injection techniques to extract database information and potentially access sensitive system data.	8.2	More Details
CVE-2025-58890	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Playful playful allows PHP Local File Inclusion.This issue affects Playful: from n/a through <= 1.19.0.	8.2	More Details
CVE-2025-53453	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Hygia hygia allows PHP Local File Inclusion.This issue affects Hygia: from n/a through <= 1.16.	8.2	More Details
CVE-2025-11774	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the software keyboard function (hereinafter referred to as "keypad function") of Mitsubishi Electric GENESIS64 versions 10.97.2 CFR3 and prior, Mitsubishi Electric Iconics Digital Solutions GENESIS64 versions 10.97.2 CFR3 and prior, Mitsubishi Electric ICONICS Suite versions 10.97.2 CFR3 and prior, Mitsubishi Electric Iconics Digital Solutions ICONICS Suite versions 10.97.2 CFR3 and prior, Mitsubishi Electric MobileHMI versions 10.97.2 CFR3 and prior, Mitsubishi Electric Iconics Digital Solutions MobileHMI versions 10.97.2 CFR3 and prior, and Mitsubishi Electric MC Works64 all versions allows a local attacker to execute arbitrary executable files (EXE) when a legitimate user uses the keypad function by tampering with the configuration file for the function. This could allow the attacker to disclose, tamper with, delete, or destroy information stored on the PC where the affected product is installed, or cause a denial-of-service (DoS) condition on the system, through the execution of the EXE.	8.2	More Details
CVE-2025-60072	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Processby Anchor smooth scroll anchor-smooth-scroll allows PHP Local File Inclusion.This issue affects Anchor smooth scroll: from n/a through <= 1.0.2.	8.2	More Details
CVE-2025-58896	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Otaku otaku allows PHP Local File Inclusion.This issue affects Otaku: from n/a through <= 1.8.0.	8.2	More Details
CVE-2025-53449	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Convex convex allows PHP Local File Inclusion.This issue affects Convex: from n/a through <= 1.11.	8.1	More Details
CVE-2025-68147	Open Source Point of Sale (opensourcepos) is a web based point of sale application written in PHP using CodeIgniter framework. Starting in version 3.4.0 and prior to version 3.4.2, a Stored Cross-Site Scripting (XSS) vulnerability exists in the "Return Policy" configuration field. The application does not properly sanitize user input before saving it to the database or displaying it on receipts. An attacker with access to the "Store Configuration" (such as a rogue administrator or an account compromised via the separate CSRF vulnerability) can inject malicious JavaScript payloads into this field. These payloads are executed in the browser of any user (including other administrators and sales staff) whenever they view a receipt or complete a transaction. This can lead to session hijacking, theft of sensitive data, or unauthorized actions performed on behalf of the victim. The vulnerability has been patched in version 3.4.2 by ensuring the output is escaped using the `esc()` function in the receipt template. As a temporary mitigation, administrators should ensure the "Return Policy" field contains only plain text and strictly avoid entering any HTML tags. There is no code-based workaround other than applying the patch.	8.1	More Details
CVE-2025-53448	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Rally rally allows PHP Local File Inclusion.This issue affects Rally: from n/a through <= 1.1.	8.1	More Details
CVE-2025-6326	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Inset inset allows PHP Local File Inclusion.This issue affects Inset: from n/a through <= 1.18.0.	8.1	More Details
CVE-2025-53447	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Assembly assembly allows PHP Local File Inclusion.This issue affects Assembly: from n/a through <= 1.1.	8.1	More Details
CVE-2025-49363	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Kings & Queens kings-queens allows PHP Local File Inclusion.This issue affects Kings & Queens: from n/a through <= 1.1.16.	8.1	More Details
CVE-2025-49942	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Gardis gardis allows PHP Local File Inclusion.This issue affects Gardis: from n/a through <= 1.2.13.	8.1	More Details
CVE-2025-49941	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes GlamChic glamchic allows PHP Local File Inclusion.This issue affects GlamChic: from n/a through <= 1.0.11.	8.1	More Details
CVE-2025-49359	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes ShieldGroup shieldgroup allows PHP Local File Inclusion.This issue affects ShieldGroup: from n/a through <= 2.13.	8.1	More Details
CVE-2025-49360	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Militarology militarology allows PHP Local File Inclusion.This issue affects Militarology: from n/a through <= 1.0.15.	8.1	More Details

CVE-2025-49361	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Mamita mamita allows PHP Local File Inclusion.This issue affects Mamita: from n/a through <= 1.0.9.	8.1	More Details
CVE-2025-49362	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Gracioza gracioza allows PHP Local File Inclusion.This issue affects Gracioza: from n/a through <= 1.0.15.	8.1	More Details
CVE-2025-49364	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Ludos Paradise ludos-paradise allows PHP Local File Inclusion.This issue affects Ludos Paradise: from n/a through <= 2.1.3.	8.1	More Details
CVE-2025-53446	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Beautique beautique allows PHP Local File Inclusion.This issue affects Beautique: from n/a through <= 1.5.	8.1	More Details
CVE-2025-49365	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Jack Well jack-well allows PHP Local File Inclusion.This issue affects Jack Well: from n/a through <= 1.0.14.	8.1	More Details
CVE-2025-49366	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Hanani hanani allows PHP Local File Inclusion.This issue affects Hanani: from n/a through <= 1.2.11.	8.1	More Details
CVE-2025-49367	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Monyxi monyxi allows PHP Local File Inclusion.This issue affects Monyxi: from n/a through <= 1.1.8.	8.1	More Details
CVE-2025-49368	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Palladio palladio allows PHP Local File Inclusion.This issue affects Palladio: from n/a through <= 1.1.10.	8.1	More Details
CVE-2025-49369	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Lettuce lettuce allows PHP Local File Inclusion.This issue affects Lettuce: from n/a through <= 1.1.7.	8.1	More Details
CVE-2025-49370	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Lymcoin lymcoin allows PHP Local File Inclusion.This issue affects Lymcoin: from n/a through <= 1.3.12.	8.1	More Details
CVE-2025-14850	Advantech WebAccess/SCADA is vulnerable to directory traversal, which may allow an attacker to delete arbitrary files.	8.1	More Details
CVE-2025-49943	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Femme femme allows PHP Local File Inclusion.This issue affects Femme: from n/a through <= 1.3.11.	8.1	More Details
CVE-2025-52745	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Farm Agrico farmagrico allows PHP Local File Inclusion.This issue affects Farm Agrico: from n/a through <= 1.3.11.	8.1	More Details
CVE-2025-52768	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Faith & Hope faith-hope allows PHP Local File Inclusion.This issue affects Faith & Hope: from n/a through <= 2.13.0.	8.1	More Details
CVE-2025-53429	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Exit Game exit-game allows PHP Local File Inclusion.This issue affects Exit Game: from n/a through <= 1.4.3.	8.1	More Details
CVE-2025-53430	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Etta etta allows PHP Local File Inclusion.This issue affects Etta: from n/a through <= 1.14.0.	8.1	More Details
CVE-2025-53431	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Emberlyn emberlyn allows PHP Local File Inclusion.This issue affects Emberlyn: from n/a through <= 1.3.1.	8.1	More Details
CVE-2025-53432	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Echo echo allows PHP Local File Inclusion.This issue affects Echo: from n/a through <= 1.15.0.	8.1	More Details
CVE-2025-53434	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes ChildHope childhope allows PHP Local File Inclusion.This issue affects ChildHope: from n/a through <= 1.1.8.	8.1	More Details
CVE-2025-53436	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in BZOTheme Monki monki allows PHP Local File Inclusion.This issue affects Monki: from n/a through <= 2.0.4.	8.1	More Details

CVE-2025-53437	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ApusTheme Greenorganic greenorganic allows PHP Local File Inclusion.This issue affects Greenorganic: from n/a through <= 2.45.	8.1	More Details
CVE-2025-53438	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes FitLine fitline allows PHP Local File Inclusion.This issue affects FitLine: from n/a through <= 1.6.	8.1	More Details
CVE-2025-53439	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Harper harper allows PHP Local File Inclusion.This issue affects Harper: from n/a through <= 1.13.	8.1	More Details
CVE-2025-53441	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Greeny greeny allows PHP Local File Inclusion.This issue affects Greeny: from n/a through <= 2.6.	8.1	More Details
CVE-2025-53442	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Rentic rentic allows PHP Local File Inclusion.This issue affects Rentic: from n/a through <= 1.1.	8.1	More Details
CVE-2025-53443	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Smash smash allows PHP Local File Inclusion.This issue affects Smash: from n/a through <= 1.7.	8.1	More Details
CVE-2025-53445	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Catwalk catwalk allows PHP Local File Inclusion.This issue affects Catwalk: from n/a through <= 1.4.	8.1	More Details
CVE-2025-53435	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Plan My Day planmyday allows PHP Local File Inclusion.This issue affects Plan My Day: from n/a through <= 1.1.13.	8.1	More Details
CVE-2025-58937	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Tacticool tacticool allows PHP Local File Inclusion.This issue affects Tacticool: from n/a through <= 1.0.13.	8.1	More Details
CVE-2025-58225	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Paragon paragon allows PHP Local File Inclusion.This issue affects Paragon: from n/a through <= 1.1.	8.1	More Details
CVE-2025-60046	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes HeartStar heartstar allows PHP Local File Inclusion.This issue affects HeartStar: from n/a through <= 1.0.14.	8.1	More Details
CVE-2025-60048	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Tripster tripster allows PHP Local File Inclusion.This issue affects Tripster: from n/a through <= 1.0.10.	8.1	More Details
CVE-2025-34438	AVideo versions prior to 20.1 contain an insecure direct object reference vulnerability allowing users with upload permissions to modify the rotation metadata of any video. The endpoint verifies upload capability but fails to enforce ownership or management rights for the targeted video.	8.1	More Details
CVE-2025-58706	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Woo Hoo woohoo allows PHP Local File Inclusion.This issue affects Woo Hoo: from n/a through <= 1.25.	8.1	More Details
CVE-2025-60057	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes DJ Rainflow dj-rainflow allows PHP Local File Inclusion.This issue affects DJ Rainflow: from n/a through <= 1.3.13.	8.1	More Details
CVE-2025-60058	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes DetailX detailx allows PHP Local File Inclusion.This issue affects DetailX: from n/a through <= 1.10.0.	8.1	More Details
CVE-2025-60059	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes smart SEO smartSEO allows PHP Local File Inclusion.This issue affects smart SEO: from n/a through <= 2.12.	8.1	More Details
CVE-2025-60060	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Pubzinne pubzinne allows PHP Local File Inclusion.This issue affects Pubzinne: from n/a through <= 1.0.12.	8.1	More Details
CVE-2025-60061	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Kicker kicker allows PHP Local File Inclusion.This issue affects Kicker: from n/a through <= 2.2.0.	8.1	More Details
CVE-2025-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Renewal renewal allows PHP Local File Inclusion.This issue affects Renewal: from n/a through <= 1.2.2.	8.1	More Details

60064			
CVE-2025-60065	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Pinevale pinevale allows PHP Local File Inclusion.This issue affects Pinevale: from n/a through <= 1.0.14.	8.1	More Details
CVE-2025-60066	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Katelyn katelyn allows PHP Local File Inclusion.This issue affects Katelyn: from n/a through <= 1.0.10.	8.1	More Details
CVE-2025-60067	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Giardino giardino allows PHP Local File Inclusion.This issue affects Giardino: from n/a through <= 1.1.10.	8.1	More Details
CVE-2025-60069	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove MinimogWP minimog allows PHP Local File Inclusion.This issue affects MinimogWP: from n/a through <= 3.9.6.	8.1	More Details
CVE-2025-60071	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in don-themes Riode | Multi-Purpose WooCommerce riode allows PHP Local File Inclusion.This issue affects Riode | Multi-Purpose WooCommerce: from n/a through <= 1.6.23.	8.1	More Details
CVE-2025-12934	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on the 'duplicate_wpml_layout' function in all versions up to, and including, 2.9.4.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary posts with the content of other existing posts, potentially exposing private and password-protected content and deleting any content that is not saved in revisions or backups. Posts must have been created with Beaver Builder to be copied or updated.	8.1	More Details
CVE-2025-64223	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in PenciDesign PenNews pennews allows PHP Local File Inclusion.This issue affects PenNews: from n/a through < 6.7.3.	8.1	More Details
CVE-2025-64373	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in shinetheme Traveler traveler allows PHP Local File Inclusion.This issue affects Traveler: from n/a through < 3.2.6.	8.1	More Details
CVE-2025-64377	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CridioStudio ListingPro listingpro allows PHP Local File Inclusion.This issue affects ListingPro: from n/a through < 2.9.10.	8.1	More Details
CVE-2025-40898	A path traversal vulnerability was discovered in the Import Arc data archive functionality due to insufficient validation of the input file. An authenticated user with limited privileges, by uploading a specifically-crafted Arc data archive, can potentially write arbitrary files in arbitrary paths, altering the device configuration and/or affecting its availability.	8.1	More Details
CVE-2025-60047	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes IPharm ipharm allows PHP Local File Inclusion.This issue affects IPharm: from n/a through <= 1.2.3.	8.1	More Details
CVE-2025-60056	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Winger winger allows PHP Local File Inclusion.This issue affects Winger: from n/a through <= 1.0.16.	8.1	More Details
CVE-2025-60044	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Fribbo fribbo allows PHP Local File Inclusion.This issue affects Fribbo: from n/a through <= 1.1.0.	8.1	More Details
CVE-2025-58927	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Stallion stallion allows PHP Local File Inclusion.This issue affects Stallion: from n/a through <= 1.17.	8.1	More Details
CVE-2025-58708	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes 777 triple-seven allows PHP Local File Inclusion.This issue affects 777: from n/a through <= 1.3.	8.1	More Details
CVE-2025-58709	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Legacy legacy allows PHP Local File Inclusion.This issue affects Legacy: from n/a through <= 1.9.	8.1	More Details
CVE-2025-58899	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Frame frame allows PHP Local File Inclusion.This issue affects Frame: from n/a through <= 2.4.0.	8.1	More Details
CVE-2025-58900	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes UniTravel unitravel allows PHP Local File Inclusion.This issue affects UniTravel: from n/a through <= 1.4.2.	8.1	More Details
CVE-2025-	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Wanderic wanderic allows PHP Local File Inclusion.This issue affects Wanderic: from n/a through <=	8.1	More

60043	1.0.10.		Details
CVE-2025-58923	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Critique critique allows PHP Local File Inclusion.This issue affects Critique: from n/a through <= 1.17.	8.1	More Details
CVE-2025-58925	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Neptunus neptunus allows PHP Local File Inclusion.This issue affects Neptunus: from n/a through <= 1.0.11.	8.1	More Details
CVE-2025-58926	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Cerebrum cerebrum allows PHP Local File Inclusion.This issue affects Cerebrum: from n/a through <= 1.12.	8.1	More Details
CVE-2025-58901	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Takeout takeout allows PHP Local File Inclusion.This issue affects Takeout: from n/a through <= 1.3.0.	8.1	More Details
CVE-2025-58928	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Heart heart allows PHP Local File Inclusion.This issue affects Heart: from n/a through <= 1.8.	8.1	More Details
CVE-2025-58948	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Aromatica aromatica allows PHP Local File Inclusion.This issue affects Aromatica: from n/a through <= 1.8.	8.1	More Details
CVE-2025-60042	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Chinchilla chinchilla allows PHP Local File Inclusion.This issue affects Chinchilla: from n/a through <= 1.16.	8.1	More Details
CVE-2025-58950	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Lione lione allows PHP Local File Inclusion.This issue affects Lione: from n/a through <= 1.16.	8.1	More Details
CVE-2025-58949	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Spock spock allows PHP Local File Inclusion.This issue affects Spock: from n/a through <= 1.17.	8.1	More Details
CVE-2025-58933	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Anubis anubis allows PHP Local File Inclusion.This issue affects Anubis: from n/a through <= 1.25.	8.1	More Details
CVE-2025-49371	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AncoraThemes Strux strux allows PHP Local File Inclusion.This issue affects Strux: from n/a through <= 1.9.	8.1	More Details
CVE-2025-14800	The Redirection for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'move_file_to_upload' function in all versions up to, and including, 3.2.7. This makes it possible for unauthenticated attackers to copy arbitrary files on the affected site's server. If 'allow_url_fopen' is set to 'On', it is possible to upload a remote file to the server.	8.1	More Details
CVE-2025-58936	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Catamaran catamaran allows PHP Local File Inclusion.This issue affects Catamaran: from n/a through <= 1.15.	8.1	More Details
CVE-2025-58934	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes The Gig thegig allows PHP Local File Inclusion.This issue affects The Gig: from n/a through <= 1.18.0.	8.1	More Details
CVE-2025-64467	There is an out of bounds read vulnerability in NI LabVIEW in LVResFile::FindRsrcListEntry() when parsing a corrupted VI file. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q3 (25.3) and prior versions.	7.8	More Details
CVE-2025-64468	There is a use-after-free vulnerability in sentry!sentry_span_set_data() when parsing a corrupted VI file. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q3 (25.3) and prior versions	7.8	More Details
CVE-2025-64469	There is a stack-based buffer overflow vulnerability in NI LabVIEW in LVResFile::FindRsrcListEntry() when parsing a corrupted VI file. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q3 (25.3) and prior versions.	7.8	More Details
CVE-2025-64465	There is an out of bounds read vulnerability in NI LabVIEW in lvre!DataSizeTDR() when parsing a corrupted VI file. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q3 (25.3) and prior versions.	7.8	More Details

CVE-2025-64464	There is an out of bounds read vulnerability in NI LabVIEW in lvre!VisaWriteFromFile() when parsing a corrupted VI file. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q3 (25.3) and prior versions.	7.8	More Details
CVE-2025-64463	There is an out of bounds read vulnerability in NI LabVIEW in LVResource::DetachResource() when parsing a corrupted VI file. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q3 (25.3) and prior versions.	7.8	More Details
CVE-2025-64462	There is an out of bounds read vulnerability in NI LabVIEW in LVResFile::RGetMemFileHandle() when parsing a corrupted VI file. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q3 (25.3) and prior versions.	7.8	More Details
CVE-2025-64461	There is an out of bounds write vulnerability in NI LabVIEW in mgocre_SH_25_3!RevBL() when parsing a corrupted VI file. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q3 (25.3) and prior versions.	7.8	More Details
CVE-2025-64466	There is an out of bounds read vulnerability in NI LabVIEW in lvre!ExecPostedProcRecPost() when parsing a corrupted VI file. This vulnerability may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2025 Q3 (25.3) and prior versions.	7.8	More Details
CVE-2023-53937	Hubstaff 1.6.14 contains a DLL search order hijacking vulnerability that allows attackers to replace a missing system32 wow64log.dll with a malicious library. Attackers can generate a custom DLL using Metasploit and place it in the system32 directory to obtain a reverse shell during application startup.	7.8	More Details
CVE-2025-53524	Fuji Electric Monitouch V-SFT-6 is vulnerable to an out-of-bounds write while processing a specially crafted project file, which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2025-46291	A logic issue was addressed with improved validation. This issue is fixed in macOS Tahoe 26.2. An app may bypass Gatekeeper checks.	7.8	More Details
CVE-2025-66494	A use-after-free vulnerability exists in the PDF file parsing of Foxit PDF Reader before 2025.2.1, 14.0.1, and 13.2.1 on Windows. A PDF object managed by multiple parent objects could be freed while still being referenced, potentially allowing a remote attacker to execute arbitrary code.	7.8	More Details
CVE-2025-66495	A use-after-free vulnerability exists in the annotation handling of Foxit PDF Reader before 2025.2.1, 14.0.1, and 13.2.1 on Windows and MacOS. When opening a PDF containing specially crafted JavaScript, a pointer to memory that has already been freed may be accessed or dereferenced, potentially allowing a remote attacker to execute arbitrary code.	7.8	More Details
CVE-2025-66499	A heap-based buffer overflow vulnerability exists in the PDF parsing of Foxit PDF Reader when processing specially crafted JBIG2 data. An integer overflow in the calculation of the image buffer size may occur, potentially allowing a remote attacker to execute arbitrary code.	7.8	More Details
CVE-2025-67792	An issue was discovered in DriveLock 24.1 before 24.1.6, 24.2 before 24.2.7, and 25.1 before 25.1.5. Local unprivileged users can manipulate a DriveLock process to execute arbitrary commands on Windows computers.	7.8	More Details
CVE-2025-27063	Memory corruption during video playback when video session open fails with time out error.	7.8	More Details
CVE-2025-47320	Memory corruption while processing MFC channel configuration during music playback.	7.8	More Details
CVE-2025-47321	Memory corruption while copying packets received from unix clients.	7.8	More Details
CVE-2025-47322	Memory corruption while handling IOCTL calls to set mode.	7.8	More Details
CVE-2025-47323	Memory corruption while routing GPR packets between user and root when handling large data packet.	7.8	More Details
CVE-2025-47350	Memory corruption while handling concurrent memory mapping and unmapping requests from a user-space application.	7.8	More Details
CVE-			More

2025- 47382	Memory corruption while loading an invalid firmware in boot loader.	7.8	Details
CVE- 2025- 47387	Memory Corruption when processing IOCTLs for JPEG data without verification.	7.8	More Details
CVE- 2024- 46062	Miniconda3 macOS installers before 23.11.0-1 contain a local privilege escalation vulnerability when installed outside the user's home directory. During installation, world-writable files are created and executed with root privileges. This flaw allows a local low-privileged user to inject arbitrary commands, leading to code execution as the root user.	7.8	More Details
CVE- 2024- 46060	Anaconda3 macOS installers before 2024.06-1 contain a local privilege escalation vulnerability when installed outside the user's home directory. During installation, world-writable files are created and executed with root privileges. This allows a local low-privileged user to inject arbitrary commands, leading to code execution as the root user.	7.8	More Details
CVE- 2025- 53919	An issue was discovered in the Portrait Dell Color Management application through 3.3.008 for Dell monitors, It creates a temporary folder, with weak permissions, during installation and uninstallation. A low-privileged attacker with local access could potentially exploit this, leading to elevation of privileges.	7.8	More Details
CVE- 2023- 53940	Codigo Markdown Editor 1.0.1 contains a code execution vulnerability that allows attackers to run arbitrary system commands by crafting a malicious markdown file. Attackers can embed a video source with an onerror event that executes shell commands through Node.js child_process module when the file is opened.	7.8	More Details
CVE- 2025- 53398	The Portrait Dell Color Management application 3.3.8 for Dell monitors has Insecure Permissions,	7.8	More Details
CVE- 2025- 14305	ListCheck.exe developed by Acer has a Local Privilege Escalation vulnerability. Authenticated local attackers can replace ListCheck.exe with a malicious executable of the same name, which will be executed by the system and result in privilege escalation.	7.8	More Details
CVE- 2025- 66493	A use-after-free vulnerability exists in the AcroForm handling of Foxit PDF Reader and Foxit PDF Editor before 2025.2.1,14.0.1 and 13.2.1 on Windows . When opening a PDF containing specially crafted JavaScript, a pointer to memory that has already been freed may be accessed or dereferenced, potentially allowing a remote attacker to execute arbitrary code.	7.8	More Details
CVE- 2025- 68432	Zed, a code editor, has an aribtrary code execution vulnerability in versions prior to 0.218.2-pre. The Zed IDE loads Language Server Protocol (LSP) configurations from the `settings.json` file located within a project’s `.zed` subdirectory. A malicious LSP configuration can contain arbitrary shell commands that run on the host system with the privileges of the user running the IDE. This can be triggered when a user opens project file for which there is an LSP entry. A concerted effort by an attacker to seed a project settings file (`./zed/settings.json`) with malicious language server configurations could result in arbitrary code execution with the user's privileges if the user opens the project in Zed without reviewing the contents. Version 0.218.2-pre fixes the issue by implementing worktree trust mechanism. As a workaround, users should carefully review the contents of project settings files (`./zed/settings.json`) before opening new projects in Zed.	7.7	More Details
CVE- 2023- 25446	Missing Authorization vulnerability in HappyFiles HappyFiles Pro happyfiles-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects HappyFiles Pro: from n/a through 1.8.1.	7.7	More Details
CVE- 2025- 68477	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to version 1.7.0, Langflow provides an API Request component that can issue arbitrary HTTP requests within a flow. This component takes a user-supplied URL, performs only normalization and basic format checks, and then sends the request using a server-side httpx client. It does not block private IP ranges (127[.]0[.]0[.]1, the 10/172/192 ranges) or cloud metadata endpoints (169[.]254[.]169[.]254), and it returns the response body as the result. Because the flow execution endpoints (/api/v1/run, /api/v1/run/advanced) can be invoked with just an API key, if an attacker can control the API Request URL in a flow, non-blind SSRF is possible—accessing internal resources from the server’s network context. This enables requests to, and collection of responses from, internal administrative endpoints, metadata services, and internal databases/services, leading to information disclosure and providing a foothold for further attacks. Version 1.7.0 contains a patch for this issue.	7.7	More Details
CVE- 2025- 67826	An issue was discovered in K7 Ultimate Security 17.0.2045. A Local Privilege Escalation (LPE) vulnerability in the K7 Ultimate Security antivirus can be exploited by a local unprivileged user on default installations of the product. Insecure access to a named pipe allows unprivileged users to edit any registry key, leading to a full compromise as SYSTEM.	7.7	More Details
CVE- 2025- 68433	Zed, a code editor, has an aribtrary code execution vulnerability in versions prior to 0.218.2-pre. The Zed IDE loads Model Context Protocol (MCP) configurations from the `settings.json` file located within a project’s `.zed` subdirectory. A malicious MCP configuration can contain arbitrary shell commands that run on the host system with the privileges of the user running the IDE. This can be triggered automatically without any user interaction besides opening the project in the IDE. Version 0.218.2-pre fixes the issue by implementing worktree trust mechanism. As a workaround, users should carefully review the contents of project settings files (`./zed/settings.json`) before opening new projects in Zed.	7.7	More Details
CVE- 2025- 68279	Weblate is a web based localization tool. In versions prior to 5.15.1, it was possible to read arbitrary files from the server file system using crafted symbolic links in the repository. Version 5.15.1 fixes the issue.	7.7	More Details
	Open OnDemand provides remote web access to supercomputers. In versions 4.0.8 and prior, the Apache proxy allows sensitive headers to be passed to origin servers. This means malicious users can create an origin server on a compute		

CVE-2025-66029	node that record these headers when unsuspecting users connect to it. Maintainers anticipate a patch in a 4.1 release. Workarounds exist for 4.0.x versions. Using `custom_location_directives` in `ood_portal.yml` in version 4.0.x (not available for versions below 4.0) centers can unset and or edit these headers. Note that `OIDCPassClaimsAs both` is the default and centers can set `OIDCPassClaimsAs` to `none` or `environment` to stop passing these headers to the client. Centers that have an OIDC provider with the `OIDCPassClaimsAs` with `none` or `environment` settings can adjust the settings using guidance provided in GHSA-2cwp-8g29-9q32 to unset the mod_auth_openidc_session cookies.	7.6	More Details
CVE-2025-7782	The WP JobHunt plugin for WordPress, used by the JobCareer theme, is vulnerable to unauthorized modification of data due to a missing capability check on the 'cs_update_application_status_callback' function in all versions up to, and including, 7.7. This makes it possible for authenticated attackers, with Candidate-level access and above, to inject cross-site scripting into the 'status' parameter of applied jobs for any user.	7.6	More Details
CVE-2025-68561	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ruben Garcia AutomatorWP allows SQL Injection.This issue affects AutomatorWP: from n/a through 5.2.4.	7.6	More Details
CVE-2025-67442	EVE-NG 6.4.0-13-PRO is vulnerable to Directory Traversal. The /api/export interface allows authenticated users to export lab files. This interface lacks effective input validation and filtering when processing file path parameters submitted by users.	7.6	More Details
CVE-2025-68550	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VillaTheme WPBulky allows Blind SQL Injection.This issue affects WPBulky: from n/a through 1.1.13.	7.6	More Details
CVE-2025-58938	Missing Authorization vulnerability in ThemeAtelier IDonatePro idonate-pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects IDonatePro: from n/a through <= 2.1.9.	7.6	More Details
CVE-2023-53962	SOUND4 IMPACT/FIRST/PULSE/Eco v2.x contains an unauthenticated directory traversal vulnerability that allows remote attackers to write arbitrary files through the 'upgfile' parameter in upload.cgi. Attackers can exploit the vulnerability by sending crafted multipart form-data POST requests with directory traversal sequences to write files to unintended system locations.	7.5	More Details
CVE-2024-29371	In jose4j before 0.9.5, an attacker can cause a Denial-of-Service (DoS) condition by crafting a malicious JSON Web Encryption (JWE) token with an exceptionally high compression ratio. When this token is processed by the server, it results in significant memory allocation and processing time during decompression.	7.5	More Details
CVE-2025-65857	An issue was discovered in Xiongmai XM530 IP cameras on firmware V5.00.R02.000807D8.10010.346624.S.ONVIF 21.06. The GetStreamUri exposes RTSP URIs containing hardcoded credentials enabling direct unauthorized video stream access.	7.5	More Details
CVE-2025-68475	Fedify is a TypeScript library for building federated server apps powered by ActivityPub. Prior to versions 1.6.13, 1.7.14, 1.8.15, and 1.9.2, a Regular Expression Denial of Service (ReDoS) vulnerability exists in Fedify's document loader. The HTML parsing regex at packages/fedify/src/runtime/docloader.ts:259 contains nested quantifiers that cause catastrophic backtracking when processing maliciously crafted HTML responses. This issue has been patched in versions 1.6.13, 1.7.14, 1.8.15, and 1.9.2.	7.5	More Details
CVE-2025-60086	Missing Authorization vulnerability in Matt WP Voting Contest wp-voting-contest allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Voting Contest: from n/a through <= 5.8.	7.5	More Details
CVE-2025-65561	An issue was discovered in function LocalNode.Sess in free5GC 4.1.0 allowing attackers to cause a denial of service or other unspecified impacts via crafted header Local SEID to the PFCP Session Modification Request.	7.5	More Details
CVE-2025-65559	An issue was discovered in Open5GS 2.7.5-49-g465e90f, when processing a PFCP Session Establishment Request (type=50), the UPF crashes with a reachable assertion in `lib/pfcp/context.c` (`ogs_pfcp_object_teid_hash_set`) if the CreatePDR?PDI?F-TEID has CH=1 and the F-TEID address-family flag(s) (IPv4/IPv6) do not match the GTP-U resource family configured for the selected DNN (Network Instance), resulting in a denial of service.	7.5	More Details
CVE-2025-63387	Dify v1.9.1 is vulnerable to Insecure Permissions. An unauthenticated attacker can directly send HTTP GET requests to the /console/api/system-features endpoint without any authentication credentials or session tokens. The endpoint fails to implement proper authorization checks, allowing anonymous access to sensitive system configuration data.	7.5	More Details
CVE-2025-14896	due to insufficient sanitazation in Vega's `convert()` function when `safeMode` is enabled and the spec variable is an array. An attacker can craft a malicious Vega diagram specification that will allow them to send requests to any URL, including local file system paths, leading to exposure of sensitive information.	7.5	More Details
CVE-2025-63391	An authentication bypass vulnerability exists in Open-WebUI <=0.6.32 in the /api/config endpoint. The endpoint lacks proper authentication and authorization controls, exposing sensitive system configuration data to unauthenticated remote attackers.	7.5	More Details
CVE-2025-64193	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in 8theme XStore xstore allows PHP Local File Inclusion.This issue affects XStore: from n/a through < 9.6.1.	7.5	More Details
CVE-2025-	Deserialization of Untrusted Data vulnerability in add-ons.org PDF for Gravity Forms + Drag And Drop Template Builder pdf-for-gravity-forms allows Object Injection.This issue affects PDF for Gravity Forms + Drag And Drop Template Builder:	7.5	More

60080	from n/a through <= 6.3.0.		Details
CVE-2025-60077	Missing Authorization vulnerability in YayCommerce YayPricing yaypricing allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects YayPricing: from n/a through <= 3.5.3.	7.5	More Details
CVE-2025-60078	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Agence web Eoxia - Montpellier Task Manager task-manager allows PHP Local File Inclusion.This issue affects Task Manager: from n/a through <= 3.0.2.	7.5	More Details
CVE-2025-64209	Missing Authorization vulnerability in StylemixThemes Masterstudy masterstudy allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Masterstudy: from n/a through < 4.8.122.	7.5	More Details
CVE-2025-60076	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in jbhovik Ray Enterprise Translation lingotek-translation allows PHP Local File Inclusion.This issue affects Ray Enterprise Translation: from n/a through <= 1.7.1.	7.5	More Details
CVE-2025-65566	A denial-of-service vulnerability exists in the omec-project UPF (pfcpiface component) in version upf-epc-pfcpiface:2.1.3-dev. When the UPF receives a PFCP Session Report Response that is missing the mandatory Cause Information Element, the session report handler dereferences a nil pointer instead of rejecting the malformed message. This triggers a panic and terminates the UPF process. An attacker who can send PFCP Session Report Response messages to the UPF's N4/PFCP endpoint can exploit this flaw to repeatedly crash the UPF and disrupt user-plane services.	7.5	More Details
CVE-2023-53974	D-Link DSL-124 ME_1.00 contains a configuration file disclosure vulnerability that allows unauthenticated attackers to retrieve router settings through a POST request. Attackers can send a specific POST request to the router's configuration endpoint to download a complete backup file containing sensitive network credentials and system configurations.	7.5	More Details
CVE-2025-65562	The free5GC UPF suffers from a lack of bounds checking on the SEID when processing PFCP Session Deletion Requests. An unauthenticated remote attacker can send a request with a very large SEID (e.g., 0xFFFFFFFFFFFFFFFF) that causes an integer conversion/underflow in LocalNode.DeleteSess() / LocalNode.Sess() when a uint64 SEID is converted to int and used in index arithmetic. This leads to a negative index into n.sess and a Go runtime panic, resulting in a denial of service (UPF crash). The issue has been reproduced on free5GC v4.1.0 with crashes observed in the session lookup/deletion path in internal/pfcp/node.go; other versions may also be affected. No authentication is required.	7.5	More Details
CVE-2025-65563	A denial-of-service vulnerability exists in the omec-project UPF (component upf-epc/pfcpiface) up to at least version upf-epc-pfcpiface:2.1.3-dev. When the UPF receives a PFCP Association Setup Request that is missing the mandatory NodeID Information Element, the association setup handler dereferences a nil pointer instead of validating the message, causing a panic and terminating the UPF process. An attacker who can send PFCP Association Setup Request messages to the UPF's N4/PFCP endpoint can exploit this issue to repeatedly crash the UPF and disrupt user-plane services.	7.5	More Details
CVE-2025-53710	Due to a product misconfiguration in certain deployment types, it was possible from different pods in the same namespace to communicate with each other. This issue resulted in bypass of access control due to the presence of a vulnerable endpoint in Foundry Container Service that executed user-controlled commands locally.	7.5	More Details
CVE-2023-53970	Screen SFT DAB 600/C Firmware 1.9.3 contains a weak session management vulnerability that allows attackers to bypass authentication controls by reusing IP-bound session identifiers. Attackers can exploit the vulnerable deviceManagement API endpoint to reset device configurations by sending crafted POST requests with manipulated session parameters.	7.5	More Details
CVE-2023-53969	Screen SFT DAB 600/C firmware 1.9.3 contains a session management vulnerability that allows attackers to bypass authentication controls by exploiting IP address session binding. Attackers can reuse the same IP address and issue unauthorized requests to the userManager API to change user passwords without proper authentication.	7.5	More Details
CVE-2023-53967	Screen SFT DAB 600/C firmware 1.9.3 contains an authentication bypass vulnerability that allows attackers to change the admin password without requiring the current credentials. Attackers can exploit the userManager.cgx API endpoint by sending a crafted POST request with a new MD5-hashed password to directly modify the admin account's authentication.	7.5	More Details
CVE-2023-53964	SOUND4 IMPACT/FIRST/PULSE/Eco v2.x contains an unauthenticated vulnerability in the /usr/cgi-bin/restorefactory.cgi endpoint that allows remote attackers to reset device configuration. Attackers can send a POST request to the endpoint with specific data to trigger a factory reset and bypass authentication, gaining full system control.	7.5	More Details
CVE-2021-47713	Hasura GraphQL 1.3.3 contains a denial of service vulnerability that allows attackers to overwhelm the service by crafting malicious GraphQL queries with excessive nested fields. Attackers can send repeated requests with extremely long query strings and multiple threads to consume server resources and potentially crash the GraphQL endpoint.	7.5	More Details
CVE-2025-67171	Incorrect access control in the /templates/ component of RiteCMS v3.1.0 allows attackers to access sensitive files via directory traversal.	7.5	More Details
CVE-2025-67174	A local file inclusion (LFI) vulnerability in RiteCMS v3.1.0 allows attackers to read arbitrary files on the host via a directory traversal in the admin_language_file and default_page_language_file in the admin.php component	7.5	More Details

CVE-2025-7358	Use of Hard-coded Credentials vulnerability in Utarit Informatics Services Inc. SoliClub allows Authentication Abuse.This issue affects SoliClub: before 5.3.7.	7.5	More Details
CVE-2024-24844	Missing Authorization vulnerability in IdeaBox Creations PowerPack Pro for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PowerPack Pro for Elementor: from n/a through 2.10.6.	7.5	More Details
CVE-2025-64213	Insertion of Sensitive Information Into Sent Data vulnerability in StylemixThemes MasterStudy LMS Pro masterstudy-lms-learning-management-system-pro allows Retrieve Embedded Sensitive Data.This issue affects MasterStudy LMS Pro: from n/a through < 4.7.16.	7.5	More Details
CVE-2025-64214	Missing Authorization vulnerability in StylemixThemes MasterStudy LMS Pro masterstudy-lms-learning-management-system-pro allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects MasterStudy LMS Pro: from n/a through < 4.7.16.	7.5	More Details
CVE-2025-14437	The Hummingbird Performance plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.18.0 via the 'request' function. This makes it possible for unauthenticated attackers to extract sensitive data including Cloudflare API credentials.	7.5	More Details
CVE-2025-11419	A flaw was found in Keycloak. This vulnerability allows an unauthenticated remote attacker to cause a denial of service (DoS) by repeatedly initiating TLS 1.2 client-initiated renegotiation requests to exhaust server CPU resources, making the service unavailable.	7.5	More Details
CVE-2025-66117	Missing Authorization vulnerability in Ays Pro Easy Form easy-form allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Easy Form: from n/a through <= 2.7.8.	7.5	More Details
CVE-2025-66116	Insertion of Sensitive Information Into Sent Data vulnerability in UserElements Ultimate Member Widgets for Elementor ultimate-member-widgets-for-elementor allows Retrieve Embedded Sensitive Data.This issue affects Ultimate Member Widgets for Elementor: from n/a through <= 2.3.	7.5	More Details
CVE-2025-66102	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FolioVision FV Antispam fv-antispam allows Reflected XSS.This issue affects FV Antispam: from n/a through <= 2.7.	7.5	More Details
CVE-2025-1029	Use of Hard-coded Credentials vulnerability in Utarit Information Services Inc. SoliClub allows Read Sensitive Constants Within an Executable.This issue affects SoliClub: from 5.2.4 before 5.3.7.	7.5	More Details
CVE-2025-66088	Missing Authorization vulnerability in Property Hive PropertyHive propertyhive allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PropertyHive: from n/a through <= 2.1.12.	7.5	More Details
CVE-2025-66070	Missing Authorization vulnerability in Tomdever wpForo Forum wpforo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects wpForo Forum: from n/a through <= 2.4.10.	7.5	More Details
CVE-2025-1030	Exposure of Private Personal Information to an Unauthorized Actor vulnerability in Utarit Informatics Services Inc. SoliClub allows Query System for Information.This issue affects SoliClub: from 5.2.4 before 5.3.7.	7.5	More Details
CVE-2025-66054	Missing Authorization vulnerability in ThimPress LearnPress learnpress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects LearnPress: from n/a through <= 4.2.9.4.	7.5	More Details
CVE-2025-64378	Missing Authorization vulnerability in CridioStudio ListingPro listingpro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ListingPro: from n/a through < 2.9.10.	7.5	More Details
CVE-2025-1031	Authorization Bypass Through User-Controlled Key vulnerability in Utarit Informatics Services Inc. SoliClub allows Functionality Misuse.This issue affects SoliClub: from 5.2.4 before 5.3.7.	7.5	More Details
CVE-2025-63757	Integer overflow vulnerability in the yuv2ya16_X_c_template function in libswscale/output.c in FFmpeg 8.0.	7.5	More Details
CVE-2025-67111	An integer overflow in the RTPS protocol implementation of OpenDDS DDS before v3.33.0 allows attackers to cause a Denial of Service (DoS) via a crafted message.	7.5	More Details
CVE-2025-65865	An integer overflow in eProsima Fast-DDS v3.3 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
	The Ninja Forms – The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 3.13.2. This is due to the plugin not properly verifying that a user is		

CVE-2025-11924	authorized before the `ninja-forms-views` REST endpoints return form metadata and submission content. This makes it possible for unauthenticated attackers to read arbitrary form definitions and submission records via a leaked bearer token granted they can load any page containing the Submissions Table block. NOTE: The developer released a patch for this issue in 3.13.1, but inadvertently introduced a REST API endpoint in which a valid bearer token could be minted for arbitrary form IDs, making this patch ineffective.	7.5	More Details
CVE-2025-64273	Missing Authorization vulnerability in GetResponse Email marketing for WordPress by GetResponse Official getresponse-official allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Email marketing for WordPress by GetResponse Official: from n/a through <= 1.5.3.	7.5	More Details
CVE-2024-9684	FreyrSCADA/IEC-60870-5-104 server v21.06.008 allows remote attackers to cause a denial of service by sending specific message sequences.	7.5	More Details
CVE-2025-64268	Missing Authorization vulnerability in Arraytics Timetics timetics allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Timetics: from n/a through <= 1.0.44.	7.5	More Details
CVE-2025-68560	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in CodexThemes TheGem Theme Elements (for Elementor).This issue affects TheGem Theme Elements (for Elementor): from n/a through 5.10.5.1.	7.5	More Details
CVE-2025-64258	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in wpweb Follow My Blog Post follow-my-blog-post allows Retrieve Embedded Sensitive Data.This issue affects Follow My Blog Post: from n/a through <= 2.3.9.	7.5	More Details
CVE-2025-64230	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WP Chill Filr filr-protection allows Path Traversal.This issue affects Filr: from n/a through <= 1.2.10.	7.5	More Details
CVE-2025-68546	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Thembay Nika allows PHP Local File Inclusion.This issue affects Nika: from n/a through 1.2.14.	7.5	More Details
CVE-2025-64222	Missing Authorization vulnerability in FantasticPlugins WooCommerce Recover Abandoned Cart rac allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WooCommerce Recover Abandoned Cart: from n/a through <= 24.6.0.	7.5	More Details
CVE-2025-68544	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Thembay Diza allows PHP Local File Inclusion.This issue affects Diza: from n/a through 1.3.15.	7.5	More Details
CVE-2025-64218	Insertion of Sensitive Information Into Sent Data vulnerability in WP Chill Passster content-protector allows Retrieve Embedded Sensitive Data.This issue affects Passster: from n/a through <= 4.2.19.	7.5	More Details
CVE-2025-63664	Incorrect access control in the /api/v1/conversations/*/messages API of GT Edge AI Platform before v2.0.10-dev allows unauthorized attackers to access other users' message history with AI agents.	7.5	More Details
CVE-2025-66735	youlai-boot V2.21.1 is vulnerable to Incorrect Access Control. The getRoleForm function in SysRoleController.java does not perform permission checks, which may allow non-root users to directly access root roles.	7.5	More Details
CVE-2023-53934	A denial of service vulnerability in Kentico Xperience allows attackers to launch DoS attacks via specially crafted requests to the GetResource handler. Improper input validation enables remote attackers to potentially disrupt service availability through maliciously constructed requests.	7.5	More Details
CVE-2025-63663	Incorrect access control in the /api/v1/conversations/*/files API of GT Edge AI Platform before v2.0.10 allows unauthorized attackers to access other users' uploaded files.	7.5	More Details
CVE-2025-58877	Missing Authorization vulnerability in javothemes Javo Core javo-core allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Javo Core: from n/a through <= 3.0.0.529.	7.5	More Details
CVE-2025-67790	An issue was discovered in DriveLock 24.1 before 24.1.6, 24.2 before 24.2.7, and 25.1 before 25.1.5. An unprivileged user could cause occasionally a Blue Screen Of Death (BSOD) on Windows computers by using an IOCTL and an unterminated string.	7.5	More Details
CVE-2025-67493	Homarr is an open-source dashboard. Prior to version 1.45.3, it was possible to craft an input which allowed privilege escalation and getting access to groups of other users due to missing sanitization of inputs in ldap search query. The vulnerability could impact all instances using ldap authentication where a malicious actor had access to a user account. Version 1.45.3 has a patch for the issue.	7.5	More Details
CVE-2023-53958	LDAP Tool Box Self Service Password 1.5.2 contains a password reset vulnerability that allows attackers to manipulate HTTP Host headers during token generation. Attackers can craft malicious password reset requests that generate tokens sent to a controlled server, enabling potential account takeover by intercepting and using stolen reset tokens.	7.5	More Details

CVE-2025-65564	A denial-of-service vulnerability exists in the omec-upf (upf-epc-pfcpiface) in version upf-epc-pfcpiface:2.1.3-dev. When the UPF receives a PFCP Association Setup Request that is missing the mandatory Recovery Time Stamp Information Element, the association setup handler dereferences a nil pointer via IE.RecoveryTimeStamp() instead of validating the message. This results in a panic and terminates the UPF process. An attacker who can send PFCP Association Setup Request messages to the UPF's N4/PFCP endpoint can exploit this issue to repeatedly crash the UPF and disrupt user-plane services.	7.5	More Details
CVE-2025-63950	An insecure deserialization vulnerability exists in the download.php script of the to3k Twittodon application through commit b1c58a7d1dc664b38deb486ca290779621342c0b (2023-02-28). The 'obj' parameter receives base64-encoded data that is passed directly to the unserialize() function without validation. This allows a remote, unauthenticated attacker to inject arbitrary PHP objects, leading to a denial of service.	7.5	More Details
CVE-2025-12980	The Post Grid Gutenberg Blocks for News, Magazines, Blog Websites – PostX plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the '/ultp/v2/get_dynamic_content/' REST API endpoint in all versions up to, and including, 5.0.3. This makes it possible for unauthenticated attackers to retrieve sensitive user metadata, including password hashes.	7.5	More Details
CVE-2025-14071	The Live Composer – Free WordPress Website Builder plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.0.2 via deserialization of untrusted input in the dslc_module_posts_output shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable plugin, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	7.5	More Details
CVE-2025-14812	ArcSearch for iOS versions prior to 1.45.2 could display a different domain in the address bar than the content being shown after an iframe-triggered URI-scheme navigation, increasing spoofing risk.	7.5	More Details
CVE-2025-66905	The Takes web framework's TkFiles take thru 2.0-SNAPSHOT fails to canonicalize HTTP request paths before resolving them against the filesystem. A remote attacker can include ../ sequences in the request path to escape the configured base directory and read arbitrary files from the host system.	7.5	More Details
CVE-2025-66909	Turms AI-Serving module v0.10.0-SNAPSHOT and earlier contains an image decompression bomb denial of service vulnerability. The ExtendedOpenCVImage class in ai/djl/opencv/ExtendedOpenCVImage.java loads images using OpenCV's imread() function without validating dimensions or pixel count before decompression. An attacker can upload a specially crafted compressed image file (e.g., PNG) that is small when compressed but expands to gigabytes of memory when loaded. This causes immediate memory exhaustion, OutOfMemoryError, and service crash. No authentication is required if the OCR service is publicly accessible. Multiple requests can completely deny service availability.	7.5	More Details
CVE-2025-15015	Enterprise Cloud Database developed by Ragic has a Arbitrary File Read vulnerability, allowing unauthenticated remote attackers to exploit Relative Path Traversal to download arbitrary system files.	7.5	More Details
CVE-2025-14847	Mismatched length fields in Zlib compressed protocol headers may allow a read of uninitialized heap memory by an unauthenticated client. This issue affects all MongoDB Server v7.0 prior to 7.0.28 versions, MongoDB Server v8.0 versions prior to 8.0.17, MongoDB Server v8.2 versions prior to 8.2.3, MongoDB Server v6.0 versions prior to 6.0.27, MongoDB Server v5.0 versions prior to 5.0.32, MongoDB Server v4.4 versions prior to 4.4.30, MongoDB Server v4.2 versions greater than or equal to 4.2.0, MongoDB Server v4.0 versions greater than or equal to 4.0.0, and MongoDB Server v3.6 versions greater than or equal to 3.6.0.	7.5	More Details
CVE-2025-50681	igmpproxy 0.4 before commit 2b30c36 allows remote attackers to cause a denial of service (application crash) via a crafted IGMPv3 membership report packet with a malicious source address. Due to insufficient validation in the \`recv_igmp()\` function in src/igmpproxy.c, an invalid group record type can trigger a NULL pointer dereference when logging the address using \`inet_fmtsrc()\`. This vulnerability can be exploited by sending malformed multicast traffic to a host running igmpproxy, leading to a crash. igmpproxy is used in various embedded networking environments and consumer-grade IoT devices (such as home routers and media gateways) to handle multicast traffic for IPTV and other streaming services. Affected devices that rely on unpatched versions of igmpproxy may be vulnerable to remote denial-of-service attacks across a LAN .	7.5	More Details
CVE-2025-63951	An insecure deserialization vulnerability exists in the rss-mp3.php script of the MiczFlor RPi-Jukebox-RFID project through commit 4b2334f0ae0e87c0568876fc41c48c38aa9a7014 (2025-10-07). The 'rss' GET parameter receives data that is passed directly to the unserialize() function without validation. This allows a remote, unauthenticated attacker to inject arbitrary PHP objects, causing the application to process them and leading to errors or a denial of service.	7.5	More Details
CVE-2025-65567	A denial-of-service vulnerability exists in the omec-project UPF (pfcpiface component) in version upf-epc-pfcpiface:2.1.3-dev. After PFCP association, a specially crafted PFCP Session Establishment Request with a CreatePDR that contains a malformed Flow-Description is not robustly validated. The Flow-Description parser (parseFlowDesc) can read beyond the bounds of the provided buffer, causing a panic and terminating the UPF process. An attacker who can send PFCP Session Establishment Request messages to the UPF's N4/PFCP endpoint can exploit this issue to repeatedly crash the UPF.	7.5	More Details
CVE-2025-34441	AVideo versions prior to 20.1 expose sensitive user information through an unauthenticated public API endpoint. Responses include emails, usernames, administrative status, and last login times, enabling user enumeration and privacy violations.	7.5	More Details

CVE-2025-34442	AVideo versions prior to 20.1 disclose absolute filesystem paths via multiple public API endpoints. Returned metadata includes full server paths to media files, revealing underlying filesystem structure and facilitating more effective attack chains.	7.5	More Details
CVE-2025-60045	Missing Authorization vulnerability in ThemeAtelier IDonatePro idonate-pro allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects IDonatePro: from n/a through <= 2.1.11.	7.5	More Details
CVE-2025-65568	A denial-of-service vulnerability exists in the omec-project UPF (pfcpiface component) in version upf-epc-pfcpiface:2.1.3-dev. After PFCP association, a PFCP Session Establishment Request that includes a CreateFAR with an empty or truncated IPv4 address field is not properly validated. During parsing, parseFAR() calls ip2int(), which performs an out-of-bounds read on the IPv4 address buffer and triggers an index-out-of-range panic. An attacker who can send PFCP Session Establishment Request messages to the UPF's N4/PFCP endpoint can exploit this issue to repeatedly crash the UPF and disrupt user-plane services.	7.5	More Details
CVE-2021-47712	A cryptography vulnerability in Kentico Xperience allows attackers to potentially manipulate URL hash values through existing hashing mechanisms. The hotfix introduces an additional security layer to prevent hash value reuse and potential exploitation.	7.5	More Details
CVE-2025-63662	Insecure permissions in the /api/v1/agents API of GT Edge AI Platform before v2.0.10-dev allows unauthorized attackers to access sensitive information.	7.5	More Details
CVE-2025-65565	A denial-of-service vulnerability exists in the omec-project UPF (pfcpiface component) in version upf-epc-pfcpiface:2.1.3-dev. After PFCP association is established, a PFCP Session Establishment Request that is missing the mandatory F-SEID (CPF-SEID) Information Element is not properly validated. The session establishment handler calls IE.FSEID() on a nil pointer, which triggers a panic and terminates the UPF process. An attacker who can send PFCP Session Establishment Request messages to the UPF's N4/PFCP endpoint can exploit this issue to repeatedly crash the UPF and disrupt user-plane services.	7.5	More Details
CVE-2025-68644	Yealink RPS before 2025-06-27 allows unauthorized access to information, including AutoP URL addresses. This was fixed by deploying an enhanced authentication mechanism through a security update to all cloud instances.	7.4	More Details
CVE-2025-14809	ArcSearch for Android versions prior to 1.12.6 could display a different domain in the address bar than the content being shown, enabling address bar spoofing after user interaction via crafted web content.	7.4	More Details
CVE-2025-14960	A security vulnerability has been detected in code-projects Simple Blood Donor Management System 1.0. Impacted is an unknown function of the file /editeddonor.php. The manipulation of the argument Name leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-14968	A security flaw has been discovered in code-projects Simple Stock System 1.0. Affected by this issue is some unknown functionality of the file /market/update.php. The manipulation of the argument email results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-15049	A vulnerability was identified in code-projects Online Farm System 1.0. Affected is an unknown function of the file /addProduct.php. The manipulation of the argument Username leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-14951	A security vulnerability has been detected in code-projects Scholars Tracking System 1.0. The impacted element is an unknown function of the file /home.php. Such manipulation of the argument post_content leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2025-14967	A vulnerability was identified in itsourcecode Student Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /candidates_report.php. The manipulation of the argument school_year leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-14961	A vulnerability was detected in code-projects Simple Blood Donor Management System 1.0. The affected element is an unknown function of the file /editedcampaign.php. The manipulation of the argument campaignname results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-13183	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Hotech Software Inc. Otello allows Stored XSS.This issue affects Otello: from 2.4.0 before 2.4.4.	7.3	More Details
CVE-2025-14832	A vulnerability was identified in itsourcecode Online Cake Ordering System 1.0. The affected element is an unknown function of the file /updateproduct.php?action=edit. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-14959	A weakness has been identified in code-projects Simple Stock System 1.0. This issue affects some unknown processing of the file /market/signup.php. Executing manipulation of the argument Username can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-15048	A vulnerability was determined in Tenda WH450 1.0.0.18. This impacts an unknown function of the file /goform/CheckTools of the component HTTP Request Handler. Executing manipulation of the argument ipaddress can lead to command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details

CVE-2025-14952	A vulnerability was detected in Campcodes Supplier Management System 1.0. This affects an unknown function of the file /admin/add_category.php. Performing manipulation of the argument txtCategoryName results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-14950	A weakness has been identified in code-projects Scholars Tracking System 1.0. The affected element is an unknown function of the file /delete_post.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	7.3	More Details
CVE-2025-14940	A vulnerability was determined in code-projects Scholars Tracking System 1.0. The affected element is an unknown function of the file /admin/delete_user.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-14833	A security flaw has been discovered in code-projects Online Appointment Booking System 1.0. The impacted element is an unknown function of the file /admin/deletemanagerclinic.php. Performing manipulation of the argument clinic results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-68429	Storybook is a frontend workshop for building user interface components and pages in isolation. A vulnerability present starting in versions 7.0.0 and prior to versions 7.6.21, 8.6.15, 9.1.17, and 10.1.10 relates to Storybook’s handling of environment variables defined in a `.env` file, which could, in specific circumstances, lead to those variables being unexpectedly bundled into the artifacts created by the `storybook build` command. When a built Storybook is published to the web, the bundle’s source is viewable, thus potentially exposing those variables to anyone with access. For a project to potentially be vulnerable to this issue, it must build the Storybook (i.e. run `storybook build` directly or indirectly) in a directory that contains a `.env` file (including variants like `.env.local`) and publish the built Storybook to the web. Storybooks built without a `.env` file at build time are not affected, including common CI-based builds where secrets are provided via platform environment variables rather than `.env` files. Storybook runtime environments (i.e. `storybook dev`) are not affected. Deployed applications that share a repo with your Storybook are not affected. Users should upgrade their Storybook—on both their local machines and CI environment—to version .6.21, 8.6.15, 9.1.17, or 10.1.10 as soon as possible. Maintainers additionally recommend that users audit for any sensitive secrets provided via `.env` files and rotate those keys. Some projects may have been relying on the undocumented behavior at the heart of this issue and will need to change how they reference environment variables after this update. If a project can no longer read necessary environmental variable values, either prefix the variables with `STORYBOOK_` or use the `env` property in Storybook’s configuration to manually specify values. In either case, do not include sensitive secrets as they will be included in the built bundle.	7.3	More Details
CVE-2025-67285	A SQL injection vulnerability was found in the '/cts/admin/?page=zone' file of ITSourcecode COVID Tracking System Using QR-Code v1.0. The reason for this issue is that attackers inject malicious code from the parameter 'id' and use it directly in SQL queries without the need for appropriate cleaning or validation.	7.3	More Details
CVE-2025-15008	A vulnerability was detected in Tenda WH450 1.0.0.18. This affects an unknown part of the file /goform/L7Port of the component HTTP Request Handler. Performing manipulation of the argument page results in stack-based buffer overflow. The attack may be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2025-15034	A security flaw has been discovered in itsourcecode Student Management System 1.0. This affects an unknown part of the file /record.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-14877	A vulnerability was identified in Campcodes Supplier Management System 1.0. This affects an unknown function of the file /admin/add_retailer.php. The manipulation of the argument cmbAreaCode leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-14989	A vulnerability was identified in Campcodes Complete Online Beauty Parlor Management System 1.0. This issue affects some unknown processing of the file /admin/search-invoices.php. Such manipulation leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2025-14018	Unquoted Search Path or Element vulnerability in NetBT Consulting Services Inc. E-Fatura allows Leveraging/Manipulating Configuration File Search Paths, Redirect Access to Libraries.This issue affects e-Fatura: before 1.2.15.	7.3	More Details
CVE-2025-14990	A security flaw has been discovered in Campcodes Complete Online Beauty Parlor Management System 1.0. Impacted is an unknown function of the file /admin/view-appointment.php. Performing manipulation of the argument viewid results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	7.3	More Details
CVE-2025-15012	A vulnerability was determined in code-projects Refugee Food Management System 1.0. The affected element is an unknown function of the file /home/home.php. This manipulation of the argument a causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2025-15011	A vulnerability was found in code-projects Simple Stock System 1.0. Impacted is an unknown function of the file /logout.php. The manipulation of the argument uname results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2025-15002	A vulnerability has been found in SeaCMS up to 13.3. The affected element is an unknown function of the file js/player/dmplayer/dmku/class/mysqli.class.php. Such manipulation of the argument page/limit leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2025-64676	'.../...//' in Microsoft Purview allows an authorized attacker to execute code over a network.	7.2	More Details

CVE-2025-13999	The HTML5 Audio Player – The Ultimate No-Code Podcast, MP3 & Audio Player plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions from 2.4.0 up to, and including, 2.5.1 via the getIcyMetadata() function. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	7.2	More Details
CVE-2025-13307	The Ocean Modal Window WordPress plugin before 2.3.3 is vulnerable to Remote Code Execution via the modal display logic. These modals can be displayed under user-controlled conditions that Editors and Administrators can set (edit_pages capability). The conditions are then executed as part of an eval statement executed on every site page. This leads to remote code execution.	7.2	More Details
CVE-2025-67172	RiteCMS v3.1.0 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the parse_special_tags() function.	7.2	More Details
CVE-2025-68460	Roundcube Webmail before 1.5.12 and 1.6 before 1.6.12 is prone to a information disclosure vulnerability in the HTML style sanitizer.	7.2	More Details
CVE-2025-55707	Incorrect Privilege Assignment vulnerability in WPXPO PostX ultimate-post allows Privilege Escalation.This issue affects PostX: from n/a through <= 4.1.35.	7.2	More Details
CVE-2025-66923	A Cross-site scripting (XSS) vulnerability in Create/Update Customer(s) in Open Source Point of Sale v3.4.1 allows remote attackers to inject arbitrary web script or HTML via the phone_number parameter.	7.2	More Details
CVE-2025-49379	Incorrect Privilege Assignment vulnerability in silverplugins217 Custom Fields Account Registration For Woocommerce custom-fields-account-registration-for-woocommerce allows Privilege Escalation.This issue affects Custom Fields Account Registration For Woocommerce: from n/a through <= 1.2.	7.2	More Details
CVE-2025-68459	RG - AP180, Indoor Wall Plate Wireless AP AP180 series provided by Ruijie Networks Co., Ltd. contain an OS command injection vulnerability. An arbitrary OS command may be executed on the product by an attacker who logs in to the CLI service.	7.2	More Details
CVE-2025-66396	ChurchCRM is an open-source church management system. Prior to version 6.5.3, a SQL injection vulnerability exists in the \`src/UserEditor.php\` file. When an administrator saves a user's configuration settings, the keys of the \`type\` POST parameter array are not properly sanitized or type-casted before being used in multiple SQL queries. This allows a malicious or compromised administrator account to execute arbitrary SQL commands, including time-based blind SQL injection attacks, to directly interact with the database. The vulnerability is located in \`src/UserEditor.php\` within the logic that handles saving user-specific configuration settings. The \`type\` parameter from the POST request is processed as an array. The code iterates through this array and uses \`key($type)\` to extract the array key, which is expected to be a numeric ID. This key is then assigned to the \`$id\` variable. The \`$id\` variable is subsequently concatenated directly into a \`SELECT\` and an \`UPDATE\` SQL query without any sanitization or validation, making it an injection vector. Although the vulnerability requires administrator privileges to exploit, it allows a malicious or compromised admin account to execute arbitrary SQL queries. This can be used to bypass any application-level logging or restrictions, directly manipulate the database, exfiltrate, modify, or delete all data (including other user credentials, financial records, and personal information), and could potentially lead to further system compromise, such as writing files to the server, depending on the database's configuration and user privileges. Version 6.5.3 patches the issue.	7.2	More Details
CVE-2025-68385	Improper neutralization of input during web page generation ('Cross-site Scripting') (CWE-79) allows an authenticated user to embed a malicious script in content that will be served to web browsers causing cross-site scripting (XSS) (CAPEC-63) via a method in Vega bypassing a previous Vega XSS mitigation.	7.2	More Details
CVE-2025-14273	Mattermost versions 11.1.x <= 11.1.0, 11.0.x <= 11.0.5, 10.12.x <= 10.12.3, 10.11.x <= 10.11.7 with the Jira plugin enabled and Mattermost Jira plugin versions <=4.4.0 fail to enforce authentication and issue-key path restrictions in the Jira plugin, which allows an unauthenticated attacker who knows a valid user ID to issue authenticated GET and POST requests to the Jira server via crafted plugin payloads that spoof the user ID and inject arbitrary issue key paths. Mattermost Advisory ID: MMSA-2025-00555	7.2	More Details
CVE-2025-14097	A vulnerability in the application software of multiple Radiometer products may allow remote code execution and unauthorized device management when specific internal conditions are met. Exploitation requires that a remote connection is established with additional information obtained through other means. The issue is caused by a weakness in the analyzer’s application software. Other related CVE's are CVE-2025-14095 & CVE-2025-14096. Affected customers have been informed about this vulnerability. This CVE is being published to provide transparency. Required Configuration for Exposure: Affected application software version is in use and remote support feature is enabled in the analyzer. Temporary work Around: If the network is not considered secure, please remove the analyzer from the network. Permanent solution: Customers should ensure the following: • The network is secure, and access follows best practices. Local Radiometer representatives will contact all affected customers to discuss a permanent solution. Exploit Status: Researchers have provided working proof-of-concept (PoC). Radiometer is not aware of any publicly available exploits at the time of this publication.	7.2	More Details
CVE-2021-47732	CMSimple 5.2 contains a stored cross-site scripting vulnerability in the Filebrowser External input field that allows attackers to inject malicious JavaScript. Attackers can place unfiltered JavaScript code that executes when users click on Page or Files tabs, enabling persistent script injection.	7.2	More Details

CVE-2025-12514	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Centreon Infra Monitoring - Open-tickets (Notification rules configuration parameters, Open tickets modules) allows SQL Injection to user with elevated privileges.This issue affects Infra Monitoring - Open-tickets: from 24.10.0 before 24.10.5, from 24.04.0 before 24.04.5, from 23.10.0 before 23.10.4.	7.2	More Details
CVE-2025-68111	ChurchCRM is an open-source church management system. In versions prior to 6.5.3, a SQL injection vulnerability exists in the `eGive.php` file within the "ReImport" functionality. An authenticated user with finance privileges can execute arbitrary SQL queries by manipulating the `MissingEgive_FamID_...` POST parameter. This can lead to unauthorized data access, modification, or deletion within the database. Version 6.5.3 has a patch for the issue.	7.2	More Details
CVE-2025-66921	A Cross-site scripting (XSS) vulnerability in Create/Update Item(s) Module in Open Source Point of Sale v3.4.1 allows remote attackers to inject arbitrary web script or HTML via the "name" parameter.	7.2	More Details
CVE-2025-14855	The SureForms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form field parameters in all versions up to, and including, 2.2.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2025-9343	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to Stored Cross-Site Scripting via ticket subjects in all versions up to, and including, 3.3.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2020-36890	An access control bypass vulnerability in Kentico Xperience allows administrators to modify global administrator user privileges via unauthorized requests. Attackers could potentially compromise global administrator accounts and invalidate security-sensitive macros by manipulating user privilege levels.	7.2	More Details
CVE-2025-68461	Roundcube Webmail before 1.5.12 and 1.6 before 1.6.12 is prone to a Cross-Site-Scripting (XSS) vulnerability via the animate tag in an SVG document.	7.2	More Details
CVE-2025-14884	A vulnerability was detected in D-Link DIR-605 202WWB03. Affected by this issue is some unknown functionality of the component Firmware Update Service. Performing manipulation results in command injection. The attack can be initiated remotely. The exploit is now public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	7.2	More Details
CVE-2025-1927	Cross-Site Request Forgery (CSRF) vulnerability in Restajet Information Technologies Inc. Online Food Delivery System allows Cross Site Request Forgery.This issue affects Online Food Delivery System: through 19122025.	7.1	More Details
CVE-2025-62000	BullWall Ransomware Containment does not entirely inspect a file to determine if it is ransomware. An authenticated attacker could bypass detection by encrypting a file and leaving the first four bytes unaltered. Versions 4.6.0.0, 4.6.0.6, 4.6.0.7, and 4.6.1.4 were confirmed to be affected; other versions before and after may also be affected.	7.1	More Details
CVE-2025-67745	MyHoard is a daemon for creating, managing and restoring MySQL backups. Starting in version 1.0.1 and prior to version 1.3.0, in some cases, myhoard logs the whole backup info, including the encryption key. Version 1.3.0 fixes the issue. As a workaround, direct logs into /dev/null.	7.1	More Details
CVE-2025-68478	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to version 1.7.0, if an arbitrary path is specified in the request body's `fs_path`, the server serializes the Flow object into JSON and creates/overwrites a file at that path. There is no path restriction, normalization, or allowed directory enforcement, so absolute paths (e.g., /etc/poc.txt) are interpreted as is. Version 1.7.0 fixes the issue.	7.1	More Details
CVE-2025-66736	youlai-boot V2.21.1 is vulnerable to Incorrect Access Control. The importUsers function in SysUserController.java does not perform a permission check on the current user's identity, which may allow regular users to import user data into the database, resulting in an authorization bypass vulnerability.	7.1	More Details
CVE-2021-47720	Orangescrum 1.8.0 contains an authenticated SQL injection vulnerability that allows authorized users to manipulate database queries through multiple vulnerable parameters. Attackers can inject malicious SQL code into parameters like old_project_id, project_id, uuid, and uniqid to potentially extract or modify database information.	7.1	More Details
CVE-2025-14701	An input neutralization vulnerability in the Server MOTD component of Crafty Controller allows a remote, unauthenticated attacker to perform stored XSS via server MOTD modification.	7.1	More Details
CVE-2025-64207	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in TieLabs Jannah jannah allows DOM-Based XSS.This issue affects Jannah: from n/a through <= 7.6.0.	7.1	More Details
CVE-2025-64191	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 8theme XStore xstore allows Reflected XSS.This issue affects XStore: from n/a through < 9.6.1.	7.1	More Details
CVE-2025-64372	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in shinetheme Traveler traveler allows Reflected XSS.This issue affects Traveler: from n/a through < 3.2.6.	7.1	More Details

CVE-2025-64376	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CridioStudio ListingPro listingpro allows Reflected XSS.This issue affects ListingPro: from n/a through < 2.9.10.	7.1	More Details
CVE-2025-64221	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in designthemes Reservation Plugin dt-reservation-plugin allows Reflected XSS.This issue affects Reservation Plugin: from n/a through <= 1.6.	7.1	More Details
CVE-2025-64217	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Photography photography allows Reflected XSS.This issue affects Photography: from n/a through <= 7.7.2.	7.1	More Details
CVE-2025-65203	KeePassXC-Browser thru 1.9.9.2 autofills or prompts to fill stored credentials into documents rendered under a browser-enforced CSP directive and iframe attribute sandbox, allowing attacker-controlled script in the sandboxed document to access populated form fields and exfiltrate credentials.	7.1	More Details
CVE-2025-66118	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BoldGrid Sprout Clients sprout-clients allows Reflected XSS.This issue affects Sprout Clients: from n/a through <= 3.2.1.	7.1	More Details
CVE-2025-64203	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in EverPress Mailster mailster allows Reflected XSS.This issue affects Mailster: from n/a through < 4.1.14.	7.1	More Details
CVE-2025-66119	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bob Hostel hostel allows Reflected XSS.This issue affects Hostel: from n/a through <= 1.1.5.9.	7.1	More Details
CVE-2025-64189	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 8theme XStore Core et-core-plugin allows Reflected XSS.This issue affects XStore Core: from n/a through < 5.6.	7.1	More Details
CVE-2025-54751	Missing Authorization vulnerability in WPXPO PostX ultimate-post allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PostX: from n/a through <= 4.1.36.	7.1	More Details
CVE-2025-57897	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in venusweb Logtik logtik allows Reflected XSS.This issue affects Logtik: from n/a through <= 2.3.	7.1	More Details
CVE-2025-60079	Missing Authorization vulnerability in bPlugins Parallax Section block parallax-section allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Parallax Section block: from n/a through <= 1.0.9.	7.1	More Details
CVE-2025-60182	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Schiocco Support Board supportboard allows Reflected XSS.This issue affects Support Board: from n/a through < 3.8.7.	7.1	More Details
CVE-2025-14101	Authorization Bypass Through User-Controlled Key vulnerability in GG Soft Software Services Inc. PaperWork allows Exploitation of Trusted Identifiers.This issue affects PaperWork: from 5.2.0.9427 before 6.0.	7.1	More Details
CVE-2025-6324	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MatrixAddons Easy Invoice easy-invoice allows DOM-Based XSS.This issue affects Easy Invoice: from n/a through <= 2.0.9.	7.1	More Details
CVE-2025-64260	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Marco Milesi ANAC XML Bandi di Gara avcp allows Reflected XSS.This issue affects ANAC XML Bandi di Gara: from n/a through <= 7.7.	7.1	More Details
CVE-2025-68617	FluidSynth is a software synthesizer based on the SoundFont 2 specifications. From versions 2.5.0 to before 2.5.2, a race condition during unloading of a DLS file can trigger a heap-based use-after-free. A concurrently running thread may be pending to unload a DLS file, leading to use of freed memory, if the synthesizer is being concurrently destroyed, or samples of the (unloaded) DLS file are concurrently used to synthesize audio. This issue has been patched in version 2.5.2. The problem will not occur, when explicitly unloading a DLS file (before synth destruction), provided that at the time of unloading, no samples of the respective file are used by active voices. The problem will not occur in versions of FluidSynth that have been compiled without native DLS support.	7.0	More Details
CVE-2025-54890	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (Hostgroup configuration page) allows Stored XSS by users with elevated privileges.This issue affects Infra Monitoring: from 24.10.0 before 24.10.15, from 24.04.0 before 24.04.19, from 23.10.0 before 23.10.29.	6.8	More Details
CVE-2025-14304	Certain motherboard models developed by ASRock and its subsidiaries, ASRockRack and ASRockInd. has a Protection Mechanism Failure vulnerability. Because IOMMU was not properly enabled, unauthenticated physical attackers can use a DMA-capable PCIe device to read and write arbitrary physical memory before the OS kernel and its security features are loaded.	6.8	More Details
	A "Privilege boundary violation" vulnerability is identified affecting multiple Radiometer Products. Exploitation of this		

CVE-2025-14095	vulnerability gives a user with physical access to the analyzer, the possibility to gain unauthorized access to functionalities outside the restricted environment. The vulnerability is due to weakness in the design of access control implementation in application software. Other related CVE's are CVE-2025-14096 & CVE-2025-14097. Affected customers have been informed about this vulnerability. This CVE is being published to provide transparency. Required configuration for Exposure: Physical access to the analyzer is needed. Temporary work Around: Only authorized people can physically access the analyzer. Permanent solution: Local Radiometer representatives will contact all affected customers to discuss a permanent solution. Exploit Status: Researchers have provided working proof-of-concept. Radiometer is not aware of any publicly available exploit at the time of publication. Note: CVSS score 6.8 when underlying OS is Windows 7 or Windows XP Operating systems and CVSS score 5.7 when underlying OS is Windows 8 or Windows 10 operating systems.	6.8	More Details
CVE-2025-68129	Auth0-PHP is a PHP SDK for Auth0 Authentication and Management APIs. In applications built with the Auth0-PHP SDK, the audience validation in access tokens is performed improperly. Without proper validation, affected applications may accept ID tokens as Access tokens. Projects are affected if they use Auth0-PHP SDK versions between v8.0.0 and v8.17.0, or applications using the following SDKs that rely on the Auth0-PHP SDK versions between v8.0.0 and v8.17.0: Auth0/symfony versions between 5.0.0 and 5.5.0, Auth0/laravel-auth0 versions between 7.0.0 and 7.19.0, and/or Auth0/wordpress plugin versions between 5.0.0-BETA0 and 5.4.0. Auth0/Auth0-PHP version 8.18.0 contains a patch for the issue.	6.8	More Details
CVE-2023-30971	Gotham Gaia application was found to be exposing multiple unauthenticated endpoints.	6.8	More Details
CVE-2025-14303	Certain motherboard models developed by MSI has a Protection Mechanism Failure vulnerability. Because IOMMU was not properly enabled, unauthenticated physical attackers can use a DMA-capable PCIe device to read and write arbitrary physical memory before the OS kernel and its security features are loaded.	6.8	More Details
CVE-2025-14302	Certain motherboard models developed by GIGABYTE has a Protection Mechanism Failure vulnerability. Because IOMMU was not properly enabled, unauthenticated physical attackers can use a DMA-capable PCIe device to read and write arbitrary physical memory before the OS kernel and its security features are loaded.	6.8	More Details
CVE-2025-8460	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (Notification rules, Open tickets module) allows Stored XSS by users with elevated privileges.This issue affects Infra Monitoring: from 24.10.0 before 24.10.5, from 24.04.0 before 24.04.5, from 23.10.0 before 23.10.4.	6.8	More Details
CVE-2025-67173	A Cross-Site Request Forgery (CSRF) in the page creation/editing function of RiteCMS v3.1.0 allows attackers to arbitrarily create pages via a crafted POST request.	6.8	More Details
CVE-2021-47714	Hasura GraphQL 1.3.3 contains a local file read vulnerability that allows attackers to access system files through SQL injection in the query endpoint. Attackers can exploit the pg_read_file() PostgreSQL function by crafting malicious SQL queries to read arbitrary files on the server.	6.8	More Details
CVE-2025-47319	Information disclosure while exposing internal TA-to-TA communication APIs to HLOS	6.7	More Details
CVE-2025-40602	A local privilege escalation vulnerability due to insufficient authorization in the SonicWall SMA1000 appliance management console (AMC).	6.6	More Details
CVE-2025-65855	The OTA firmware update mechanism in Netun Solutions HelpFlash IoT (firmware v18_178_221102_ASCII_PRO_1R5_50) uses hard-coded WiFi credentials identical across all devices and does not authenticate update servers or validate firmware signatures. An attacker with brief physical access can activate OTA mode (8-second button press), create a malicious WiFi AP using the known credentials, and serve malicious firmware via unauthenticated HTTP to achieve arbitrary code execution on this safety-critical emergency signaling device.	6.6	More Details
CVE-2025-60088	Missing Authorization vulnerability in Saleswonder Team: Tobias WebinarIgnition webinar-ignition allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WebinarIgnition: from n/a through <= 4.06.04.	6.5	More Details
CVE-2025-60070	Improper Control of Generation of Code ('Code Injection') vulnerability in The4 Molla molla allows Code Injection.This issue affects Molla: from n/a through <= 1.5.13.	6.5	More Details
CVE-2025-60068	Improper Control of Generation of Code ('Code Injection') vulnerability in javothemes Javo Core javo-core allows Code Injection.This issue affects Javo Core: from n/a through <= 3.0.0.266.	6.5	More Details
CVE-2025-15033	A vulnerability in WooCommerce 8.1 to 10.4.2 can allow logged-in customers to access order data of guest customers on sites with a certain configuration. This has been fixed in WooCommerce 10.4.3, as well as all the previously affected versions through point releases, starting from 8.1, where it has been fixed in 8.1.3. It does not affect WooCommerce 8.0 or earlier.	6.5	More Details
CVE-2025-34435	AVideo versions prior to 20.1 are vulnerable to an insecure direct object reference (IDOR) that allows any authenticated user to delete media files belonging to other users. The affected endpoint validates authentication but fails to verify ownership or edit permissions for the targeted video.	6.5	More Details

CVE-2025-10019	Authorization Bypass Through User-Controlled Key vulnerability in codepeople Contact Form Email contact-form-to-email allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Contact Form Email: from n/a through <= 1.3.60.	6.5	More Details
CVE-2025-54748	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in RomanCode MapSVG mapsvg allows Path Traversal.This issue affects MapSVG: from n/a through < 8.6.12.	6.5	More Details
CVE-2025-54745	Missing Authorization vulnerability in miniOrange miniOrange's Google Authenticator miniorange-2-factor-authentication allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects miniOrange's Google Authenticator: from n/a through <= 6.1.1.	6.5	More Details
CVE-2025-62901	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tormorten WP Microdata allows Stored XSS.This issue affects WP Microdata: from n/a through 1.0.	6.5	More Details
CVE-2023-53907	Bludit versions before 3.13.1 contain an authenticated file download vulnerability in the Backup Plugin that allows logged-in users to access arbitrary files. Attackers can exploit the plugin's download functionality by manipulating file path parameters to read sensitive system files through directory traversal.	6.5	More Details
CVE-2025-67436	Authenticated Remote Code Execution (RCE) in PluXml CMS 5.8.22 allows an attacker with administrator panel access to inject a malicious PHP webshell into a theme file (e.g., home.php).	6.5	More Details
CVE-2025-68389	Allocation of Resources Without Limits or Throttling (CWE-770) in Kibana can allow a low-privileged authenticated user to cause Excessive Allocation (CAPEC-130) of computing resources and a denial of service (DoS) of the Kibana process via a crafted HTTP request.	6.5	More Details
CVE-2025-62926	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HappyDevs TempTool allows Stored XSS.This issue affects TempTool: from n/a through 1.3.1.	6.5	More Details
CVE-2025-49914	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in jetmonsters Restaurant Menu by MotoPress mp-restaurant-menu allows Retrieve Embedded Sensitive Data.This issue affects Restaurant Menu by MotoPress: from n/a through <= 2.4.7.	6.5	More Details
CVE-2025-68381	Improper Bounds Check (CWE-787) in Packetbeat can allow a remote unauthenticated attacker to exploit a Buffer Overflow (CAPEC-100) and reliably crash the application or cause significant resource exhaustion via a single crafted UDP packet with an invalid fragment sequence number.	6.5	More Details
CVE-2025-12689	Mattermost versions 11.0.x <= 11.0.4, 10.12.x <= 10.12.2, 10.11.x <= 10.11.6 fail to check WebSocket request field for proper UTF-8 format, which allows attacker to crash Calls plug-in via sending malformed request.	6.5	More Details
CVE-2025-49902	Missing Authorization vulnerability in A WP Life Login Page Customizer &#8211; Customizer Login Page, Admin Page, Custom Design customizer-login-page allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Login Page Customizer &#8211; Customizer Login Page, Admin Page, Custom Design: from n/a through <= 2.1.1.	6.5	More Details
CVE-2025-49041	Missing Authorization vulnerability in The African Boss Get Cash get-cash allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Get Cash: from n/a through <= 3.2.3.	6.5	More Details
CVE-2025-8304	An authenticated local user can obtain information that allows claiming security policy rules of another user due to sensitive information being accessible in the Windows Registry keys for Check Point Identity Agent running on a Terminal Server.	6.5	More Details
CVE-2025-8305	An authenticated local user can obtain information that allows claiming security policy rules of another user due to sensitive information being printed in plaintext in Identity Agent for Terminal Services debug files.	6.5	More Details
CVE-2025-62094	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Voidthemes Void Elementor WHMCS Elements For Elementor Page Builder.This issue affects Void Elementor WHMCS Elements For Elementor Page Builder: from n/a through 2.0.1.2.	6.5	More Details
CVE-2023-53944	EasyPHP Webserver 14.1 contains a path traversal vulnerability that allows remote users with low privileges to access files outside the document root by bypassing SecurityManager restrictions. Attackers can send GET requests with encoded directory traversal sequences like /..%5c..%5c to read system files such as /windows/win.ini.	6.5	More Details
CVE-2025-68382	Out-of-bounds read (CWE-125) allows an unauthenticated remote attacker to perform a buffer overflow (CAPEC-100) via the NFS protocol dissector, leading to a denial-of-service (DoS) through a reliable process crash when handling truncated XDR-encoded RPC messages.	6.5	More Details
CVE-2025-68383	Improper Validation of Specified Index, Position, or Offset in Input (CWE-1285) in Filebeat Syslog parser and the Libbeat Dissect processor can allow a user to trigger a Buffer Overflow (CAPEC-100) and cause a denial of service (panic/crash) of the Filebeat process via either a malformed Syslog message or a malicious tokenizer pattern in the Dissect configuration.	6.5	More Details

CVE-2025-68384	Allocation of Resources Without Limits or Throttling (CWE-770) in Elasticsearch can allow a low-privileged authenticated user to cause Excessive Allocation (CAPEC-130) causing a persistent denial of service (OOM crash) via submission of oversized user settings data.	6.5	More Details
CVE-2025-67074	A Buffer overflow vulnerability in function fromAdvSetMacMtuWan of bin httpd in Tenda AC10V4.0 V16.03.10.20 allows remote attackers to cause denial of service and possibly code execution by sending a post request with a crafted payload (field `serverName`) to /goform/AdvSetMacMtuWan.	6.5	More Details
CVE-2022-50682	A CRLF injection vulnerability in Kentico Xperience allows attackers to manipulate URL query string redirects via improper encoding in the routing engine. This could enable header injection and potentially facilitate further web application attacks.	6.5	More Details
CVE-2025-47325	Information disclosure while processing system calls with invalid parameters.	6.5	More Details
CVE-2025-66058	Missing Authorization vulnerability in PickPlugins Post Grid and Gutenberg Blocks allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Post Grid and Gutenberg Blocks: from n/a through 2.3.17.	6.5	More Details
CVE-2025-14817	The component com.transsion.tranfacmode.entrance.main.MainActivity in com.transsion.tranfacmode has no permission control and can be accessed by third-party apps which can construct intents to directly open adb debugging functionality without user interaction.	6.5	More Details
CVE-2025-64355	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetElements For Elementor allows DOM-Based XSS.This issue affects JetElements For Elementor: from n/a through 2.7.12.	6.5	More Details
CVE-2023-53917	Affiliate Me version 5.0.1 contains a SQL injection vulnerability in the admin.php endpoint that allows authenticated administrators to manipulate database queries. Attackers can exploit the 'id' parameter with crafted union-based queries to extract sensitive user information including usernames and password hashes.	6.5	More Details
CVE-2025-66911	Turms IM Server v0.10.0-SNAPSHOT and earlier contains a broken access control vulnerability in the user online status query functionality. The handleQueryUserOnlineStatusesRequest() method in UserServiceController.java allows any authenticated user to query the online status, device information, and login timestamps of arbitrary users without proper authorization checks.	6.5	More Details
CVE-2025-64270	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in masteriyo Masteriyo - LMS learning-management-system allows Retrieve Embedded Sensitive Data.This issue affects Masteriyo - LMS: from n/a through <= 2.0.3.	6.5	More Details
CVE-2025-45493	Netgear EX8000 V1.0.0.126 is vulnerable to Command Injection via the iface parameter in the action_bandwidth function.	6.5	More Details
CVE-2025-64272	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in GetResponse Email marketing for WordPress by GetResponse Official getresponse-official allows Retrieve Embedded Sensitive Data.This issue affects Email marketing for WordPress by GetResponse Official: from n/a through <= 1.5.3.	6.5	More Details
CVE-2025-64295	Insertion of Sensitive Information Into Sent Data vulnerability in Syed Balkhi All In One SEO Pack all-in-one-seo-pack allows Retrieve Embedded Sensitive Data.This issue affects All In One SEO Pack: from n/a through <= 4.8.6.1.	6.5	More Details
CVE-2025-64375	Missing Authorization vulnerability in Mahmudul Hasan Arif WP Social Ninja wp-social-reviews allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Social Ninja: from n/a through <= 3.20.1.	6.5	More Details
CVE-2025-66068	Missing Authorization vulnerability in InstaWP InstaWP Connect instawp-connect allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects InstaWP Connect: from n/a through <= 0.1.1.9.	6.5	More Details
CVE-2025-66100	Missing Authorization vulnerability in Magnigenie RestroPress restropress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects RestroPress: from n/a through <= 3.2.3.5.	6.5	More Details
CVE-2025-66104	Missing Authorization vulnerability in Anton Vanyukov Offload, AI &amp; Optimize with Cloudflare Images cf-images allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Offload, AI &amp; Optimize with Cloudflare Images: from n/a through <= 1.9.5.	6.5	More Details
CVE-2025-14744	Unicode RTLO characters could allow malicious websites to spoof filenames in the downloads UI for Firefox for iOS, potentially tricking users into saving files of an unexpected file type. This vulnerability affects Firefox for iOS < 144.0.	6.5	More Details
CVE-2025-13880	The WP Social Ninja – Embed Social Feeds, Customer Reviews, Chat Widgets (Google Reviews, YouTube Feed, Photo Feeds, and More) plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on the getAdvanceSettings and saveAdvanceSettings functions in all versions up to, and including, 4.0.1. This makes it possible for unauthenticated attackers to view and modify plugin's advanced settings.	6.5	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebCodingPlace		

2025-68548	Responsive Posts Carousel Pro allows Stored XSS.This issue affects Responsive Posts Carousel Pro: from n/a through 15.2.	6.5	More Details
CVE-2025-67546	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in weDevs WP ERP erp allows Retrieve Embedded Sensitive Data.This issue affects WP ERP: from n/a through <= 1.16.6.	6.5	More Details
CVE-2025-68559	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem Theme Elements (for Elementor).This issue affects TheGem Theme Elements (for Elementor): from n/a through 5.10.5.1.	6.5	More Details
CVE-2023-53908	HiSecOS 04.0.01 contains a privilege escalation vulnerability that allows authenticated users to modify their access role through XML-based NETCONF configuration. Attackers can send crafted XML payloads to the /mops_data endpoint with a specific role value to elevate their user privileges to administrative level.	6.5	More Details
CVE-2025-63039	Missing Authorization vulnerability in CridioStudio ListingPro listingpro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ListingPro: from n/a through <= 2.9.9.	6.5	More Details
CVE-2025-66174	There is an improper authentication vulnerability in some Hikvision DVR products. Due to the improper implementation of authentication for the serial port, an attacker with physical access could exploit this vulnerability by connecting to the affected products and run a series of commands.	6.5	More Details
CVE-2025-68551	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Vikas Ratudi VPSUForm allows Retrieve Embedded Sensitive Data.This issue affects VPSUForm: from n/a through 3.2.24.	6.5	More Details
CVE-2025-64997	Insufficient permission validation in Checkmk versions prior to 2.4.0p17 and 2.3.0p42 allow low-privileged users to view agent information via the REST API, which could lead to information disclosure.	6.5	More Details
CVE-2025-64235	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in AmentoTech Tuturn allows Path Traversal.This issue affects Tuturn: from n/a before 3.6.	6.5	More Details
CVE-2025-12885	The Embed Any Document – Embed PDF, Word, PowerPoint and Excel Files plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the sanitize_pdf_src function regex bypass in all versions up to, and including, 2.7.10 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-2025-13537	The Live Composer – Free WordPress Website Builder plugin for WordPress is vulnerable to multiple Stored Cross-Site Scripting vulnerabilities via DOM manipulation in all versions up to, and including, 2.0.2 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-2023-53953	WebsiteBaker 2.13.3 contains a stored cross-site scripting vulnerability that allows authenticated users to inject malicious scripts when creating web pages. Attackers can craft malicious payloads in page titles that execute arbitrary JavaScript when the page is viewed by other users.	6.4	More Details
CVE-2025-12976	The Events Manager – Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'events_list_grouped' shortcode in all versions up to, and including, 7.2.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-13977	The Essential Addons for Elementor – Popular Elementor Templates & Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple attack vectors in all versions up to, and including, 6.5.3. This is due to insufficient input sanitization and output escaping in the Event Calendar widget's custom attributes handling and the Image Masking module's element ID rendering. 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-2025-11747	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the colibri_blog_posts shortcode in all versions up to, and including, 1.0.345 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-2021-47738	CSZ CMS 1.2.7 contains a persistent cross-site scripting vulnerability that allows unauthorized users to embed malicious JavaScript in private messages. Attackers can send messages with script payloads in the user-agent header, which will execute when an admin views the message in the backend dashboard.	6.4	More Details
CVE-2025-	The vulnerability affects Ignition SCADA applications where Python scripting is utilized for automation purposes. The vulnerability arises from the absence of proper security controls that restrict which Python libraries can be imported and executed within the scripting environment. The core issue lies in the Ignition service account having system permissions beyond what an Ignition privileged user requires. When an authenticated administrator uploads a malicious	6.4	More Details

13911	project file containing Python scripts with bind shell capabilities, the application executes these scripts with the same privileges as the Ignition Gateway process, which typically runs with SYSTEM-level permissions on Windows. Alternative code execution patterns could lead to similar results.		
CVE-2025-65035	pluginsGLPI's Database Inventory Plugin "manages" the Teclib' inventory agents in order to perform an inventory of the databases present on the workstation. Prior to version 1.1.2, in certain conditions (database write access must first be obtained through another vulnerability or misconfiguration), user-controlled data is stored insecurely in the database via computergroup, and is later unserialized on every page load, allowing arbitrary PHP object instantiation. Version 1.1.2 fixes the issue.	6.4	More Details
CVE-2025-14635	The Happy Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ha_page_custom_js' parameter in all versions up to, and including, 3.20.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page, despite the intended role restriction of Custom JS to Administrators.	6.4	More Details
CVE-2025-67845	A Directory Traversal vulnerability in the Static Asset Proxy Endpoint in Mintlify Platform before 2025-11-15 allows remote attackers to inject arbitrary web script or HTML via a crafted URL containing path traversal sequences.	6.4	More Details
CVE-2025-13693	The Image Photo Gallery Final Tiles Grid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Custom scripts' setting in all versions up to, and including, 3.6.8 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-2025-13730	The OpenID Connect Generic Client plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'openid_connect_generic_auth_url' shortcode in all versions up to, and including, 3.10.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14548	The Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'event_desc' parameter in all versions up to, and including, 1.3.16 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, granted they can convince an administrator to enable lower privilege users to manage calendar events via the plugin settings.	6.4	More Details
CVE-2025-14449	The BA Book Everything plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's babe-search-form shortcode in all versions up to, and including, 1.8.14 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-2023-53978	myBB Forums 1.8.26 contains a stored cross-site scripting vulnerability in the forum announcement system that allows authenticated administrators to inject malicious scripts when creating announcements. Attackers can exploit this vulnerability by inserting script payloads in the announcement title field when adding announcements through the 'Forums and Posts' > 'Forum Announcements' interface, causing arbitrary JavaScript to execute when the announcement is displayed on the forum.	6.4	More Details
CVE-2025-67842	The Static Asset API in Mintlify Platform before 2025-11-15 allows remote attackers to inject arbitrary web script or HTML via the subdomain parameter because any tenant's assets can be served on any other tenant's documentation site.	6.4	More Details
CVE-2023-53977	myBB Forums 1.8.26 contains a stored cross-site scripting vulnerability in the forum management system that allows authenticated administrators to inject malicious scripts when creating new forums. Attackers can exploit this vulnerability by inserting script payloads in the forum title field when adding new forums through the 'Forums and Posts' > 'Forum Management' interface, causing arbitrary JavaScript to execute when the forum listing is viewed.	6.4	More Details
CVE-2023-53976	myBB Forums 1.8.26 contains a stored cross-site scripting vulnerability in the template management system that allows authenticated administrators to inject malicious scripts when creating new templates. Attackers can exploit this vulnerability by inserting script payloads in the template title field when adding new templates through the 'Templates and Style' > 'Templates' > 'Manage Templates' > 'Global Templates' interface, causing arbitrary JavaScript to execute when the template is viewed.	6.4	More Details
CVE-2025-13838	The WishSuite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button_text' parameter of the 'wishsuite_button' shortcode in all versions up to, and including, 1.5.1 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-2025-13217	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the YouTube Video 'value' field in all versions up to, and including, 2.11.0. This is due to insufficient input sanitization and output escaping on user-supplied YouTube video URLs in the `um_profile_field_filter_hook__youtube_video()` function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that execute whenever a user accesses the injected user's profile page.	6.4	More Details
CVE-2025-14000	The Membership Plugin – Restrict Content plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'register_form' and 'restrict' shortcodes in all versions up to, and including, 3.2.15 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	6.4	More Details

	an injected page.		
CVE-2025-14385	The WP Recipe Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name' parameter in all versions up to, and including, 10.2.3 due to insufficient input sanitization and output escaping on user-supplied attributes in the wprm-recipe-roundup-item shortcode. 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-2025-13220	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode attributes in all versions up to, and including, 2.11.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-14546	Versions of the package fastapi-sso before 0.19.0 are vulnerable to Cross-site Request Forgery (CSRF) due to the improper validation of the OAuth state parameter during the authentication callback. While the get_login_url method allows for state generation, it does not persist the state or bind it to the user's session. Consequently, the verify_and_process method accepts the state received in the query parameters without verifying it against a trusted local value. This allows a remote attacker to trick a victim into visiting a malicious callback URL, which can result in the attacker's account being linked to the victim's internal account.	6.3	More Details
CVE-2025-14856	A security vulnerability has been detected in y_project RuoYi up to 4.8.1. The affected element is an unknown function of the file /monitor/cache/getnames. Such manipulation of the argument fragment leads to code injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	6.3	More Details
CVE-2025-66500	A stored cross-site scripting (XSS) vulnerability exists in webplugins.foxit.com. A postMessage handler fails to validate the message origin and directly assigns externalPath to a script source, allowing an attacker to execute arbitrary JavaScript when a crafted postMessage is received.	6.3	More Details
CVE-2025-15009	A flaw has been found in liweiyi ChestnutCMS up to 1.5.8. This vulnerability affects the function FilenameUtils.getExtension of the file /dev-api/common/upload of the component Filename Handler. Executing manipulation of the argument File can lead to unrestricted upload. The attack may be launched remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-66501	A stored cross-site scripting (XSS) vulnerability exists in pdfonline.foxit.com within the Predefined Text feature of the Foxit eSign section. A crafted payload can be stored via the Identity “First Name” field, which is later rendered into the DOM without proper sanitization. As a result, the injected script may execute when predefined text is used or when viewing document properties.	6.3	More Details
CVE-2025-66502	A stored cross-site scripting (XSS) vulnerability exists in pdfonline.foxit.com within the Page Templates feature. A crafted payload can be stored as the template name, which is later rendered into the DOM without proper sanitization. As a result, the injected script executes each time the affected PDF is loaded.	6.3	More Details
CVE-2025-14908	A security flaw has been discovered in JeecgBoot up to 3.9.0. The affected element is an unknown function of the file jeecg-boot/jeecg-module-system/jeecg-system-biz/src/main/java/org/jeecg/modules/system/controller/SysTenantController.java of the component Multi-Tenant Management Module. Performing manipulation of the argument ID results in improper authentication. The attack can be initiated remotely. The exploit has been released to the public and may be exploited. The patch is named e1c8f00bf2a2e0edddbaa8119afe1dc92d9dc1d2/67795493bdc579e489d3ab12e52a1793c4f8a0ee. It is recommended to apply a patch to fix this issue.	6.3	More Details
CVE-2025-15004	A vulnerability was identified in DedeCMS up to 5.7.118. This impacts an unknown function of the file /freelist_main.php. The manipulation of the argument orderby leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2025-66519	A stored cross-site scripting (XSS) vulnerability exists in pdfonline.foxit.com within the Layer Import functionality. A crafted payload can be injected into the “Create new Layer” field during layer import and is later rendered into the DOM without proper sanitization. As a result, the injected script executes when the Layers panel is accessed.	6.3	More Details
CVE-2025-66520	A stored cross-site scripting (XSS) vulnerability exists in the Portfolio feature of the Foxit PDF Editor cloud (pdfonline.foxit.com). User-supplied SVG files are not properly sanitized or validated before being inserted into the HTML structure. As a result, embedded HTML or JavaScript within a crafted SVG may execute whenever the Portfolio file list is rendered.	6.3	More Details
CVE-2025-66521	A stored cross-site scripting (XSS) vulnerability exists in pdfonline.foxit.com within the Trusted Certificates feature. A crafted payload can be injected as the certificate name, which is later rendered into the DOM without proper sanitization. As a result, the injected script executes each time the Trusted Certificates view is loaded.	6.3	More Details
CVE-2025-14834	A weakness has been identified in code-projects Simple Stock System 1.0. This affects an unknown function of the file /checkuser.php. Executing manipulation of the argument Username can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.	6.3	More Details
CVE-2025-15014	A security flaw has been discovered in loganhong php loganSite up to c035fb5c3edd0b2a5e32fd4051cbbc9e61a31426. This affects an unknown function of the file /includes/article_detail.php of the component Article Handler. Performing manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	6.3	More Details

CVE-2025-66522	A stored cross-site scripting (XSS) vulnerability exists in the Digital IDs functionality of the Foxit PDF Editor Cloud (pdfonline.foxit.com). The application does not properly sanitize or encode the Common Name field of Digital IDs before inserting user-supplied content into the DOM. As a result, embedded HTML or JavaScript may execute whenever the Digital IDs dialog is accessed or when the affected PDF is loaded.	6.3	More Details
CVE-2025-46268	Advantech WebAccess/SCADA is vulnerable to SQL injection, which may allow an attacker to execute arbitrary SQL commands.	6.3	More Details
CVE-2025-64192	Missing Authorization vulnerability in 8theme XStore xstore allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects XStore: from n/a through < 9.6.	6.3	More Details
CVE-2025-67743	Local Deep Research is an AI-powered research assistant for deep, iterative research. In versions from 1.3.0 to before 1.3.9, the download service (download_service.py) makes HTTP requests using raw requests.get() without utilizing the application's SSRF protection (safe_requests.py). This can allow attackers to access internal services and attempt to reach cloud provider metadata endpoints (AWS/GCP/Azure), as well as perform internal network reconnaissance, by submitting malicious URLs through the API, depending on the deployment and surrounding controls. This issue has been patched in version 1.3.9.	6.3	More Details
CVE-2025-14885	A flaw has been found in SourceCodester Client Database Management System 1.0. This affects an unknown part of the file /user_leads.php of the component Leads Generation Module. Executing manipulation can lead to unrestricted upload. The attack can be launched remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2025-14347	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Proliz Software Ltd. OBS (Student Affairs Information System)0 allows Reflected XSS.This issue affects OBS (Student Affairs Information System)0: before 26.5009.	6.3	More Details
CVE-2023-53912	USB Flash Drives Control 4.1.0.0 contains an unquoted service path vulnerability in its service configuration that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in 'C:\Program Files\USB Flash Drives Control\usbcs.exe' to inject malicious executables and escalate privileges on Windows systems.	6.2	More Details
CVE-2022-50689	Cobian Reflector 0.9.93 RC1 contains a denial of service vulnerability that allows attackers to crash the application by overflowing the password input field. Attackers can paste a large 8000-byte buffer into the password field to trigger an application crash during SFTP task configuration.	6.2	More Details
CVE-2025-65410	A stack overflow in the src/main.c component of GNU Unrtf v0.21.10 allows attackers to cause a Denial of Service (DoS) via injecting a crafted input into the filename parameter.	6.2	More Details
CVE-2023-53954	ActFax 10.10 contains an unquoted service path vulnerability that allows local attackers to potentially escalate privileges by exploiting the ActiveFaxServiceNT service configuration. Attackers with write permissions to Program Files directories can inject a malicious ActSrvNT.exe executable to gain elevated system access when the service restarts.	6.2	More Details
CVE-2022-50687	Cobian Backup 11 Gravity 11.2.0.582 contains a denial of service vulnerability in the FTP password input field that allows attackers to crash the application. Attackers can generate a specially crafted 800-byte buffer and paste it into the password field to trigger an application crash.	6.2	More Details
CVE-2025-66173	There is a privilege escalation vulnerability in some Hikvision DVR products. Due to the improper implementation of authentication for the serial port, an attacker with physical access could exploit this vulnerability by connecting to the affected products and gaining access to an unrestricted shell environment.	6.2	More Details
CVE-2025-62003	BullWall Server Intrusion Protection has a noticeable delay before the MFA check when connecting via RDP. A remote authenticated attacker with administrative privileges can potentially bypass detection during this window. Versions 4.6.0.0, 4.6.0.6, 4.6.0.7, and 4.6.1.4 were confirmed to be affected; other versions before and after may also be affected.	6.2	More Details
CVE-2025-62004	BullWall Server Intrusion Protection services are initialized after login services. An authenticated attacker with administrative permissions can log in after boot and bypass MFA. SIP service does not retroactively enforce the challenge or disconnect unauthenticated sessions. Versions 4.6.0.0, 4.6.0.6, 4.6.0.7, and 4.6.1.4 were confirmed to be affected; other versions before and after may also be affected.	6.2	More Details
CVE-2025-66924	A Cross-site scripting (XSS) vulnerability in Create/Update Item Kit(s) in Open Source Point of Sale v3.4.1 allows remote attackers to inject arbitrary web script or HTML via the "name" parameter.	6.1	More Details
CVE-2025-66845	A reflected Cross-Site Scripting (XSS) vulnerability has been identified in TechStore version 1.0. The user_name endpoint reflects the id query parameter directly into the HTML response without output encoding or sanitization, allowing execution of arbitrary JavaScript code in a victim’s browser.	6.1	More Details
CVE-2025-11496	The Five Star Restaurant Reservations – WordPress Booking Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'rtb-name' parameter in all versions up to, and including, 2.7.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.1	More Details
CVE-2025-14154	The Better Messages – Live Chat for WordPress, BuddyPress, PeepSo, Ultimate Member, BuddyBoss plugin for WordPress is vulnerable to Stored Cross-Site Scripting via guest display name in all versions up to, and including, 2.10.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.1	More Details

CVE-2025-14151	The SlimStat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'outbound_resource' parameter in the slimtrack AJAX action in all versions up to, and including, 5.3.2. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.1	More Details
CVE-2025-13624	The Overstock Affiliate Links plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` parameter in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-13365	The WP Hallo Welt plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4. This is due to missing or incorrect nonce validation on the 'hallo_welt_seite' function. This makes it possible for unauthenticated attackers to update plugin 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. Due to the insufficient input sanitization and output escaping, this can lead to Stored Cross-Site Scripting.	6.1	More Details
CVE-2025-13861	The HTML Forms – Simple WordPress Forms Plugin for WordPress is vulnerable to Unauthenticated Stored Cross-Site Scripting in all versions up to and including 1.6.0 due to insufficient sanitization of fabricated file upload field metadata before displaying it in the WordPress admin dashboard. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute whenever an administrator accesses the form submissions page.	6.1	More Details
CVE-2025-12581	The Attachments Handler plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via URL in all versions up to, and including, 1.1.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-68387	Improper neutralization of input during web page generation ('Cross-site Scripting') (CWE-79) allows an unauthenticated user to embed a malicious script in content that will be served to web browsers causing cross-site scripting (XSS) (CAPEC-63) via a vulnerability a function handler in the Vega AST evaluator.	6.1	More Details
CVE-2025-12398	The Product Table for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'search_key' parameter in all versions up to, and including, 5.0.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2025-9787	Zohocorp ManageEngine Applications Manager versions 177400 and below are vulnerable to Stored Cross-Site Scripting vulnerability in the NOC view.	6.1	More Details
CVE-2025-67290	A stored cross-site scripting (XSS) vulnerability in the Page Settings module of Piranha CMS v12.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Excerpt field.	6.1	More Details
CVE-2025-67443	Schlix CMS before v2.2.9-5 is vulnerable to Cross Site Scripting (XSS). Due to lack of javascript sanitization in the login form, incorrect login attempts in logs are triggered as XSS in the admin panel.	6.1	More Details
CVE-2025-34439	AVideo versions prior to 20.1 are vulnerable to an open redirect flaw due to missing validation of the cancelUri parameter during user login. An attacker can craft a link to redirect users to arbitrary external sites, enabling phishing attacks.	6.1	More Details
CVE-2025-40893	A Stored HTML Injection vulnerability was discovered in the Asset List functionality due to improper validation of network traffic data. An unauthenticated attacker can send specially crafted network packets to inject HTML tags into asset attributes. When a victim views the affected assets in the Asset List (and similar functions), the injected HTML renders in their browser, enabling phishing and possibly open redirect attacks. Full XSS exploitation and direct information disclosure are prevented by the existing input validation and Content Security Policy configuration.	6.1	More Details
CVE-2025-64225	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in colabrio Stockie Extra stockie-extra allows Code Injection.This issue affects Stockie Extra: from n/a through <= 1.2.11.	6.1	More Details
CVE-2025-63949	A Reflected Cross-Site Scripting (XSS) vulnerability in yohanawi Hotel Management System (commit 87e004a) allows a remote attacker to execute arbitrary web script via the 'error' parameter in pages/room.php.	6.1	More Details
CVE-2025-67291	A stored cross-site scripting (XSS) vulnerability in the Media module of Piranha CMS v12.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Name field.	6.1	More Details
CVE-2025-66906	Cross Site Request Forgery (CSRF) vulnerability in Turms Admin API thru v0.10.0-SNAPSHOT allows attackers to gain escalated privileges.	6.1	More Details
CVE-2025-65790	A reflected cross-site scripting (XSS) vulnerability exists in FuguHub 8.1 when serving SVG files through the /fs/ file manager interface. FuguHub does not sanitize or restrict script execution inside SVG content. When a victim opens a crafted SVG containing an inline <script> element, the browser executes the attacker-controlled JavaScript.	6.1	More Details
CVE-	CMSimple 5.4 contains a cross-site scripting vulnerability that allows attackers to bypass input filtering by using HTML		More

2021-47733	to Unicode encoding. Attackers can inject malicious scripts by encoding payloads like ')-alert(1)// and execute arbitrary JavaScript when victims interact with delete buttons.	6.1	Details
CVE-2025-67794	An issue was discovered in DriveLock 24.1 through 24.1.*, 24.2 before 24.2.8, and 25.1 before 25.1.6. Directories and files created by the agent are created with overly permissive ACLs, allowing local users without administrator rights to trigger actions or destabilize the agent.	6.1	More Details
CVE-2024-25812	MyNET up to v26.05 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the src parameter.	6.1	More Details
CVE-2025-34440	AVideo versions prior to 20.1 contain an open redirect vulnerability caused by insufficient validation of the siteRedirectUri parameter during user registration. Attackers can redirect users to external sites, facilitating phishing attacks.	6.1	More Details
CVE-2024-25814	MyNET up to v26.05 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the msg parameter.	6.1	More Details
CVE-2025-65233	Reflected cross-site scripting (XSS) in SLiMS (slims9_bulian) before 9.6.0 via improper handling of $_SERVER['PHP_SELF'] in index.php/sysconfig.inc.php, which allows remote attackers to execute arbitrary JavaScript in a victim's browser by supplying a crafted URL path.	6.1	More Details
CVE-2025-65270	Reflected cross-site scripting (XSS) vulnerability in ClinCapture EDC 3.0 and 2.2.3, allowing an unauthenticated remote attacker to execute JavaScript code in the context of the victim's browser.	6.1	More Details
CVE-2025-67163	A stored cross-site scripting (XSS) vulnerability in Simple Machines Forum v2.1.6 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Forum Name parameter.	6.1	More Details
CVE-2025-67170	A reflected cross-site scripting (XSS) vulnerability in RiteCMS v3.1.0 allows attackers to execute arbitrary code in the context of a user's browser via a crafted payload.	6.1	More Details
CVE-2025-66910	Turms Server v0.10.0-SNAPSHOT and earlier contains a plaintext password storage vulnerability in the administrator authentication system. The BaseAdminService class caches administrator passwords in plaintext within AdminInfo objects to optimize authentication performance. Upon successful login, raw passwords are stored unencrypted in memory in the rawPassword field. Attackers with local system access can extract these passwords through memory dumps, heap analysis, or debugger attachment, bypassing bcrypt protection.	6.0	More Details
CVE-2025-49918	Insertion of Sensitive Information Into Sent Data vulnerability in e4jvikwp VikBooking Hotel Booking Engine & PMS vikbooking allows Retrieve Embedded Sensitive Data.This issue affects VikBooking Hotel Booking Engine & PMS: from n/a through <= 1.8.2.	5.9	More Details
CVE-2025-68481	FastAPI Users allows users to quickly add a registration and authentication system to their FastAPI project. Prior to version 15.0.2, the OAuth login state tokens are completely stateless and carry no per-request entropy or any data that could link them to the session that initiated the OAuth flow. `generate_state_token()` is always called with an empty `state_data` dict, so the resulting JWT only contains the fixed audience claim plus an expiration timestamp. On callback, the library merely checks that the JWT verifies under `state_secret` and is unexpired; there is no attempt to match the state value to the browser that initiated the OAuth request, no correlation cookie, and no server-side cache. Any attacker can hit `/authorize`, capture the server-generated state, finish the upstream OAuth flow with their own provider account, and then trick a victim into loading `.../callback?code=<attacker_code>&state=<attacker_state>`. Because the state JWT is valid for any client for \~1 hour, the victim’s browser will complete the flow. This leads to login CSRF. Depending on the app’s logic, the login CSRF can lead to an account takeover of the victim account or to the victim user getting logged in to the attacker's account. Version 15.0.2 contains a patch for the issue.	5.9	More Details
CVE-2025-49919	Insertion of Sensitive Information Into Sent Data vulnerability in WPCenter eRoom eroom-zoom-meetings-webinar allows Retrieve Embedded Sensitive Data.This issue affects eRoom: from n/a through <= 1.5.6.	5.8	More Details
CVE-2021-47734	CMSimple 5.4 contains an authenticated local file inclusion vulnerability that allows remote attackers to manipulate PHP session files and execute arbitrary code. Attackers can leverage the vulnerability by changing the functions file path and uploading malicious PHP code through session file upload mechanisms.	5.5	More Details
CVE-2025-14721	The Responsive and Swipe slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's rsSlider shortcode in all versions up to, and including, 1.0.2 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.	5.5	More Details
CVE-2025-46292	This issue was addressed with additional entitlement checks. This issue is fixed in iOS 26.2 and iPadOS 26.2, iOS 18.7.3 and iPadOS 18.7.3. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2025-14965	A vulnerability was found in 1541492390c yougou-mall up to 0a771fa817c924efe52c8fe0a9a6658eee675f9f. This impacts the function Upload of the file src/main/java/per/ccm/ygmall/extra/controller/ResourceController.java. Performing manipulation results in path traversal. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	5.5	More Details

CVE-2025-46283	A logic issue was addressed with improved validation. This issue is fixed in macOS Tahoe 26.2. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-46288	A permissions issue was addressed with additional restrictions. This issue is fixed in visionOS 26.2, iOS 26.2 and iPadOS 26.2, watchOS 26.2, macOS Tahoe 26.2. An app may be able to access sensitive payment tokens.	5.5	More Details
CVE-2025-59529	Avahi is a system which facilitates service discovery on a local network via the mDNS/DNS-SD protocol suite. In versions up to and including 0.9-rc2, the simple protocol server ignores the documented client limit and accepts unlimited connections, allowing for easy local DoS. Although \`CLIENTS_MAX\` is defined, \`server_work()\` unconditionally \`accept()\`s and \`client_new()\` always appends the new client and increments \`n_clients\`. There is no check against the limit. When client cannot be accepted as a result of maximal socket number of avahi-daemon, it logs unconditionally error per each connection. Unprivileged local users can exhaust daemon memory and file descriptors, causing a denial of service system-wide for mDNS/DNS-SD. Exhausting local file descriptors causes increased system load caused by logging errors of each of request. Overloading prevents glibc calls using nss-mdns plugins to resolve \`*.local.\` names and link-local addresses. As of time of publication, no known patched versions are available, but a candidate fix is available in pull request 808, and some workarounds are available. Simple clients are offered for nss-mdns package functionality. It is not possible to disable the unix socket \`/run/avahi-daemon/socket\`, but resolution requests received via DBus are not affected directly. Tools avahi-resolve, avahi-resolve-address and avahi-resolve-host-name are not affected, they use DBus interface. It is possible to change permissions of unix socket after avahi-daemon is started. But avahi-daemon does not provide any configuration for it. Additional access restrictions like SELinux can also prevent unwanted tools to access the socket and keep resolution working for trusted users.	5.5	More Details
CVE-2025-46282	The issue was addressed with additional permissions checks. This issue is fixed in macOS Tahoe 26.2, Safari 26.2. An app may be able to access sensitive user data.	5.5	More Details
CVE-2025-43514	The issue was addressed with improved handling of caches. This issue is fixed in macOS Tahoe 26.2. An app may be able to access protected user data.	5.5	More Details
CVE-2025-46278	The issue was addressed with improved handling of caches. This issue is fixed in macOS Tahoe 26.2. An app may be able to access protected user data.	5.5	More Details
CVE-2025-43475	A logging issue was addressed with improved data redaction. This issue is fixed in iOS 26.2 and iPadOS 26.2. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2023-53916	Zenphoto 1.6 contains a stored cross-site scripting vulnerability in the user postal code field accessible through the admin-users.php interface. When administrators view user information imported as HTML, malicious JavaScript payloads injected into the postal code field execute in their browser context.	5.4	More Details
CVE-2024-58318	A stored cross-site scripting vulnerability in Kentico Xperience allows attackers to inject malicious scripts via the rich text editor component for page and form builders. Attackers can exploit this vulnerability by entering malicious URIs, potentially allowing malicious scripts to execute in users' browsers.	5.4	More Details
CVE-2023-53910	WBCE CMS 1.6.1 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious JavaScript by inserting script tags into page content through the WYSIWYG editor. Attackers can submit POST requests to /wbce/modules/wysiwyg/save.php with malicious script content in the content parameter to execute JavaScript when users view the affected page.	5.4	More Details
CVE-2025-14889	A security flaw has been discovered in Campcodes Advanced Voting Management System 1.0. The impacted element is an unknown function of the file /admin/voters_edit.php of the component Password Handler. Performing manipulation of the argument ID results in improper authorization. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.	5.4	More Details
CVE-2025-1885	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Restajet Information Technologies Inc. Online Food Delivery System allows Phishing, Forceful Browsing.This issue affects Online Food Delivery System: through 19122025.	5.4	More Details
CVE-2025-65837	PublicCMS V5.202506.b is vulnerable to Cross Site Scripting (XSS) in the Content Search module.	5.4	More Details
CVE-2023-53915	Zenphoto 1.6 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by inserting HTML content into album descriptions. Attackers can create albums with malicious iframe or script tags in the description field that execute when users view the album page.	5.4	More Details
CVE-2025-14455	The Image Photo Gallery Final Tiles Grid plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.6.7. This is due to the plugin not properly verifying that a user is authorized to perform actions on gallery management functions. This makes it possible for authenticated attackers, with Contributor-level access and above, to delete, modify, or clone galleries created by any user, including administrators.	5.4	More Details
CVE-2023-53938	RockMongo 1.1.7 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts through multiple unencoded input parameters. Attackers can exploit the vulnerability by submitting crafted payloads in database, collection, and login parameters to execute arbitrary JavaScript in victim's browser.	5.4	More Details

CVE-2021-47716	Orangescrum 1.8.0 contains multiple cross-site scripting vulnerabilities that allow authenticated attackers to inject malicious scripts through various input parameters. Attackers can exploit parameters like 'projid', 'CS_message', and 'name' to execute arbitrary JavaScript code in victim's browsers by submitting crafted payloads through application endpoints.	5.4	More Details
CVE-2025-67875	ChurchCRM is an open-source church management system. A privilege escalation vulnerability exists in ChurchCRM prior to version 6.5.3. An authenticated user with specific mid-level permissions ("Edit Records" and "Manage Properties and Classifications") can inject a persistent Cross-Site Scripting (XSS) payload into an administrator's profile. The payload executes when the administrator views their own profile page, allowing the attacker to hijack the administrator's session, perform administrative actions, and achieve a full account takeover. This vulnerability is a combination of two separate flaws: an Insecure Direct Object Reference (IDOR) that allows any user to view any other user's profile, and a Broken Access Control vulnerability that allows a user with general edit permissions to modify any other user's record properties. Version 6.5.3 fixes the issue.	5.4	More Details
CVE-2025-67876	ChurchCRM is an open-source church management system. A stored cross-site scripting (XSS) vulnerability exists in ChurchCRM versions 6.4.0 and prior that allows a low-privilege user with the “Manage Groups” permission to inject persistent JavaScript into group role names. The payload is saved in the database and executed whenever any user (including administrators) views a page that displays that role, such as GroupView.php or PersonView.php. This allows full session hijacking and account takeover. As of time of publication, no known patched versions are available.	5.4	More Details
CVE-2023-53936	Cameleon CMS 2.7.4 contains a persistent cross-site scripting vulnerability that allows authenticated administrators to inject malicious scripts into post titles. Attackers can create posts with embedded SVG scripts that execute when other users mouse over the post title, potentially stealing session cookies and executing arbitrary JavaScript.	5.4	More Details
CVE-2023-53909	WBCE CMS 1.6.1 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious JavaScript by uploading crafted SVG files through the media manager. Attackers can upload SVG files containing script tags to the /wbce/modules/elfinder/ef/php/connector.wbce.php endpoint and execute JavaScript when victims access the uploaded file.	5.4	More Details
CVE-2023-53918	PodcastGenerator 3.2.9 contains a stored cross-site scripting vulnerability in the episode title field accessible through the episodes upload interface (episodes_upload.php). Malicious JavaScript payloads injected into episode titles execute when administrators view the episodes list page (episodes_list.php).	5.4	More Details
CVE-2023-53939	TinyWebGallery v2.5 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through the folder name parameter. Attackers can edit album folder names with script tags to execute arbitrary JavaScript when other users view the affected gallery pages.	5.4	More Details
CVE-2022-50681	A reflected cross-site scripting vulnerability in Kentico Xperience allows attackers to inject malicious scripts via administration input fields in the Rich text editor component. Attackers can exploit this vulnerability to execute arbitrary scripts in users' browsers.	5.4	More Details
CVE-2025-62961	Missing Authorization vulnerability in Sparkle WP Sparkle FSE allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sparkle FSE: from n/a through 1.0.9.	5.4	More Details
CVE-2025-63947	A Reflected Cross-Site Scripting (XSS) vulnerability exists in phpMsAdmin version 2.2 in the database_mode.php file. An attacker can execute arbitrary web script or HTML via the dbname parameter after a user is authenticated.	5.4	More Details
CVE-2021-47737	CSZ CMS 1.2.7 contains an HTML injection vulnerability that allows authenticated users to insert malicious hyperlinks in message titles. Attackers can craft POST requests to the member messaging system with HTML-based links to potentially conduct phishing or social engineering attacks.	5.4	More Details
CVE-2023-25445	Missing Authorization vulnerability in HappyFiles HappyFiles Pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects HappyFiles Pro: from n/a through 1.8.1.	5.4	More Details
CVE-2023-53931	Revive Adserver 5.4.1 contains a cross-site scripting vulnerability in the banner advanced configuration page that allows attackers to inject malicious scripts. Attackers can craft a malicious link to the banner-advanced.php endpoint with XSS payloads in prepend and append parameters to execute arbitrary JavaScript when an admin views the page.	5.4	More Details
CVE-2025-14298	The FiboSearch – Ajax Search for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `thegem_te_search` shortcode in all versions up to, and including, 1.32.0 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. This vulnerability requires TheGem theme (premium) to be installed with Header Builder mode enabled, and the FiboSearch "Replace search bars" option enabled for TheGem integration.	5.4	More Details
CVE-2025-63948	A SQL Injection vulnerability exists in phpMsAdmin version 2.2 in the database_mode.php file. An attacker can execute arbitrary SQL commands via the dbname parameter, potentially leading to information disclosure or database manipulation.	5.4	More Details
CVE-2024-58319	A reflected cross-site scripting vulnerability in Kentico Xperience allows attackers to inject malicious scripts via the Pages dashboard widget configuration dialog. Attackers can exploit this vulnerability to execute malicious scripts in administrative users' browsers.	5.4	More Details
CVE-2023-	PHPFusion 9.10.30 contains a stored cross-site scripting vulnerability in the file manager that allows attackers to upload malicious SVG files with embedded JavaScript. Attackers can upload SVG files with script tags that execute arbitrary	5.4	More Details

53928	JavaScript when viewed, potentially stealing user session information or performing client-side attacks.		
CVE-2023-53925	UliCMS 2023.1 contains a stored cross-site scripting vulnerability that allows attackers to upload malicious SVG files with embedded JavaScript. Attackers can upload crafted SVG files through the file management interface that execute arbitrary scripts when viewed by other users.	5.4	More Details
CVE-2025-62960	Missing Authorization vulnerability in Sparkle WP Construction Light allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Construction Light: from n/a through 1.6.7.	5.4	More Details
CVE-2025-68399	ChurchCRM is an open-source church management system. In versions prior to 6.5.4, there is a Stored Cross-Site Scripting (XSS) vulnerability within the GroupEditor.php page of the application. When a user attempts to create a group role, they can execute malicious JavaScript. However, for this to work, the user must have permission to view and modify groups in the application. Version 6.5.4 fixes the issue.	5.4	More Details
CVE-2025-14734	The Amazon affiliate lite Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing or incorrect nonce validation on the 'ADAL_settings_page' function. This makes it possible for unauthenticated attackers to update plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2023-53935	WBiz Desk 1.2 contains a SQL injection vulnerability that allows non-admin users to manipulate database queries through the 'tk' parameter in ticket.php. Attackers can inject crafted SQL statements using UNION-based techniques to extract sensitive database information by sending malformed requests to the ticket endpoint.	5.4	More Details
CVE-2025-14760	Missing cryptographic key commitment in the AWS SDK for C++ may allow a user with write access to the S3 bucket to introduce a new EDK that decrypts to different plaintext when the encrypted data key is stored in an "instruction file" instead of S3's metadata record. To mitigate this issue, upgrade AWS SDK for C++ to version 1.11.712 or later	5.3	More Details
CVE-2025-67789	An issue was discovered in DriveLock 24.1 before 24.1.6, 24.2 before 24.2.7, and 25.1 before 25.1.5. Authenticated users can retrieve the computer count of other DriveLock tenants via the DriveLock API.	5.3	More Details
CVE-2025-14759	Missing cryptographic key commitment in the Amazon S3 Encryption Client for .NET may allow a user with write access to the S3 bucket to introduce a new EDK that decrypts to different plaintext when the encrypted data key is stored in an "instruction file" instead of S3's metadata record. To mitigate this issue, upgrade Amazon S3 Encryption Client for .NET to version 3.2.0 or later.	5.3	More Details
CVE-2025-14958	A security flaw has been discovered in floooh sokol up to 33e2271c431bf21de001e972f72da17a984da932. This vulnerability affects the function _sg_pipeline_common_init in the library sokol_gfx.h. Performing manipulation results in heap-based buffer overflow. The attack needs to be approached locally. The exploit has been released to the public and may be exploited. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The patch is named 33e2271c431bf21de001e972f72da17a984da932. It is suggested to install a patch to address this issue.	5.3	More Details
CVE-2025-14956	A vulnerability was determined in WebAssembly Binaryen up to 125. Affected by this issue is the function WasmBinaryReader::readExport of the file src/wasm/wasm-binary.cpp. This manipulation causes heap-based buffer overflow. It is possible to launch the attack on the local host. The exploit has been publicly disclosed and may be utilized. Patch name: 4f52bff8c4075b5630422f902dd92a0af2c9f398. It is recommended to apply a patch to fix this issue.	5.3	More Details
CVE-2021-47715	Hasura GraphQL 1.3.3 contains a server-side request forgery vulnerability that allows attackers to inject arbitrary remote schema URLs through the add_remote_schema endpoint. Attackers can exploit the vulnerability by sending crafted POST requests to the /v1/query endpoint with malicious URL definitions to potentially access internal network resources.	5.3	More Details
CVE-2025-14080	The Frontend Post Submission Manager Lite plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.2.5. This is due to missing authorization checks on the post update functionality in the fpsml_form_process AJAX action. This makes it possible for unauthenticated attackers to modify arbitrary posts by providing a post_id parameter via the guest posting form, allowing them to change post titles, content, excerpts, and remove post authors.	5.3	More Details
CVE-2025-14761	Missing cryptographic key commitment in the AWS SDK for PHP may allow a user with write access to the S3 bucket to introduce a new EDK that decrypts to different plaintext when the encrypted data key is stored in an "instruction file" instead of S3's metadata record. To mitigate this issue, upgrade AWS SDK for PHP to version 3.368.0 or later	5.3	More Details
CVE-2025-67168	RiteCMS v3.1.0 was discovered to use insecure encryption to store passwords.	5.3	More Details
CVE-2025-14043	The Tainacan plugin for WordPress is vulnerable to unauthorized metadata section creation due to missing authorization checks in all versions up to, and including, 1.0.1. This is due to the \`create_item_permissions_check()\` function unconditionally returning true, which bypasses authentication and authorization validation. This makes it possible for unauthenticated attackers to create arbitrary metadata sections for any collection via the public REST API granted they can access the WordPress site.	5.3	More Details
CVE-2023-52210	Vulnerability in Tyche softwares Product Delivery Date for WooCommerce – Lite.This issue affects Product Delivery Date for WooCommerce – Lite: from n/a through 2.7.0.	5.3	More Details

CVE-2025-68480	Marshmallow is a lightweight library for converting complex objects to and from simple Python datatypes. In versions from 3.0.0rc1 to before 3.26.2 and from 4.0.0 to before 4.1.2, Schema.load(data, many=True) is vulnerable to denial of service attacks. A moderately sized request can consume a disproportionate amount of CPU time. This issue has been patched in version 3.26.2 and 4.1.2.	5.3	More Details
CVE-2024-29370	In python-jose 3.3.0 (specifically jwe.decrypt), a vulnerability allows an attacker to cause a Denial-of-Service (DoS) condition by crafting a malicious JSON Web Encryption (JWE) token with an exceptionally high compression ratio. When this token is processed by the server, it results in significant memory allocation and processing time during decompression.	5.3	More Details
CVE-2025-12820	The Pure WC Variation Swatches WordPress plugin through 1.1.7 does not have an authorization check when updating its settings, which could allow any authenticated users to update them.	5.3	More Details
CVE-2025-14633	The F70 Lead Document Download plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'file_download' function in all versions up to, and including, 1.4.4. This makes it possible for unauthenticated attackers to download any file from the WordPress media library by guessing or enumerating WordPress attachment IDs.	5.3	More Details
CVE-2025-68556	Missing Authorization vulnerability in VillaTheme HAPPY allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects HAPPY: from n/a through 1.0.9.	5.3	More Details
CVE-2025-14061	The Cookie Banner, Cookie Consent, Consent Log, Cookie Scanner, Script Blocker (for GDPR, CCPA & ePrivacy) : WP Cookie Consent plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability check on the gdpr_delete_policy_data function in all versions up to, and including, 4.0.7. This makes it possible for unauthenticated attackers to permanently delete arbitrary posts, pages, attachments, and other post types by ID.	5.3	More Details
CVE-2025-14764	Missing cryptographic key commitment in the Amazon S3 Encryption Client for Go may allow a user with write access to the S3 bucket to introduce a new EDK that decrypts to different plaintext when the encrypted data key is stored in an "instruction file" instead of S3's metadata record. To mitigate this issue, upgrade Amazon S3 Encryption Client for Go to version 4.0 or later.	5.3	More Details
CVE-2025-14763	Missing cryptographic key commitment in the Amazon S3 Encryption Client for Java may allow a user with write access to the S3 bucket to introduce a new EDK that decrypts to different plaintext when the encrypted data key is stored in an "instruction file" instead of S3's metadata record. To mitigate this issue, upgrade Amazon S3 Encryption Client for Java to version 4.0.0 or later.	5.3	More Details
CVE-2025-15013	A vulnerability was identified in floooh sokol up to 5d11344150973f15e16d3ec4ee7550a73fb995e0. The impacted element is the function _sg_validate_pipeline_desc in the library sokol_gfx.h. Such manipulation leads to stack-based buffer overflow. The attack must be carried out locally. The exploit is publicly available and might be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The name of the patch is b95c5245ba357967220c9a860c7578a7487937b0. It is best practice to apply a patch to resolve this issue.	5.3	More Details
CVE-2025-14155	The Premium Addons for Elementor – Powerful Elementor Templates & Widgets plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'get_template_content' function in all versions up to, and including, 4.11.53. This makes it possible for unauthenticated attackers to view the content of private, draft, and pending templates.	5.3	More Details
CVE-2023-53961	SOUND4 IMPACT/FIRST/PULSE/Eco v2.x contains a cross-site request forgery vulnerability that allows attackers to perform administrative actions without user consent. Attackers can craft malicious web pages that submit HTTP requests to the radio processing interface, triggering unintended administrative operations when a logged-in user visits the page.	5.3	More Details
CVE-2025-14762	Missing cryptographic key commitment in the AWS SDK for Ruby may allow a user with write access to the S3 bucket to introduce a new EDK that decrypts to different plaintext when the encrypted data key is stored in an "instruction file" instead of S3's metadata record. To mitigate this issue, upgrade AWS SDK for Ruby to version 1.208.0 or later.	5.3	More Details
CVE-2025-12898	The Pretty Google Calendar plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the pgcal_ajax_handler() function in all versions up to, and including, 2.0.0. This makes it possible for unauthenticated attackers to retrieve the Google API key set in the plugin's settings.	5.3	More Details
CVE-2025-14874	A flaw was found in Nodemailer. This vulnerability allows a denial of service (DoS) via a crafted email address header that triggers infinite recursion in the address parser.	5.3	More Details
CVE-2025-12492	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.11.0 via the ajax_get_members function. This is due to the use of a predictable low-entropy token (5 hex characters derived from md5 of post ID) to identify member directories and insufficient authorization checks on the unauthenticated AJAX endpoint. This makes it possible for unauthenticated attackers to extract sensitive data including usernames, display names, user roles (including administrator accounts), profile URLs, and user IDs by enumerating predictable directory_id values or brute-forcing the small 16^5 token space.	5.3	More Details
	Turms AI-Serving module v0.10.0-SNAPSHOT and earlier contains an improper file type validation vulnerability in the OCR image upload functionality. The OcrController in turms-ai-serving/src/main/java/im/turms/ai/domain/ocr/controller/OcrController.java uses the @FormData(contentType =		

CVE-2025-66908	MediaTypeConst.IMAGE) annotation to restrict uploads to image files, but this constraint is not properly enforced. The system relies solely on client-provided Content-Type headers and file extensions without validating actual file content using magic bytes (file signatures). An attacker can upload arbitrary file types including executables, scripts, HTML, or web shells by setting the Content-Type header to "image/*" or using an image file extension. This bypass enables potential server-side code execution, stored XSS, or information disclosure depending on how uploaded files are processed and served.	5.3	More Details
CVE-2025-59949	FreshRSS is a free, self-hostable RSS aggregator. Versions prior to 1.27.1 have a logout cross-site request forgery vulnerability that can lead to denial of service via <track src>. Version 1.27.1 patches the issue.	5.3	More Details
CVE-2025-66498	A memory corruption vulnerability exists in the 3D annotation handling of Foxit PDF Reader due to insufficient bounds checking when parsing U3D data. When opening a PDF file containing malformed or specially crafted PRC content, out-of-bounds memory access may occur, resulting in memory corruption.	5.3	More Details
CVE-2025-66497	A memory corruption vulnerability exists in the 3D annotation handling of Foxit PDF Reader due to insufficient bounds checking when parsing PRC data. When opening a PDF file containing malformed or specially crafted PRC content, out-of-bounds memory access may occur, resulting in memory corruption.	5.3	More Details
CVE-2024-58320	An information disclosure vulnerability in Kentico Xperience allows public users to access sensitive administration interface hostname details during authentication. Attackers can retrieve confidential hostname configuration information through a public endpoint, potentially exposing internal network details.	5.3	More Details
CVE-2024-58317	A cookie security configuration vulnerability in Kentico Xperience allows attackers to bypass SSL requirements when setting administration cookies via web.config. The vulnerability affects .NET Framework projects by incorrectly handling the 'requireSSL' attribute, potentially compromising session security and authentication state.	5.3	More Details
CVE-2023-53943	GLPI 9.5.7 contains a username enumeration vulnerability in the lost password recovery mechanism that allows attackers to validate email addresses. Attackers can systematically test email addresses by submitting requests to the password reset endpoint and analyzing response differences to identify valid user accounts.	5.3	More Details
CVE-2025-66496	A memory corruption vulnerability exists in the 3D annotation handling of Foxit PDF Reader due to insufficient bounds checking when parsing PRC data. When opening a PDF file containing malformed or specially crafted PRC content, out-of-bounds memory access may occur, resulting in memory corruption.	5.3	More Details
CVE-2025-13754	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.6.9.16. This is due to the plugin exposing its admin embed endpoint at `/wp-json/ssa/v1/embed-inner-admin` without authentication, which leaks plugin settings including staff names, business names, and configuration data that are not publicly displayed on the booking form. This makes it possible for unauthenticated attackers to extract private business configuration. In premium versions with integrations configured, this might also expose other sensitive data including API keys for external services.	5.3	More Details
CVE-2022-50686	An information disclosure vulnerability in Kentico Xperience allows attackers to view sensitive stack trace details via Portal Engine form control error messages. Detailed error messages can expose internal system information and potentially reveal implementation details to unauthorized users.	5.3	More Details
CVE-2025-54743	Missing Authorization vulnerability in mkscripts Download After Email download-after-email allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Download After Email: from n/a through 2.1.5-2.1.6.	5.3	More Details
CVE-2019-25228	An information disclosure vulnerability in Kentico Xperience allows attackers to leak virtual context URLs via the HTTP Referer header when users interact with third-party domains. Sensitive virtual context information can be exposed to external domains through page builder interactions and link/image loading.	5.3	More Details
CVE-2025-68388	Allocation of resources without limits or throttling (CWE-770) allows an unauthenticated remote attacker to cause excessive allocation (CAPEC-130) of memory and CPU via the integration of malicious IPv4 fragments, leading to a degradation in Packetbeat.	5.3	More Details
CVE-2025-63043	Authorization Bypass Through User-Controlled Key vulnerability in PickPlugins Post Grid and Gutenberg Blocks allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Post Grid and Gutenberg Blocks: from n/a through 2.3.19.	5.3	More Details
CVE-2025-65000	SSH private keys of the "Remote alert handlers (Linux)" rule were exposed in the rule page's HTML source in Checkmk <= 2.4.0p18 and all versions of Checkmk 2.3.0. This potentially allowed unauthorized triggering of predefined alert handlers on hosts where the handler was deployed.	5.3	More Details
CVE-2025-14823	In deployments using the ScreenConnect™ Certificate Signing Extension, encrypted configuration values including an Azure Key Vault-related key, could be returned to unauthenticated users through a client-facing endpoint under certain conditions. The values remained encrypted and securely stored at rest; however, an encrypted representation could be exposed in client responses. Updating the Certificate Signing Extension to version 1.0.12 or higher ensures configuration handling occurs exclusively on the server side, preventing encrypted values from being transmitted to or rendered by client-side components.	5.3	More Details
CVE-2025-63390	An authentication bypass vulnerability exists in AnythingLLM v1.8.5 in via the /api/workspaces endpoint. The endpoint fails to implement proper authentication checks, allowing unauthenticated remote attackers to enumerate and retrieve detailed information about all configured workspaces. Exposed data includes: workspace identifiers (id, name, slug), AI model configurations (chatProvider, chatModel, agentProvider), system prompts (openAiPrompt), operational parameters (temperature, history length, similarity thresholds), vector search settings, chat modes, and timestamps.	5.3	More Details

CVE-2025-63002	Missing Authorization vulnerability in wpforchurch Sermon Manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sermon Manager: from n/a through 2.30.0.	5.3	More Details
CVE-2025-11009	Cleartext Storage of Sensitive Information vulnerability in Mitsubishi Electric GT Designer3 Version1 (GOT2000) all versions and Mitsubishi Electric GT Designer3 Version1 (GOT1000) all versions allows a local unauthenticated attacker to obtain plaintext credentials from the project file for GT Designer3. This could allow the attacker to operate illegally GOT2000 series or GOT1000 series by using the obtained credentials.	5.1	More Details
CVE-2025-62998	Insertion of Sensitive Information Into Sent Data vulnerability in WP Messiah WP AI CoPilot allows Retrieve Embedded Sensitive Data.This issue affects WP AI CoPilot: from n/a through 1.2.7.	5.0	More Details
CVE-2025-67844	The GitHub Integration API in Mintlify Platform before 2025-11-15 allows remote attackers to obtain sensitive repository metadata via the repository owner and name fields. It fails to validate that the repository owner and name fields provided during configuration belong to the specific GitHub App Installation ID associated with the user's organization.	5.0	More Details
CVE-2025-68463	Bio.Entrez in Biopython through 186 allows doctype XXE.	4.9	More Details
CVE-2025-67846	The Deployment Infrastructure in Mintlify Platform before 2025-11-15 allows remote attackers to bypass security patches and execute downgrade attacks via predictable deployment identifiers on the Vercel preview domain. An attacker can identify the URL structure of a previous deployment that contains unpatched vulnerabilities. By browsing directly to the specific git-ref or deployment-id subdomain, the attacker can force the application to load the vulnerable version.	4.9	More Details
CVE-2025-68390	Allocation of Resources Without Limits or Throttling (CWE-770) in Elasticsearch can allow an authenticated user with snapshot restore privileges to cause Excessive Allocation (CAPEC-130) of memory and a denial of service (DoS) via crafted HTTP request.	4.9	More Details
CVE-2025-12496	The Zephyr Project Manager plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 3.3.203 via the \`file\` parameter. This makes it possible for authenticated attackers, with Custom-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information. On a servers that have \`allow_url_fopen\` enabled, this issue allows for Server-Side Request Forgery	4.9	More Details
CVE-2025-14946	A flaw was found in libnbd. A malicious actor could exploit this by convincing libnbd to open a specially crafted Uniform Resource Identifier (URI). This vulnerability arises because non-standard hostnames starting with '-o' are incorrectly interpreted as arguments to the Secure Shell (SSH) process, rather than as hostnames. This could lead to arbitrary code execution with the privileges of the user running libnbd.	4.8	More Details
CVE-2025-68275	ChurchCRM is an open-source church management system. Versions prior to 6.5.3 have a stored cross-site scripting vulnerability on the pages \`View Active People\`, \`View Inactive people\`, and \`View All People\`. Version 6.5.3 fixes the issue.	4.8	More Details
CVE-2025-67873	Capstone is a disassembly framework. In versions 6.0.0-Alpha5 and prior, Skipdata length is not bounds-checked, so a user-provided skipdata callback can make cs_disasm/cs_disasm_iter memcpy more than 24 bytes into cs_insn.bytes, causing a heap buffer overflow in the disassembly path. Commit cbef767ab33b82166d263895f24084b75b316df3 fixes the issue.	4.8	More Details
CVE-2025-68114	Capstone is a disassembly framework. In versions 6.0.0-Alpha5 and prior, an unchecked vsnprintf return in SStream_concat lets a malicious cs_opt_mem.vsnprintf drive SStream’s index negative or past the end, leading to a stack buffer underflow/overflow when the next write occurs. Commit 2c7797182a1618be12017d7d41e0b6581d5d529e fixes the issue.	4.8	More Details
CVE-2025-68401	ChurchCRM is an open-source church management system. Prior to version 6.0.0, the application stores user-supplied HTML/JS without sufficient sanitization/encoding. When other users later view this content, attacker-controlled JavaScript executes in their browser (stored XSS). In affected contexts the script can access web origin data and perform privileged actions as the victim. Where session cookies are not marked HttpOnly, the script can read document.cookie, enabling session theft and account takeover. Version 6.0.0 patches the issue.	4.8	More Details
CVE-2025-14899	A weakness has been identified in CodeAstro Real Estate Management System 1.0. This impacts an unknown function of the file /admin/stateadd.php of the component Administrator Endpoint. This manipulation causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	4.7	More Details
CVE-2025-14898	A security flaw has been discovered in CodeAstro Real Estate Management System 1.0. This affects an unknown function of the file /admin/userbuilderdelete.php of the component Administrator Endpoint. The manipulation results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	4.7	More Details
CVE-2025-59849	Improper management of Content Security Policy in HCL BigFix Remote Control Lite Web Portal (versions 10.1.0.0326 and lower) may allow the execution of malicious code in web pages.	4.7	More Details
CVE-2025-14900	A security vulnerability has been detected in CodeAstro Real Estate Management System 1.0. Affected is an unknown function of the file /admin/userdelete.php of the component Administrator Endpoint. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	4.7	More Details

CVE-2025-15003	A vulnerability was found in SeaCMS up to 13.3. The impacted element is an unknown function of the file admin_video.php. Performing manipulation of the argument e_id results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	4.7	More Details
CVE-2025-14966	A vulnerability was determined in FastAdmin up to 1.7.0.20250506. Affected is the function selectpage of the file application/common/controller/Backend.php of the component Backend Controller. Executing manipulation of the argument custom/searchField can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2025-14897	A vulnerability was identified in CodeAstro Real Estate Management System 1.0. The impacted element is an unknown function of the file /admin/useragentdelete.php of the component Administrator Endpoint. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	4.7	More Details
CVE-2025-40891	A Stored HTML Injection vulnerability was discovered in the Time Machine Snapshot Diff functionality due to improper validation of network traffic data. An unauthenticated attacker can send specially crafted network packets at two different times to inject HTML tags into asset attributes across two snapshots. Exploitation requires a victim to use the Time Machine Snapshot Diff feature on those specific snapshots and perform specific GUI actions, at which point the injected HTML renders in their browser, enabling phishing and open redirect attacks. Full XSS exploitation is prevented by input validation and Content Security Policy. Attack complexity is high due to multiple required conditions.	4.7	More Details
CVE-2025-14939	A vulnerability was found in code-projects Online Appointment Booking System 1.0. Impacted is an unknown function of the file /admin/deletemanager.php. The manipulation of the argument managername results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	4.7	More Details
CVE-2025-26787	An error in the SignServer container startup logic was found in Keyfactor SignServer versions prior to 7.2. The Admin CLI command used to configure Certificate access to the initial startup of the container sets a property of "allowany" to allow any user with a valid and trusted client auth certificate to connect. Admins can then set more restricted access to specific certificates. A logic error caused this admin CLI command to be run on each restart of the container instead of only the first startup as intended resetting the configuration to "allowany".	4.7	More Details
CVE-2025-14837	A vulnerability has been found in ZZCMS 2025. Affected by this issue is the function stripfxg of the file /admin/siteconfig.php of the component Backend Website Settings Module. Such manipulation of the argument icp leads to code injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2025-67712	There is an HTML injection issue in Esri ArcGIS Web AppBuilder developer edition versions prior to 2.30 that allows a remote, unauthenticated attacker to potentially entice a user to click a link that causes arbitrary HTML to render in a victim's browser. There is no evidence of JavaScript execution, which limits the impact. At the time of submission, ArcGIS Web App Builder developer edition is retired and unsupported. ArcGIS Web App Builder 2.30 is not susceptible to this vulnerability.	4.7	More Details
CVE-2023-53906	projectSend r1605 contains a stored cross-site scripting vulnerability that allows authenticated administrators to inject malicious JavaScript through the custom assets configuration page. Attackers can craft a JavaScript payload in the custom assets section that will execute when other users load the affected page, enabling persistent script injection.	4.6	More Details
CVE-2024-58323	A stored cross-site scripting vulnerability in Kentico Xperience allows attackers to inject malicious scripts via the Checkbox form component. This allows malicious scripts to execute in users' browsers by exploiting HTML support in the form builder.	4.6	More Details
CVE-2024-58322	A stored cross-site scripting vulnerability in Kentico Xperience allows attackers to inject malicious code into shipping options configuration. This could lead to potential theft of sensitive data by executing malicious scripts in users' browsers.	4.6	More Details
CVE-2024-58321	A stored cross-site scripting vulnerability in Kentico Xperience allows attackers to inject malicious scripts via form validation rule configuration. Attackers can exploit this vulnerability to execute malicious scripts that will run in users' browsers.	4.6	More Details
CVE-2023-53738	A reflected cross-site scripting vulnerability in Kentico Xperience allows authenticated users to inject malicious scripts via page preview URLs. Attackers can exploit this vulnerability to execute arbitrary scripts in users' browsers during page preview interactions.	4.6	More Details
CVE-2023-53737	A stored cross-site scripting vulnerability in Kentico Xperience allows global administrators to inject malicious payloads via the Localization application. Attackers can execute scripts that could affect multiple parts of the administration interface.	4.6	More Details
CVE-2023-53736	A reflected cross-site scripting vulnerability in Kentico Xperience allows authenticated users to inject malicious scripts in the administration interface. Attackers can exploit this vulnerability to execute arbitrary scripts within the administrative context.	4.6	More Details
CVE-2022-50684	An HTML injection vulnerability in Kentico Xperience allows attackers to inject malicious HTML values into form submission emails via unencoded form fields. Unencoded form values could enable HTML content execution in recipient email clients, potentially compromising email security.	4.6	More Details
CVE-2022-50683	A stored cross-site scripting vulnerability in Kentico Xperience allows attackers to inject malicious scripts via form redirect URL configuration. This allows malicious scripts to execute in users' browsers through unvalidated form configuration settings.	4.6	More Details
CVE-	A stored cross-site scripting vulnerability in Kentico Xperience allows administration users to inject malicious scripts via		More

2022-50680	email marketing templates. Attackers can exploit this vulnerability to execute malicious scripts that could compromise user browsers and steal sensitive information.	4.6	Details
CVE-2020-36891	A stored cross-site scripting vulnerability in Kentico Xperience allows attackers to upload files with spoofed Content-Type that do not match file extensions. Attackers can exploit this vulnerability by uploading malicious files with manipulated MIME types, allowing malicious scripts to execute in users' browsers.	4.6	More Details
CVE-2020-36889	A stored cross-site scripting vulnerability in Kentico Xperience allows attackers to inject malicious scripts via error messages containing specially crafted object names. This allows malicious scripts to execute in users' browsers when administrators view error messages in the administration interface.	4.6	More Details
CVE-2023-53932	Serendipity 2.4.0 contains a stored cross-site scripting vulnerability that allows authenticated users to inject malicious scripts through blog entry creation. Attackers can craft entries with JavaScript payloads that will execute when other users view the compromised blog post.	4.6	More Details
CVE-2022-50685	A stored cross-site scripting vulnerability in Kentico Xperience allows authenticated users to inject malicious scripts via XML file uploads as page attachments or metafiles. Attackers can upload malicious XML files that enable stored XSS, allowing malicious scripts to execute in users' browsers.	4.6	More Details
CVE-2023-53920	PodcastGenerator 3.2.9 contains a stored cross-site scripting vulnerability in the podcast title field accessible through the podcast details interface (podcast_details.php). Malicious JavaScript payloads injected into the podcast title execute when users visit the application's home page.	4.6	More Details
CVE-2023-53904	Xenforo 2.2.13 contains a stored cross-site scripting vulnerability that allows authenticated administrators to inject malicious scripts through the smilie category title parameter. Attackers can create a smilie category with a malicious script that will execute when the admin panel is loaded, potentially enabling further client-side attacks.	4.6	More Details
CVE-2023-53911	Textpattern CMS 4.8.8 contains a stored cross-site scripting vulnerability in the article excerpt field that allows authenticated users to inject malicious scripts. Attackers can insert JavaScript payloads into the excerpt, which will execute when the article is viewed by other users.	4.6	More Details
CVE-2023-53919	PodcastGenerator 3.2.9 contains a stored cross-site scripting vulnerability in the Freebox content field accessible through the theme customization interface (theme_freebox.php). Malicious JavaScript payloads injected into the Freebox content execute when users visit the application's home page.	4.6	More Details
CVE-2025-14735	The "Amazon affiliate lite Plugin" plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with 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-2025-14054	The WC Builder – WooCommerce Page Builder for WPBakery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'heading_color' parameter (and multiple other styling parameters) of the `wpbforwpbakery_product_additional_information` shortcode in all versions up to, and including, 1.2.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details
CVE-2025-68386	Improper Authorization (CWE-285) in Kibana can lead to privilege escalation (CAPEC-233) by allowing an authenticated user to change a document's sharing type to "global," even though they do not have permission to do so, making it visible to everyone in the space via a crafted a HTTP request.	4.3	More Details
CVE-2025-14848	Advantech WebAccess/SCADA is vulnerable to absolute directory traversal, which may allow an attacker to determine the existence of arbitrary files.	4.3	More Details
CVE-2025-13498	The Download Manager plugin for WordPress is vulnerable to unauthorized access of sensitive information in all versions up to, and including, 3.3.32. This is due to missing authorization and capability checks on the `wpdm_media_access` AJAX action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve passwords and access control settings for protected media attachments, which can then be used to bypass the intended media protection and download restricted files.	4.3	More Details
CVE-2025-14081	The Ultimate Member plugin for WordPress is vulnerable to Profile Privacy Setting Bypass in all versions up to, and including, 2.11.0. This is due to a flaw in the secure fields mechanism where field keys are stored in the allowed fields list before the `required_perm` check is applied during rendering. This makes it possible for authenticated attackers with Subscriber-level access to modify their profile privacy settings (e.g., setting profile to "Only me") via direct parameter manipulation, even when the administrator has explicitly disabled the option for their role.	4.3	More Details
CVE-2025-64282	Authorization Bypass Through User-Controlled Key vulnerability in RadiusTheme Radius Blocks allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Radius Blocks: from n/a through 2.2.1.	4.3	More Details
CVE-2025-43501	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in Safari 26.2, iOS 18.7.3 and iPadOS 18.7.3, iOS 26.2 and iPadOS 26.2, macOS Tahoe 26.2, visionOS 26.2. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
	A vulnerability was detected in Edimax BR-6208AC 1.02. This impacts the function handle_retr of the component FTP Daemon Service. The manipulation results in path traversal. The attack may be launched remotely. The exploit is now public and may be used. Edimax confirms this issue: "This product is no longer available in the market and has been		

CVE-2025-14910	discontinued for five years. Consequently, Edimax no longer provides technical support, firmware updates, or security patches for this specific model. However, to ensure the safety of our remaining active users, we acknowledge this report and will take the following mitigation actions: (A) We will issue an official security advisory on our support website. (B) We will strongly advise users to disable the FTP service on this device to mitigate the reported risk, by which the product will still work for common use. (C) We will recommend users upgrade to newer, supported models." This vulnerability only affects products that are no longer supported by the maintainer.	4.3	More Details
CVE-2025-14909	A weakness has been identified in JeecgBoot up to 3.9.0. The impacted element is the function SysUserOnlineController of the file jeecg-boot/jeecg-module-system/jeecg-system-biz/src/main/java/org/jeecg/modules/system/controller/SysUserOnlineController.java. Executing manipulation can lead to manage user sessions. The attack can be launched remotely. The exploit has been made available to the public and could be exploited. This patch is called b686f9fbd1917edffe5922c6362c817a9361cfbd. Applying a patch is advised to resolve this issue.	4.3	More Details
CVE-2025-68422	Improper Authorization (CWE-285) in Kibana can lead to privilege escalation (CAPEC-233) by allowing an authenticated user to bypass intended permission restrictions via a crafted HTTP request. This allows an attacker who lacks the live queries - read permission to successfully retrieve the list of live queries.	4.3	More Details
CVE-2025-13110	The HUSKY – Products Filter Professional for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.3.7.3 via the "woof_add_subscr" function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber level access and above, to create product messenger subscriptions on behalf of arbitrary users, including administrators.	4.3	More Details
CVE-2025-62107	Cross-Site Request Forgery (CSRF) vulnerability in PluginOps Feather Login Page allows Cross Site Request Forgery.This issue affects Feather Login Page: from n/a through 1.1.7.	4.3	More Details
CVE-2025-62880	Cross-Site Request Forgery (CSRF) vulnerability in Kunal Nagar Custom 404 Pro allows Cross Site Request Forgery.This issue affects Custom 404 Pro: from n/a through 3.12.0.	4.3	More Details
CVE-2025-7733	The WP JobHunt plugin for WordPress, used by the JobCareer theme, is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 7.7 via the 'cs_update_application_status_callback' due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Candidate-level access and above, to send a site-generated email with injected HTML to any user.	4.3	More Details
CVE-2025-14618	The Sweet Energy Efficiency plugin for WordPress is vulnerable to unauthorized access, modification, and loss of data due to a missing capability check on the 'sweet_energy_efficiency_action' AJAX handler in all versions up to, and including, 1.0.6. This makes it possible for authenticated attackers, with subscriber level access and above, to read, modify, and delete arbitrary graphs.	4.3	More Details
CVE-2025-68557	Missing Authorization vulnerability in Vikas Ratudi Chakra test allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Chakra test: from n/a through 1.0.1.	4.3	More Details
CVE-2025-14277	The Prime Slider – Addons for Elementor plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.0.9 via the import_elementor_template AJAX action. This makes it possible for authenticated attackers, with subscriber level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	4.3	More Details
CVE-2025-14399	The Download Plugins and Themes in ZIP from Dashboard plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.9.6. This is due to missing or incorrect nonce validation on the download_plugin_bulk and download_theme_bulk functions. This makes it possible for unauthenticated attackers to archive all the sites plugins and themes and place them in the `wp-content/uploads/` directory 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-2025-14163	The Premium Addons for Elementor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.11.53. This is due to missing nonce validation in the 'insert_inner_template' function. This makes it possible for unauthenticated attackers to create arbitrary Elementor templates via a forged request granted they can trick a site administrator or other user with the edit_posts capability into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-14164	The Quran Gateway plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5. This is due to missing nonce validation in the quran_gateway_options function. This makes it possible for unauthenticated attackers to modify the plugin's display settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-12361	The myCred – Points Management System For Gamification, Ranks, Badges, and Loyalty Program plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 2.9.7.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve sensitive information including user IDs, display names, and email addresses of all users on the site via the get_bank_accounts AJAX action. Passwords are not exposed.	4.3	More Details
CVE-2025-62002	BullWall Ransomware Containment relies on the number of file modifications to trigger detection. An authenticated attacker could encrypt a single large file without triggering a detection alert. Versions 4.6.0.0, 4.6.0.6, 4.6.0.7, and 4.6.1.4 were confirmed to be affected; other versions before and after may also be affected.	4.3	More Details
CVE-2023-	Vulnerability in mojofywp WP Affiliate Disclosure wp-affiliate-disclosure.This issue affects WP Affiliate Disclosure: from	4.3	More

47232	n/a through 1.2.6.		Details
CVE-2023-25068	Missing Authorization vulnerability in Mapro Collins Magazine Edge allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Magazine Edge: from n/a through 1.13.	4.3	More Details
CVE-2019-25230	An information disclosure vulnerability in Kentico Xperience allows authenticated users to view sensitive system objects through the live site widget properties dialog. Attackers can exploit this vulnerability to access unauthorized system information without proper access controls.	4.3	More Details
CVE-2025-11369	The Gutenberg Essential Blocks – Page Builder for Gutenberg Blocks & Patterns plugin for WordPress is vulnerable to unauthorized access of data due to a missing or incorrect capability checks on the get_instagram_access_token_callback, google_map_api_key_save_callback and get_siteinfo functions in all versions up to, and including, 5.7.2. This makes it possible for authenticated attackers, with Author-level access and above, to view API keys configured for the external services.	4.3	More Details
CVE-2024-35321	MyNET up to v26.08 was discovered to contain a Reflected cross-site scripting (XSS) vulnerability via the msgtipo parameter.	4.3	More Details
CVE-2025-13750	The Converter for Media – Optimize images | Convert WebP & AVIF plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `/webp-converter/v1/regenerate-attachment` REST endpoint in all versions up to, and including, 6.3.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete optimized WebP/AVIF variants for arbitrary attachments.	4.3	More Details
CVE-2025-14168	The WP DB Booster plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing nonce validation on the cleanup_all AJAX action. This makes it possible for unauthenticated attackers to delete database records including post drafts, revisions, comments, and metadata via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2025-68614	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Prior to version 25.12.0, the Alert Rule API is vulnerable to stored cross-site scripting. Alert rules can be created or updated via LibreNMS API. The alert rule name is not properly sanitized, and can be used to inject HTML code. This issue has been patched in version 25.12.0.	4.3	More Details
CVE-2025-13361	The Web to SugarCRM Lead plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing nonce validation on the custom field deletion functionality. This makes it possible for unauthenticated attackers to delete custom fields 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-2025-62190	Mattermost versions 11.0.x <= 11.0.4, 10.12.x <= 10.12.2, 10.11.x <= 10.11.6 and Mattermost Calls versions <=1.10.0 fail to implement CSRF protection on the Calls widget page which allows an authenticated attacker to initiate calls and inject messages into channels or direct messages via a malicious webpage or crafted link	4.3	More Details
CVE-2025-62955	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in HappyDevs TempTool allows Retrieve Embedded Sensitive Data.This issue affects TempTool: from n/a through 1.3.1.	4.3	More Details
CVE-2025-13324	Mattermost versions 10.11.x <= 10.11.5, 11.0.x <= 11.0.4, 10.12.x <= 10.12.2 fail to invalidate invite tokens after use which allows malicious actors who have intercepted invite tokens to manipulate channel memberships including adding or removing users from private channels via token replay attack.	4.3	More Details
CVE-2025-14962	A flaw has been found in code-projects Simple Stock System 1.0. The impacted element is an unknown function of the file /market/chatuser.php. This manipulation causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been published and may be used.	4.3	More Details
CVE-2025-7047	Missing Authorization vulnerability in Utarit Informatics Services Inc. SoliClub allows Privilege Abuse.This issue affects SoliClub: before 5.3.7.	4.3	More Details
CVE-2025-67653	Advantech WebAccess/SCADA is vulnerable to directory traversal, which may allow an attacker to determine the existence of arbitrary files.	4.3	More Details
CVE-2025-43541	A type confusion issue was addressed with improved state handling. This issue is fixed in Safari 26.2, iOS 18.7.3 and iPadOS 18.7.3, iOS 26.2 and iPadOS 26.2, macOS Tahoe 26.2, visionOS 26.2. Processing maliciously crafted web content may lead to an unexpected Safari crash.	4.3	More Details
CVE-2025-43536	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Tahoe 26.2, iOS 26.2 and iPadOS 26.2, Safari 26.2, iOS 18.7.3 and iPadOS 18.7.3. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-2025-43535	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.2, iOS 18.7.3 and iPadOS 18.7.3, iOS 26.2 and iPadOS 26.2, macOS Tahoe 26.2, visionOS 26.2. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details
CVE-	Control Panel provides an API for pre-registering into an enrollment and organization prior to a user's first login. The API		

2025- 64400	for creating users checks that the account requesting a user creation has `edit` on the enrollment-level user directory, but is missing a separate check that the enrollment editor has access (or belongs to) the organization that they are adding a user to.	4.1	More Details
CVE- 2025- 59301	Delta Electronics DVP15MC11T lacks proper validation of the modbus/tcp packets and can lead to denial of service.	4.0	More Details
CVE- 2025- 65713	Home Assistant Core before v2025.8.0 is vulnerable to Directory Traversal. The Downloader integration does not fully validate file paths during concatenation, leaving a path traversal vulnerability.	4.0	More Details
CVE- 2025- 13326	Mattermost Desktop App versions <6.0.0 fail to enable the Hardened Runtime on the Mattermost Desktop App when packaged for Mac App Store which allows an attacker to inherit TCC permissions via copying the binary to a tmp folder.	3.9	More Details
CVE- 2025- 14955	A vulnerability was found in Open5GS up to 2.7.5. Affected by this vulnerability is the function ogs_pfcp_handle_create_pdr in the library lib/pfcp/handler.c of the component PFCP. The manipulation results in improper initialization. It is possible to launch the attack remotely. This attack is characterized by high complexity. The exploitation appears to be difficult. The exploit has been made public and could be used. The patch is identified as 773117aa5472af26fc9f80e608d3386504c3bdb7. It is best practice to apply a patch to resolve this issue.	3.7	More Details
CVE- 2025- 14954	A vulnerability has been found in Open5GS up to 2.7.5. Affected is the function ogs_pfcp_pdr_find_or_add/ogs_pfcp_far_find_or_add/ogs_pfcp_urr_find_or_add/ogs_pfcp_qer_find_or_add in the library lib/pfcp/context.c of the component QER/FAR/URR/PDR. The manipulation leads to reachable assertion. It is possible to initiate the attack remotely. The attack's complexity is rated as high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier of the patch is 442369dcd964f03d95429a6a01a57ed21f7779b7. Applying a patch is the recommended action to fix this issue.	3.7	More Details
CVE- 2025- 55254	Improper management of Path-relative stylesheet import in HCL BigFix Remote Control Lite Web Portal (versions 10.1.0.0326 and lower) may allow to execute malicious code in certain web pages.	3.7	More Details
CVE- 2025- 15005	A security flaw has been discovered in CouchCMS up to 2.4. Affected is an unknown function of the file couch/config.example.php of the component reCAPTCHA Handler. The manipulation of the argument K_RECAPTCHA_SITE_KEY/K_RECAPTCHA_SECRET_KEY results in use of hard-coded cryptographic key . It is possible to launch the attack remotely. This attack is characterized by high complexity. The exploitability is told to be difficult. The exploit has been released to the public and may be exploited.	3.7	More Details
CVE- 2025- 43533	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in watchOS 26.2, iOS 26.2 and iPadOS 26.2, macOS Tahoe 26.2, visionOS 26.2, tvOS 26.2. A malicious HID device may cause an unexpected process crash.	3.5	More Details
CVE- 2021- 47722	Zucchetti Axess CLOKI Access Control 1.64 contains a cross-site request forgery vulnerability that allows attackers to manipulate access control settings without user interaction. Attackers can craft malicious web pages with hidden forms to disable or modify access control parameters by tricking authenticated users into loading the page.	3.5	More Details
CVE- 2025- 14957	A vulnerability was identified in WebAssembly Binaryen up to 125. This affects the function IRBuilder::makeLocalGet/IRBuilder::makeLocalSet/IRBuilder::makeLocalTee of the file src/wasm/wasm-ir-builder.cpp of the component IRBuilder. Such manipulation of the argument Index leads to null pointer dereference. Local access is required to approach this attack. The exploit is publicly available and might be used. The name of the patch is 6fb2b917a79578ab44cf3b900a6da4c27251e0d4. Applying a patch is advised to resolve this issue.	3.3	More Details
CVE- 2025- 14841	A flaw has been found in OFFIS DCMTK up to 3.6.9. The impacted element is the function DcmQueryRetrieveIndexDatabaseHandle::startFindRequest/DcmQueryRetrieveIndexDatabaseHandle::startMoveRequest in the library dcmqrdb/libsrc/dcmqrdbi.cc of the component dcmqrscp. This manipulation causes null pointer dereference. The attack requires local access. Upgrading to version 3.7.0 is sufficient to resolve this issue. Patch name: ffb1a4a37d2c876e3feeb31df4930f2aed7fa030. You should upgrade the affected component.	3.3	More Details
CVE- 2025- 13321	Mattermost Desktop App versions <6.0.0 fail to sanitize sensitive information from Mattermost logs and clear data on server deletion which allows an attacker with access to the users system to gain access to potentially sensitive information via reading the application logs.	3.3	More Details
CVE- 2025- 46279	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 26.2, iOS 18.7.3 and iPadOS 18.7.3, iOS 26.2 and iPadOS 26.2, macOS Tahoe 26.2, visionOS 26.2, tvOS 26.2. An app may be able to identify what other apps a user has installed.	3.3	More Details
CVE- 2025- 46277	A logging issue was addressed with improved data redaction. This issue is fixed in macOS Tahoe 26.2, iOS 26.2 and iPadOS 26.2, watchOS 26.2. An app may be able to access a user’s Safari history.	3.3	More Details
CVE- 2025- 68462	Freedombox before 25.17.1 does not set proper permissions for the backups-data directory, allowing the reading of dump files of databases.	3.2	More Details
CVE- 2025-	A flaw has been found in Open5GS up to 2.7.5. This impacts the function ogs_pfcp_handle_create_pdr in the library lib/pfcp/handler.c of the component FAR-ID Handler. Executing manipulation can lead to null pointer dereference. The attack may be performed from remote. The attack requires a high level of complexity. The exploitability is said to be	3.1	More

14953	difficult. The exploit has been published and may be used. This patch is called 93a9fd98a8baa94289be3b982028201de4534e32. It is advisable to implement a patch to correct this issue.		Details
CVE-2025-43531	A race condition was addressed with improved state handling. This issue is fixed in watchOS 26.2, Safari 26.2, iOS 18.7.3 and iPadOS 18.7.3, iOS 26.2 and iPadOS 26.2, macOS Tahoe 26.2, visionOS 26.2, tvOS 26.2. Processing maliciously crafted web content may lead to an unexpected process crash.	3.1	More Details
CVE-2025-65046	Microsoft Edge (Chromium-based) Spoofing Vulnerability	3.1	More Details
CVE-2025-62690	Mattermost versions 10.11.x <= 10.11.4 fail to validate redirect URLs on the /error page, which allows an attacker to redirect a victim to a malicious site via a crafted link opened in a new tab.	3.1	More Details
CVE-2025-13352	Mattermost versions 10.11.x <= 10.11.6 and Mattermost GitHub plugin versions <=2.4.0 fail to validate plugin bot identity in reaction forwarding which allows attackers to hijack the GitHub reaction feature to make users add reactions to arbitrary GitHub objects via crafted notification posts.	3.0	More Details
CVE-2025-65185	There is a username enumeration via local user login in Entrinsik Informer v5.10.1 which allows malicious users to enumerate users by entering an OTP code and new password then reviewing application responses.	2.8	More Details
CVE-2025-12654	The Migration, Backup, Staging – WPvivid Backup & Migration plugin for WordPress is vulnerable to arbitrary directory creation in all versions up to, and including, 0.9.120. This is due to the check_filesystem_permissions() function not properly restricting the directories that can be created, or in what location. This makes it possible for authenticated attackers, with Administrator-level access and above, to create arbitrary directories.	2.7	More Details
CVE-2025-14836	A flaw has been found in ZZCMS 2025. Affected by this vulnerability is an unknown functionality of the file /reg/user_save.php of the component User Data Storage Module. This manipulation causes cleartext storage in a file or on disk. Remote exploitation of the attack is possible. The exploit has been published and may be used.	2.7	More Details
CVE-2025-14991	A weakness has been identified in Campcodes Complete Online Beauty Parlor Management System 1.0. The affected element is an unknown function of the file /admin/bwdates-reports-details.php. Executing manipulation of the argument fromdate can lead to cross site scripting. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	2.4	More Details
CVE-2025-14801	A security vulnerability has been detected in xiweicheng TMS up to 2.28.0. This affects the function createComment of the file /admin/blog/comment/create. Such manipulation of the argument content leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2025-13698	Deciso OPNsense diag_backup.php filename Directory Traversal Arbitrary File Creation Vulnerability. This vulnerability allows network-adjacent attackers to create arbitrary files on affected installations of Deciso OPNsense. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of backup configuration files. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to create files in the context of root. Was ZDI-CAN-28133.	N/A	More Details
CVE-2025-13699	MariaDB mariadb-dump Utility Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of MariaDB. Interaction with the mariadb-dump utility is required to exploit this vulnerability but attack vectors may vary depending on the implementation. The specific flaw exists within the handling of view names. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27000.	N/A	More Details
CVE-2025-13700	DreamFactory saveZipFile Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of DreamFactory. Authentication is required to exploit this vulnerability. The specific flaw exists within the implementation of the saveZipFile method. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-26589.	N/A	More Details
CVE-2025-12495	Academy Software Foundation OpenEXR EXR File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Academy Software Foundation OpenEXR. 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 EXR files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27946.	N/A	More Details
CVE-2025-14936	NSF Unidata NetCDF-C Attribute Name Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NSF Unidata NetCDF-C. 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 attribute names. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27269.	N/A	More Details
CVE-2025-	Senstar Symphony FetchStoredLicense Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Senstar Symphony. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of FetchStoredLicense method. The issue results	N/A	More

12491	from the exposure of sensitive information. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-26908.		Details
CVE-2025-12839	Academy Software Foundation OpenEXR EXR File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Academy Software Foundation OpenEXR. 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 EXR files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27947.	N/A	More Details
CVE-2025-12840	Academy Software Foundation OpenEXR EXR File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Academy Software Foundation OpenEXR. 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 EXR files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27948.	N/A	More Details
CVE-2025-13703	VIPRE Advanced Security Incorrect Permission Assignment Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of VIPRE Advanced Security for PC. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the product installer. The issue results from incorrect permissions on a folder. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27147.	N/A	More Details
CVE-2025-12838	MSP360 Free Backup Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of MSP360 Free Backup. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. User interaction on the part of an administrator is needed additionally. The specific flaw exists within the restore functionality. By creating a junction, an attacker can abuse the service to create arbitrary files. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27245.	N/A	More Details
CVE-2025-14935	NSF Unidata NetCDF-C Dimension Name Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NSF Unidata NetCDF-C. 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 dimension names. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27168.	N/A	More Details
CVE-2025-53000	The nbconvert tool, jupyter nbconvert, converts Jupyter notebooks to various other formats via Jinja templates. Versions of nbconvert up to and including 7.16.6 on Windows have a vulnerability in which converting a notebook containing SVG output to a PDF results in unauthorized code execution. Specifically, a third party can create a `inkscape.bat` file that defines a Windows batch script, capable of arbitrary code execution. When a user runs `jupyter nbconvert --to pdf` on a notebook containing SVG output to a PDF on a Windows platform from this directory, the `inkscape.bat` file is run unexpectedly. As of time of publication, no known patches exist.	N/A	More Details
CVE-2025-14934	NSF Unidata NetCDF-C Variable Name Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NSF Unidata NetCDF-C. 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 variable names. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27267.	N/A	More Details
CVE-2025-65007	In WODESYS WD-R608U router (also known as WDR122B V2.0 and WDR28) due to lack of authentication in the configuration change module in the adm.cgi endpoint, the unauthenticated attacker can execute commands including backup creation, device restart and resetting the device to factory settings. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version WDR28081123OV1.01 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-68325	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_cake: Fix incorrect qlen reduction in cake_drop In cake_drop(), qdisc_tree_reduce_backlog() is used to update the qlen and backlog of the qdisc hierarchy. Its caller, cake_enqueue(), assumes that the parent qdisc will enqueue the current packet. However, this assumption breaks when cake_enqueue() returns NET_XMIT_CN: the parent qdisc stops enqueuing current packet, leaving the tree qlen/backlog accounting inconsistent. This mismatch can lead to a NULL dereference (e.g., when the parent Qdisc is qfq_qdisc). This patch computes the qlen/backlog delta in a more robust way by observing the difference before and after the series of cake_drop() calls, and then compensates the qdisc tree accounting if cake_enqueue() returns NET_XMIT_CN. To ensure correct compensation when ACK thinning is enabled, a new variable is introduced to keep qlen unchanged.	N/A	More Details
CVE-2025-13074	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-10863	Rejected reason: This CVE id was assigned but later discarded.	N/A	More Details

CVE-2025-68324	In the Linux kernel, the following vulnerability has been resolved: scsi: imm: Fix use-after-free bug caused by unfinished delayed work The delayed work item 'imm_tq' is initialized in imm_attach() and scheduled via imm_queuecommand() for processing SCSI commands. When the IMM parallel port SCSI host adapter is detached through imm_detach(), the imm_struct device instance is deallocated. However, the delayed work might still be pending or executing when imm_detach() is called, leading to use-after-free bugs when the work function imm_interrupt() accesses the already freed imm_struct memory. The race condition can occur as follows: CPU 0(detach thread) | CPU 1 | imm_queuecommand() | imm_queuecommand_lck() imm_detach() | schedule_delayed_work() kfree(dev) //FREE | imm_interrupt() | dev = container_of(...) //USE dev-> //USE Add disable_delayed_work_sync() in imm_detach() to guarantee proper cancellation of the delayed work item before imm_struct is deallocated.	N/A	More Details
CVE-2025-68323	In the Linux kernel, the following vulnerability has been resolved: usb: typec: ucsi: fix use-after-free caused by uec->work The delayed work uec->work is scheduled in gaokun_ucsi_probe() but never properly canceled in gaokun_ucsi_remove(). This creates use-after-free scenarios where the ucsi and gaokun_ucsi structure are freed after ucsi_destroy() completes execution, while the gaokun_ucsi_register_worker() might be either currently executing or still pending in the work queue. The already-freed gaokun_ucsi or ucsi structure may then be accessed. Furthermore, the race window is 3 seconds, which is sufficiently long to make this bug easily reproducible. The following is the trace captured by KASAN: == BUG: KASAN: slab-use-after-free in __run_timers+0x5ec/0x630 Write of size 8 at addr ffff00000ec28cc8 by task swapper/0/0 ... Call trace: show_stack+0x18/0x24 (C) dump_stack_lvl+0x78/0x90 print_report+0x114/0x580 kasan_report+0xa4/0xf0 __asan_report_store8_noabort+0x20/0x2c __run_timers+0x5ec/0x630 run_timer_softirq+0xe8/0x1cc handle_softirqs+0x294/0x720 __do_softirq+0x14/0x20 ____do_softirq+0x10/0x1c call_on_irq_stack+0x30/0x48 do_softirq_own_stack+0x1c/0x28 __irq_exit_rcu+0x27c/0x364 irq_exit_rcu+0x10/0x1c el1_interrupt+0x40/0x60 el1h_64_irq_handler+0x18/0x24 el1h_64_irq+0x6c/0x70 arch_local_irq_enable+0x4/0x8 (P) do_idle+0x334/0x458 cpu_startup_entry+0x60/0x70 rest_init+0x158/0x174 start_kernel+0x2f8/0x394 __primary_switched+0x8c/0x94 Allocated by task 72 on cpu 0 at 27.510341s: kasan_save_stack+0x2c/0x54 kasan_save_track+0x24/0x5c kasan_save_alloc_info+0x40/0x54 __kasan_kmalloc+0xa0/0xb8 __kmalloc_node_track_caller_noprof+0x1c0/0x588 devm_kmalloc+0x7c/0x1c8 gaokun_ucsi_probe+0xa0/0x840 auxiliary_bus_probe+0x94/0xf8 really_probe+0x17c/0x5b8 __driver_probe_device+0x158/0x2c4 driver_probe_device+0x10c/0x264 __device_attach_driver+0x168/0x2d0 bus_for_each_drv+0x100/0x188 __device_attach+0x174/0x368 device_initial_probe+0x14/0x20 bus_probe_device+0x120/0x150 device_add+0xb3c/0x10fc __auxiliary_device_add+0x88/0x130 ... Freed by task 73 on cpu 1 at 28.910627s: kasan_save_stack+0x2c/0x54 kasan_save_track+0x24/0x5c __kasan_save_free_info+0x4c/0x74 __kasan_slab_free+0x60/0x8c kfree+0xd4/0x410 devres_release_all+0x140/0x1f0 device_unbind_cleanup+0x20/0x190 device_release_driver_internal+0x344/0x460 device_release_driver+0x18/0x24 bus_remove_device+0x198/0x274 device_del+0x310/0xa84 ... The buggy address belongs to the object at ffff00000ec28c00 which belongs to the cache kmalloc-512 of size 512 The buggy address is located 200 bytes inside of freed 512-byte region The buggy address belongs to the physical page: page: refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x4ec28 head: order:2 mapcount:0 entire_mapcount:0 nr_pages_mapped:0 pincount:0 flags: 0x3fffe0000000040(head|node=0|zone=0|lastcpupid=0x1ffff) page_type: f5(slab) raw: 03fffe0000000040 ffff000008801c80 dead000000000122 0000000000000000 raw: 0000000000000000 0000000080100010 00000000f5000000 0000000000000000 head: 03fffe0000000040 ffff000008801c80 dead000000000122 0000000000000000 head: 0000000000000000 0000000080100010 00000000f5000000 0000000000000000 head: 03fffe0000000002 fffffdffc03b0a01 00000000ffffffff 00000000ffffffff head: ffffffffffffffff 0000000000000000 00000000ffffffff 0000000000000004 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff00000ec28b80: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ffff00000ec28c00: fa fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb >ffff00000ec28c80: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ^ ffff00000ec28d00: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff00000ec28d80: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb == ---truncated---	N/A	More Details
CVE-2025-65011	In WODESYS WD-R608U router (also known as WDR122B V2.0 and WDR28) an unauthorised user can view configuration files by directly referencing the resource in question. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version WDR28081123OV1.01 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-65010	WODESYS WD-R608U router (also known as WDR122B V2.0 and WDR28) is vulnerable to Broken Access Control in initial configuration wizard.cgi endpoint. Malicious attacker can change admin panel password without authorization. The vulnerability can also be exploited after the initial configuration has been set. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version WDR28081123OV1.01 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-11901	An uncontrolled resource consumption vulnerability affects certain ASUS motherboards using Intel B460, B560, B660, B760, H410, H510, H610, H470, Z590, Z690, Z790, W480, W680 series chipsets. Exploitation requires physical access to internal expansion slots to install a specially crafted device and supporting software utility, and may lead to uncontrolled resource consumption that increases the risk of unauthorized direct memory access (DMA). Refer to the 'Security Update for UEFI firmware' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-65009	In WODESYS WD-R608U router (also known as WDR122B V2.0 and WDR28) admin password is stored in configuration file as plaintext and can be obtained by unauthorized user by direct references to the resource in question. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version WDR28081123OV1.01 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
	In WODESYS WD-R608U router (also known as WDR122B V2.0 and WDR28) due to lack of validation in the langGet		

CVE-2025-65008	parameter in the adm.cgi endpoint, the malicious attacker can execute system shell commands. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version WDR28081123OV1.01 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2025-11775	An out-of-bounds read vulnerability has been identified in the asComSvc service. This vulnerability can be triggered by sending specially crafted requests, which may lead to a service crash or partial loss of functionality. This vulnerability only affects ASUS motherboard series products. Refer to the 'Security Update for Armoury Crate App' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2025-58052	Galette is a membership management web application for non profit organizations. Starting in version 0.9.6 and prior to version 1.2.0, attackers with group manager role can bypass intended restrictions allowing unauthorized access and changes despite role-based controls. Since it requires privileged access initially, exploitation is restricted to malicious insiders or compromised group managers accounts. Version 1.2.0 fixes the issue.	N/A	More Details
CVE-2025-14933	NSF Unidata NetCDF-C NC Variable Integer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NSF Unidata NetCDF-C. 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 NC variables. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27266.	N/A	More Details
CVE-2025-14921	Hugging Face Transformers Transformer-XL Model Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Hugging Face Transformers. 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 model files. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-25424.	N/A	More Details
CVE-2025-14922	Hugging Face Diffusers CogView4 Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Hugging Face Diffusers. 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 checkpoints. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27424.	N/A	More Details
CVE-2025-14924	Hugging Face Transformers megatron_gpt2 Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Hugging Face Transformers. 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 checkpoints. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27984.	N/A	More Details
CVE-2025-14925	Hugging Face Accelerate Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Hugging Face Accelerate. 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 checkpoints. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-27985.	N/A	More Details
CVE-2025-14926	Hugging Face Transformers SEW convert_config Code Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Hugging Face Transformers. User interaction is required to exploit this vulnerability in that the target must convert a malicious checkpoint. The specific flaw exists within the convert_config function. The issue results from the lack of proper validation of a user-supplied string before using it to execute Python code. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-28251.	N/A	More Details
CVE-2025-14927	Hugging Face Transformers SEW-D convert_config Code Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Hugging Face Transformers. User interaction is required to exploit this vulnerability in that the target must convert a malicious checkpoint. The specific flaw exists within the convert_config function. The issue results from the lack of proper validation of a user-supplied string before using it to execute Python code. An attacker can leverage this vulnerability to execute code in the context of the current user. . Was ZDI-CAN-28252.	N/A	More Details
CVE-2025-14928	Hugging Face Transformers HuBERT convert_config Code Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Hugging Face Transformers. User interaction is required to exploit this vulnerability in that the target must convert a malicious checkpoint. The specific flaw exists within the convert_config function. The issue results from the lack of proper validation of a user-supplied string before using it to execute Python code. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-28253.	N/A	More Details
CVE-2025-14929	Hugging Face Transformers X-CLIP Checkpoint Conversion Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Hugging Face Transformers. 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 checkpoints. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28308.	N/A	More Details

CVE-2025-14930	Hugging Face Transformers GLM4 Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Hugging Face Transformers. 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 weights. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28309.	N/A	More Details
CVE-2025-14931	Hugging Face smolagents Remote Python Executor Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Hugging Face smolagents. Authentication is not required to exploit this vulnerability. The specific flaw exists within the parsing of pickle data. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-28312.	N/A	More Details
CVE-2025-14932	NSF Unidata NetCDF-C Time Unit Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NSF Unidata NetCDF-C. 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 time units. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27273.	N/A	More Details
CVE-2025-14920	Hugging Face Transformers Perceiver Model Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Hugging Face Transformers. 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 model files. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-25423.	N/A	More Details
CVE-2025-14401	PDFsam Enhanced App Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDFsam Enhanced. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of App objects. 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-27260.	N/A	More Details
CVE-2025-13706	Tencent PatrickStar merge_checkpoint Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tencent PatrickStar. 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 merge_checkpoint endpoint. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27182.	N/A	More Details
CVE-2025-14496	RealDefense SUPERAntiSpyware Exposed Dangerous Function Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of RealDefense SUPERAntiSpyware. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the SAS Core Service. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27678.	N/A	More Details
CVE-2025-14422	GIMP PNM File Parsing Integer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PNM files. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28273.	N/A	More Details
CVE-2025-14423	GIMP LBM File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of LBM files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28311.	N/A	More Details
CVE-2025-14424	GIMP XCF File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of XCF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28376.	N/A	More Details
CVE-2025-14425	GIMP JP2 File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GIMP. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-28248.	N/A	More Details
	RealDefense SUPERAntiSpyware Exposed Dangerous Function Local Privilege Escalation Vulnerability. This vulnerability		

CVE-2025-14488	allows local attackers to escalate privileges on affected installations of RealDefense SUPERAntiSpyware. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the SAS Core Service. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27657.	N/A	More Details
CVE-2025-14489	RealDefense SUPERAntiSpyware Exposed Dangerous Function Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of RealDefense SUPERAntiSpyware. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the SAS Core Service. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27658.	N/A	More Details
CVE-2025-14490	RealDefense SUPERAntiSpyware Exposed Dangerous Function Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of RealDefense SUPERAntiSpyware. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the SAS Core Service. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27659.	N/A	More Details
CVE-2025-14491	RealDefense SUPERAntiSpyware Exposed Dangerous Function Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of RealDefense SUPERAntiSpyware. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the SAS Core Service. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27660.	N/A	More Details
CVE-2025-14492	RealDefense SUPERAntiSpyware Exposed Dangerous Function Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of RealDefense SUPERAntiSpyware. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the SAS Core Service. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27668.	N/A	More Details
CVE-2025-14493	RealDefense SUPERAntiSpyware Exposed Dangerous Function Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of RealDefense SUPERAntiSpyware. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the SAS Core Service. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27675.	N/A	More Details
CVE-2025-14494	RealDefense SUPERAntiSpyware Exposed Dangerous Function Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of RealDefense SUPERAntiSpyware. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the SAS Core Service. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27676.	N/A	More Details
CVE-2025-14495	RealDefense SUPERAntiSpyware Exposed Dangerous Function Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of RealDefense SUPERAntiSpyware. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the SAS Core Service. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27677.	N/A	More Details
CVE-2025-14497	RealDefense SUPERAntiSpyware Exposed Dangerous Function Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of RealDefense SUPERAntiSpyware. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the SAS Core Service. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27680.	N/A	More Details
CVE-2025-13707	Tencent HunyuanDiT model_resume Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tencent HunyuanDiT. 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 model_resume function. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27183.	N/A	More Details
CVE-2025-14498	TradingView Desktop Electron Uncontrolled Search Path Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of TradingView Desktop. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the configuration of the Electron framework. The product loads a script file from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of a target user. Was ZDI-CAN-27395.	N/A	More Details
	IceWarp gmaps Cross-Site Scripting Authentication Bypass Vulnerability. This vulnerability allows remote attackers to		

CVE-2025-14499	bypass authentication on affected installations of IceWarp. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of a parameter passed to the gmaps webpage. The issue results from the lack of proper validation of user-supplied data, which can lead to the injection of an arbitrary script. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-25441.	N/A	More Details
CVE-2025-14500	IceWarp14 X-File-Operation Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IceWarp. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the X-File-Operation header. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-27394.	N/A	More Details
CVE-2025-14501	Sante PACS Server HTTP Content-Length Header Handling NULL Pointer Dereference Denial-of-Service Vulnerability. This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of Sante PACS Server. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HTTP Content-Length header. The issue results from the lack of proper validation of a pointer prior to accessing it. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-26770.	N/A	More Details
CVE-2025-66209	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.451, an authenticated command injection vulnerability in the Database Backup functionality allows users with application/service management permissions to execute arbitrary commands as root on managed servers. Database names used in backup operations are passed directly to shell commands without sanitization, enabling full remote code execution. Version 4.0.0-beta.451 fixes the issue.	N/A	More Details
CVE-2025-66210	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.451, an authenticated command injection vulnerability in the Database Import functionality allows users with application/service management permissions to execute arbitrary commands as root on managed servers. Database names used in import operations are passed directly to shell commands without sanitization, enabling full remote code execution. Version 4.0.0-beta.451 fixes the issue.	N/A	More Details
CVE-2025-66211	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.451, an authenticated command injection vulnerability in PostgreSQL Init Script Filename handling allows users with application/service management permissions to execute arbitrary commands as root on managed servers. PostgreSQL initialization script filenames are passed to shell commands without proper validation, enabling full remote code execution. Version 4.0.0-beta.451 fixes the issue.	N/A	More Details
CVE-2025-66212	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.451, an authenticated command injection vulnerability in the Dynamic Proxy Configuration Filename handling allows users with application/service management permissions to execute arbitrary commands as root on managed servers. Proxy configuration filenames are passed to shell commands without proper escaping, enabling full remote code execution. Version 4.0.0-beta.451 fixes the issue.	N/A	More Details
CVE-2025-66213	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.451, an authenticated command injection vulnerability in the File Storage Directory Mount Path functionality allows users with application/service management permissions to execute arbitrary commands as root on managed servers. The file_storage_directory_source parameter is passed directly to shell commands without proper sanitization, enabling full remote code execution on the host system. Version 4.0.0-beta.451 fixes the issue.	N/A	More Details
CVE-2025-10910	A flaw in the binding process of Govee’s cloud platform and devices allows a remote attacker to bind an existing, online Govee device to the attacker’s account, resulting in full control of the device and removal of the device from its legitimate owner’s account. The server-side API allows device association using a set of identifiers: "device", "sku", "type", and a client-computed "value", that are not cryptographically bound to a secret originating from the device itself. The vulnerability has been verified for the Govee H6056 - lamp device in firmware version 1.08.13, but may affect also other Govee cloud-connected devices. The vendor is investigating other potentially affected models. The vendor has deployed server-side security enhancements and automatic firmware updates for model H6056. Most of H6056 devices have been successfully patched through automatic updates. Remaining H6056 users with upgradeable hardware versions must manually update firmware through the Govee Home app while keeping their device WiFi-connected. Users should open the Govee Home app, tap their H6056 device card to enter the device details page, tap the settings icon in the upper right corner, navigate to Device Information section (Firmware Version), and tap the Update button to install the security patch immediately. Govee H6056 devices with hardware versions 1.00.10 or 1.00.11 cannot receive firmware update due to hardware limitations.	N/A	More Details
CVE-2025-67048	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2025-67039. Reason: This record is a reservation duplicate of CVE-2025-67039. Notes: All CVE users should reference CVE-2025-67039 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-68667	continuwuity is a Matrix homeserver written in Rust. Prior to version 0.5.0, this vulnerability allows a remote, unauthenticated attacker to force the target server to cryptographically sign arbitrary membership events. The flaw exists because the server fails to validate the origin of a signing request, provided the event's state_key is a valid user ID belonging to the target server. This issue has been patched in version 0.5.0. A workaround for this issue involves blocking access to the PUT /_matrix/federation/v2/invite/{roomId}/{eventId} endpoint using the reverse proxy.	N/A	More Details
CVE-2025-14421	pdfforge PDF Architect PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of pdfforge PDF Architect. 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 PDF 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 object. An attacker can leverage this in	N/A	More Details

	conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-27915.		
CVE-2025-14420	pdfforge PDF Architect CBZ File Parsing Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of pdfforge PDF Architect. 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 CBZ files. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27514.	N/A	More Details
CVE-2025-14419	pdfforge PDF Architect PDF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of pdfforge PDF Architect. 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 PDF 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-27902.	N/A	More Details
CVE-2025-14418	pdfforge PDF Architect XLS File Insufficient UI Warning Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of pdfforge PDF Architect. 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 processing of XLS files. The issue results from allowing the execution of dangerous script without user warning. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27502.	N/A	More Details
CVE-2025-13708	Tencent NeuralNLP-NeuralClassifier _load_checkpoint Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tencent NeuralNLP-NeuralClassifier. 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 _load_checkpoint function. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27184.	N/A	More Details
CVE-2025-13709	Tencent TFace restore_checkpoint Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tencent TFace. 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 restore_checkpoint function. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27185.	N/A	More Details
CVE-2025-13710	Tencent HunyuanVideo load_vae Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tencent HunyuanVideo. 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 load_vae function.The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27186.	N/A	More Details
CVE-2025-13711	Tencent TFace eval Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tencent TFace. 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 eval endpoint. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27187.	N/A	More Details
CVE-2025-13712	Tencent HunyuanDiT merge Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tencent HunyuanDiT. 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 merge endpoint. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27190.	N/A	More Details
CVE-2025-13713	Tencent Hunyuan3D-1 load_pretrained Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tencent Hunyuan3D-1. 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 load_pretrained function. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27191.	N/A	More Details
CVE-2025-13714	Tencent MedicalNet generate_model Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tencent MedicalNet. 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 generate_model function. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27192.	N/A	More Details
CVE-2025-13715	Tencent FaceDetection-DSFD resnet Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tencent FaceDetection-DSFD. 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 resnet endpoint. The issue results from the lack of proper validation of	N/A	More Details

	user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27197.		
CVE-2025-13716	Tencent MimicMotion create_pipeline Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tencent MimicMotion. 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 create_pipeline function. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-27208.	N/A	More Details
CVE-2025-14402	PDFsam Enhanced DOC File Insufficient UI Warning Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDFsam Enhanced. 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 processing of DOC files. The issue results from allowing the execution of dangerous script without user warning. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27499.	N/A	More Details
CVE-2025-14403	PDFsam Enhanced Launch Insufficient UI Warning Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDFsam Enhanced. 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 implementation of the Launch action. The issue results from allowing the execution of dangerous script without user warning. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27500.	N/A	More Details
CVE-2025-14404	PDFsam Enhanced XLS File Insufficient UI Warning Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDFsam Enhanced. 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 processing of XLS files. The issue results from allowing the execution of dangerous script without user warning. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27498.	N/A	More Details
CVE-2025-14405	PDFsam Enhanced Uncontrolled Search Path Element Local Privilege Escalation Vulnerability. This vulnerability allows phyiscally-present attackers to escalate privileges on affected installations of PDFsam Enhanced. An attacker must first obtain the ability to mount a malicious drive onto the target system in order to exploit this vulnerability. The specific flaw exists within the configuration of OpenSSL. The product loads an OpenSSL configuration file from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-27867.	N/A	More Details
CVE-2025-14406	Soda PDF Desktop Uncontrolled Search Path Element Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Soda PDF Desktop. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the configuration of OpenSSL. The product loads an OpenSSL configuration file from an unsecured location. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-25793.	N/A	More Details
CVE-2025-14407	Soda PDF Desktop PDF File Parsing Memory Corruption Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Soda PDF Desktop. 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 PDF 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-27141.	N/A	More Details
CVE-2025-14408	Soda PDF Desktop PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Soda PDF Desktop. 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 PDF 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 object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-27143.	N/A	More Details
CVE-2025-14409	Soda PDF Desktop PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Soda PDF Desktop. 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 PDF 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-27120.	N/A	More Details
CVE-2025-14410	Soda PDF Desktop PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Soda PDF Desktop. 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 PDF 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 object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-27142.	N/A	More Details
CVE-2025-	Soda PDF Desktop PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Soda PDF Desktop. 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 PDF files. The issue results from the lack of proper validation of user-supplied data,	N/A	More Details

14411	which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-27140.		
CVE-2025-14412	Soda PDF Desktop XLS File Insufficient UI Warning Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Soda PDF Desktop. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XLS files. The issue results from allowing the execution of dangerous script without user warning. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27495.	N/A	More Details
CVE-2025-14413	Soda PDF Desktop CBZ File Parsing Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Soda PDF Desktop. 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 CBZ files. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27509.	N/A	More Details
CVE-2025-14414	Soda PDF Desktop Word File Insufficient UI Warning Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Soda PDF Desktop. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Word files. The issue results from allowing the execution of dangerous script without user warning. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27496.	N/A	More Details
CVE-2025-14415	Soda PDF Desktop Launch Insufficient UI Warning Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Soda PDF Desktop. 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 implementation of the Launch action. The issue results from allowing the execution of dangerous script without user warning. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27494.	N/A	More Details
CVE-2025-14416	pdfforge PDF Architect DOC File Insufficient UI Warning Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of pdfforge PDF Architect. 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 processing of DOC files. The issue results from allowing the execution of dangerous script without user warning. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27503.	N/A	More Details
CVE-2025-14417	pdfforge PDF Architect Launch Insufficient UI Warning Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of pdfforge PDF Architect. 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 implementation of the Launch action. The issue results from allowing the execution of dangerous script without user warning. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-27501.	N/A	More Details
CVE-2025-64700	Cross-site request forgery vulnerability exists in GROWI v7.3.3 and earlier. If a user views a malicious page while logged in, the user may be tricked to do unintended operations.	N/A	More Details
CVE-2025-68430	CVAT is an open source interactive video and image annotation tool for computer vision. In versions 2.8.1 through 2.52.0, an attacker with an account on a CVAT instance is able to retrieve the contents of any file system directory accessible to the CVAT server. The exposed information is names of contained files and subdirectories. The contents of files are not accessible. Version 2.53.0 contains a patch. No known workarounds are available.	N/A	More Details
CVE-2025-48864	Rejected reason: This CVE id was assigned but later discarded.	N/A	More Details
CVE-2025-61739	Due to Nonce reuse, attackers can perform reply attack or decrypt captured packets.	N/A	More Details
CVE-2025-14202	A vulnerability in the file upload at bookmark + asset rendering pipeline allows an attacker to upload a malicious SVG file with JavaScript content. When an authenticated admin user views the SVG file with embedded JavaScript code of shared bookmark, JavaScript executes in the admin’s browser, retrieves the CSRF token, and sends a request to change the admin's password resulting in a full account takeover.	N/A	More Details
CVE-2025-26379	Use of a weak pseudo-random number generator, which may allow an attacker to read or inject encrypted PowerG packets.	N/A	More Details
CVE-2025-61740	Authentication issue that does not verify the source of a packet which could allow an attacker to create a denial-of-service condition or modify the configuration of the device.	N/A	More Details
CVE-	RIOT is an open-source microcontroller operating system, designed to match the requirements of Internet of Things (IoT) devices and other embedded devices. A vulnerability was discovered in the IPv6 fragmentation reassembly implementation of RIOT OS v2025.07. When receiving an fragmented IPv6 packet with fragment offset 0 and an empty		More

2025-66646	payload, the payload pointer is set to NULL. However, the implementation still tries to copy the payload into the reassembly buffer, resulting in a NULL pointer dereference which crashes the OS (DoS). To trigger the vulnerability, the `gnrc_ipv6_ext_frag` module must be enabled and the attacker must be able to send arbitrary IPv6 packets to the victim. RIOT OS v2025.10 fixes the issue.	N/A	Details
CVE-2025-10021	A Use of Uninitialized Variable vulnerability exists in Open Design Alliance Drawings SDK static versions (mt) before 2026.12. Static object `COdaMfcAppApp theApp` may access `OdString::kEmpty` before its initialization. Due to undefined initialization order of static objects across translation units (Static Initialization Order Fiasco), the application accesses uninitialized memory. This results in application crash on startup, causing denial of service. Due to undefined behavior, memory corruption and potential arbitrary code execution cannot be ruled out in specific exploitation scenarios.	N/A	More Details
CVE-2025-14591	In Delphix Continuous Compliance version 2025.3.0 and later, following a recent bug fix to correctly handle CR+LF (Windows and DOS) End-of-Record (EOR) characters in delimited files, an issue was identified: using an incorrect EOR configuration can cause inaccurate parsing and leave personally identifiable information (PII) unmasked.	N/A	More Details
CVE-2025-68326	In the Linux kernel, the following vulnerability has been resolved: drm/xe/guc: Fix stack_depot usage Add missing stack_depot_init() call when CONFIG_DRM_XE_DEBUG_GUC is enabled to fix the following call stack: [] BUG: kernel NULL pointer dereference, address: 0000000000000000 [] Workqueue: drm_sched_run_job_work [gpu_sched] [] RIP: 0010:stack_depot_save_flags+0x172/0x870 [] Call Trace: [] <TASK> [] fast_req_track+0x58/0xb0 [xe] (cherry picked from commit 64fdf496a6929a0a194387d2bb5efaf5da2b542f)	N/A	More Details
CVE-2025-68327	In the Linux kernel, the following vulnerability has been resolved: usb: renesas_usbhs: Fix synchronous external abort on unbind A synchronous external abort occurs on the Renesas RZ/G3S SoC if unbind is executed after the configuration sequence described above: modprobe usb_f_ecm modprobe libcomposite modprobe configfs cd /sys/kernel/config/usb_gadget mkdir -p g1 cd g1 echo "0x1d6b" > idVendor echo "0x0104" > idProduct mkdir -p strings/0x409 echo "0123456789" > strings/0x409/serialnumber echo "Renesas." > strings/0x409/manufacturer echo "Ethernet Gadget" > strings/0x409/product mkdir -p functions/ecm.usb0 mkdir -p configs/c.1 mkdir -p configs/c.1/strings/0x409 echo "ECM" > configs/c.1/strings/0x409/configuration if [! -L configs/c.1/ecm.usb0]; then ln -s functions/ecm.usb0 configs/c.1 fi echo 11e20000.usb > UDC echo 11e20000.usb > /sys/bus/platform/drivers/renesas_usbhs/unbind The displayed trace is as follows: Internal error: synchronous external abort: 0000000096000010 [#1] SMP CPU: 0 UID: 0 PID: 188 Comm: sh Tainted: G M 6.17.0-rc7-next-20250922-00010-g41050493b2bd #55 PREEMPT Tainted: [M]=MACHINE_CHECK Hardware name: Renesas SMARC EVK version 2 based on r9a08g045s33 (DT) pstate: 604000c5 (nZCv daIF +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : usbhs_sys_function_pullup+0x10/0x40 [renesas_usbhs] lr : usbhsg_update_pullup+0x3c/0x68 [renesas_usbhs] sp : ffff8000838b3920 x29: ffff8000838b3920 x28: ffff00000d585780 x27: 0000000000000000 x26: 0000000000000000 x25: 0000000000000000 x24: ffff00000c3e3810 x23: ffff00000d5e5c80 x22: ffff00000d5e5d40 x21: 0000000000000000 x20: 0000000000000000 x19: ffff00000d5e5c80 x18: 0000000000000020 x17: 2e30303230316531 x16: 312d7968703a7968 x15: 3d454d414e5f4344 x14: 000000000000002c x13: 0000000000000000 x12: 0000000000000000 x11: ffff00000f358f38 x10: ffff00000f358db0 x9 : ffff00000b41f418 x8 : 0101010101010101 x7 : 7f7f7f7f7f7f7f7f x6 : fefefeff6364626d x5 : 8080808000000000 x4 : 000000004b5ccb9d x3 : 0000000000000000 x2 : 0000000000000000 x1 : ffff800083790000 x0 : ffff00000d5e5c80 Call trace: usbhs_sys_function_pullup+0x10/0x40 [renesas_usbhs] (P) usbhsg_pullup+0x4c/0x7c [renesas_usbhs] usb_gadget_disconnect_locked+0x48/0xd4 gadget_unbind_driver+0x44/0x114 device_remove+0x4c/0x80 device_release_driver_internal+0x1c8/0x224 device_release_driver+0x18/0x24 bus_remove_device+0xcc/0x10c device_del+0x14c/0x404 usb_del_gadget+0x88/0xc0 usb_del_gadget_udc+0x18/0x30 usbhs_mod_gadget_remove+0x24/0x44 [renesas_usbhs] usbhs_mod_remove+0x20/0x30 [renesas_usbhs] usbhs_remove+0x98/0xdc [renesas_usbhs] platform_remove+0x20/0x30 device_remove+0x4c/0x80 device_release_driver_internal+0x1c8/0x224 device_driver_detach+0x18/0x24 unbind_store+0xb4/0xb8 drv_attr_store+0x24/0x38 sysfs_kf_write+0x7c/0x94 kernfs_fop_write_iter+0x128/0x1b8 vfs_write+0x2ac/0x350 ksys_write+0x68/0xfc __arm64_sys_write+0x1c/0x28 invoke_syscall+0x48/0x110 el0_svc_common.constprop.0+0xc0/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x34/0xf0 el0t_64_sync_handler+0xa0/0xe4 el0t_64_sync+0x198/0x19c Code: 7100003f 1a9f07e1 531c6c22 f9400001 (79400021) ---[end trace 0000000000000000]--- note: sh[188] exited with irqs disabled note: sh[188] exited with preempt_count 1 The issue occurs because usbhs_sys_function_pullup(), which accesses the IP registers, is executed after the USBHS clocks have been disabled. The problem is reproducible on the Renesas RZ/G3S SoC starting with the addition of module stop in the clock enable/disable APIs. With module stop functionality enabled, a bus error is expected if a master accesses a module whose clock has been stopped and module stop activated. Disable the IP clocks at the end of remove.	N/A	More Details
CVE-2025-68328	In the Linux kernel, the following vulnerability has been resolved: firmware: stratix10-svc: fix bug in saving controller data Fix the incorrect usage of platform_set_drvdata and dev_set_drvdata. They both are of the same data and overrides each other. This resulted in the rmmod of the svc driver to fail and throw a kernel panic for kthread_stop and fifo free.	N/A	More Details
CVE-2025-68329	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix WARN_ON in tracing_buffers_mmap_close for split VMAs When a VMA is split (e.g., by partial munmap or MAP_FIXED), the kernel calls vm_ops->close on each portion. For trace buffer mappings, this results in ring_buffer_unmap() being called multiple times while ring_buffer_map() was only called once. This causes ring_buffer_unmap() to return -ENODEV on subsequent calls because user_mapped is already 0, triggering a WARN_ON. Trace buffer mappings cannot support partial mappings because the ring buffer structure requires the complete buffer including the meta page. Fix this by adding a may_split callback that returns -EINVAL to prevent VMA splits entirely.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: iio: accel: bmc150: Fix irq assumption regression The code in bmc150-accel-core.c unconditionally calls bmc150_accel_set_interrupt() in the iio_buffer_setup_ops, such as on the runtime PM resume path giving a kernel splat like this if the device has no interrupts: Unable to handle kernel NULL pointer dereference at virtual address 00000001 when read PC is at bmc150_accel_set_interrupt+0x98/0x194 LR is at		

2025-68330	__pm_runtime_resume+0x5c/0x64 (...) Call trace: bmc150_accel_set_interrupt from bmc150_accel_buffer_postenable+0x40/0x108 bmc150_accel_buffer_postenable from __iio_update_buffers+0xbe0/0xcbc __iio_update_buffers from enable_store+0x84/0xc8 enable_store from kernfs_fop_write_iter+0x154/0x1b4 This bug seems to have been in the driver since the beginning, but it only manifests recently, I do not know why. Store the IRQ number in the state struct, as this is a common pattern in other drivers, then use this to determine if we have IRQ support or not.	N/A	More Details
CVE-2025-68331	In the Linux kernel, the following vulnerability has been resolved: usb: uas: fix urb unmapping issue when the uas device is remove during ongoing data transfer When a UAS device is unplugged during data transfer, there is a probability of a system panic occurring. The root cause is an access to an invalid memory address during URB callback handling. Specifically, this happens when the dma_direct_unmap_sg() function is called within the usb_hcd_unmap_urb_for_dma() interface, but the sg->dma_address field is 0 and the sg data structure has already been freed. The SCSI driver sends transfer commands by invoking uas_queuecommand_lck() in uas.c, using the uas_submit_urbs() function to submit requests to USB. Within the uas_submit_urbs() implementation, three URBs (sense_urb, data_urb, and cmd_urb) are sequentially submitted. Device removal may occur at any point during uas_submit_urbs execution, which may result in URB submission failure. However, some URBs might have been successfully submitted before the failure, and uas_submit_urbs will return the -ENODEV error code in this case. The current error handling directly calls scsi_done(). In the SCSI driver, this eventually triggers scsi_complete() to invoke scsi_end_request() for releasing the sgtable. The successfully submitted URBs, when being unlinked to giveback, call usb_hcd_unmap_urb_for_dma() in hcd.c, leading to exceptions during sg unmapping operations since the sg data structure has already been freed. This patch modifies the error condition check in the uas_submit_urbs() function. When a UAS device is removed but one or more URBs have already been successfully submitted to USB, it avoids immediately invoking scsi_done() and save the cmnd to devinfo->cmnd array. If the successfully submitted URBs is completed before devinfo->resetting being set, then the scsi_done() function will be called within uas_try_complete() after all pending URB operations are finalized. Otherwise, the scsi_done() function will be called within uas_zap_pending(), which is executed after usb_kill_anchored_urbs(). The error handling only takes effect when uas_queuecommand_lck() calls uas_submit_urbs() and returns the error value -ENODEV . In this case, the device is disconnected, and the flow proceeds to uas_disconnect(), where uas_zap_pending() is invoked to call uas_try_complete().	N/A	More Details
CVE-2025-68332	In the Linux kernel, the following vulnerability has been resolved: comedi: c6xdigio: Fix invalid PNP driver unregistration The Comedi low-level driver "c6xdigio" seems to be for a parallel port connected device. When the Comedi core calls the driver's Comedi "attach" handler `c6xdigio_attach()` to configure a Comedi to use this driver, it tries to enable the parallel port PNP resources by registering a PNP driver with `pnp_register_driver()`, but ignores the return value. (The `struct pnp_driver` it uses has only the `name` and `id_table` members filled in.) The driver's Comedi "detach" handler `c6xdigio_detach()` unconditionally unregisters the PNP driver with `pnp_unregister_driver()`. It is possible for `c6xdigio_attach()` to return an error before it calls `pnp_register_driver()` and it is possible for the call to `pnp_register_driver()` to return an error (that is ignored). In both cases, the driver should not be calling `pnp_unregister_driver()` as it does in `c6xdigio_detach()`. (Note that `c6xdigio_detach()` will be called by the Comedi core if `c6xdigio_attach()` returns an error, or if the Comedi core decides to detach the Comedi device from the driver for some other reason.) The unconditional call to `pnp_unregister_driver()` without a previous successful call to `pnp_register_driver()` will cause `driver_unregister()` to issue a warning "Unexpected driver unregister!". This was detected by Syzbot [1]. Also, the PNP driver registration and unregistration should be done at module init and exit time, respectively, not when attaching or detaching Comedi devices to the driver. (There might be more than one Comedi device being attached to the driver, although that is unlikely.) Change the driver to do the PNP driver registration at module init time, and the unregistration at module exit time. Since `c6xdigio_detach()` now only calls `comedi_legacy_detach()`, remove the function and change the Comedi driver "detach" handler to `comedi_legacy_detach`. -- [1] Syzbot sample crash report: Unexpected driver unregister! WARNING: CPU: 0 PID: 5970 at drivers/base/driver.c:273 driver_unregister drivers/base/driver.c:273 [inline] WARNING: CPU: 0 PID: 5970 at drivers/base/driver.c:273 driver_unregister+0x90/0xb0 drivers/base/driver.c:270 Modules linked in: CPU: 0 UID: 0 PID: 5970 Comm: syz.0.17 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/02/2025 RIP: 0010:driver_unregister drivers/base/driver.c:273 [inline] RIP: 0010:driver_unregister+0x90/0xb0 drivers/base/driver.c:270 Code: 48 89 ef e8 c2 e6 82 fc 48 89 df e8 3a 93 ff ff 5b 5d e9 c3 6d d9 fb e8 be 6d d9 fb 90 48 c7 c7 e0 f8 1f 8c e8 51 a2 97 fb 90 <0f> 0b 90 90 5b 5d e9 a5 6d d9 fb e8 e0 f4 41 fc eb 94 e8 d9 f4 41 RSP: 0018:ffffc9000373f9a0 EFLAGS: 00010282 RAX: 0000000000000000 RBX: ffffffff8ff24720 RCX: ffffffff817b6ee8 RDX: ffff88807c932480 RSI: ffffffff817b6ef5 RDI: 0000000000000001 RBP: 0000000000000000 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000000000001 R11: 0000000000000001 R12: ffffffff8ff24660 R13: dffffc0000000000 R14: 0000000000000000 R15: ffff88814cca0000 FS: 000055556dab1500(0000) GS:ffff8881249d9000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055f77f285cd0 CR3: 000000007d871000 CR4: 00000000003526f0 Call Trace: <TASK> comedi_device_detach_locked+0x12f/0xa50 drivers/comedi/drivers.c:207 comedi_device_detach+0x67/0xb0 drivers/comedi/drivers.c:215 comedi_device_attach+0x43d/0x900 drivers/comedi/drivers.c:1011 do_devconfig_ioctl+0x1b1/0x710 drivers/comedi/comedi_fops.c:872 comedi_unlocked_ioctl+0x165d/0x2f00 drivers/comedi/comedi_fops.c:2178 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:597 [inline] __se_sys_ioctl fs/ioctl.c:583 [inline] __x64_sys_ioctl+0x18e/0x210 fs/ioctl.c:583 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_sys ---truncated---	N/A	More Details
CVE-2025-68333	In the Linux kernel, the following vulnerability has been resolved: sched_ext: Fix possible deadlock in the deferred_irq_workfn() For PREEMPT_RT=y kernels, the deferred_irq_workfn() is executed in the per-cpu irq_work/* task context and not disable-irq, if the rq returned by container_of() is current CPU's rq, the following scenarios may occur: lock(&rq->__lock); <Interrupt> lock(&rq->__lock); This commit use IRQ_WORK_INIT_HARD() to replace init_irq_work() to initialize rq->scx.deferred_irq_work, make the deferred_irq_workfn() is always invoked in hard-irq context.	N/A	More Details
CVE-2025-	In the Linux kernel, the following vulnerability has been resolved: platform/x86/amd/pmc: Add support for Van Gogh SoC The ROG Xbox Ally (non-X) SoC features a similar architecture to the Steam Deck. While the Steam Deck supports S3 (s2idle causes a crash), this support was dropped by the Xbox Ally which only S0ix suspend. Since the handler is	N/A	More Details

68334	missing here, this causes the device to not suspend and the AMD GPU driver to crash while trying to resume afterwards due to a power hang.		
CVE-2025-68335	In the Linux kernel, the following vulnerability has been resolved: comedi: pcl818: fix null-ptr-deref in pcl818_ai_cancel() Syzbot identified an issue [1] in pcl818_ai_cancel(), which stems from the fact that in case of early device detach via pcl818_detach(), subdevice dev->read_subdev may not have initialized its pointer to &struct comedi_async as intended. Thus, any such dereferencing of &s->async->cmd will lead to general protection fault and kernel crash. Mitigate this problem by removing a call to pcl818_ai_cancel() from pcl818_detach() altogether. This way, if the subdevice setups its support for async commands, everything async-related will be handled via subdevice's own ->cancel() function in comedi_device_detach_locked() even before pcl818_detach(). If no support for asynchronous commands is provided, there is no need to cancel anything either. [1] Syzbot crash: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000005: 0000 [#1] SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000028-0x000000000000002f] CPU: 1 UID: 0 PID: 6050 Comm: syz.0.18 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/18/2025 RIP: 0010:pcl818_ai_cancel+0x69/0x3f0 drivers/comedi/drivers/pcl818.c:762 ... Call Trace: <TASK> pcl818_detach+0x66/0xd0 drivers/comedi/drivers/pcl818.c:1115 comedi_device_detach_locked+0x178/0x750 drivers/comedi/drivers.c:207 do_devconfig_ioctl drivers/comedi/comedi_fops.c:848 [inline] comedi_unlocked_ioctl+0xcde/0x1020 drivers/comedi/comedi_fops.c:2178 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:597 [inline] ...	N/A	More Details
CVE-2025-68336	In the Linux kernel, the following vulnerability has been resolved: locking/spinlock/debug: Fix data-race in do_raw_write_lock KCSAN reports: BUG: KCSAN: data-race in do_raw_write_lock / do_raw_write_lock write (marked) to 0xffff800009cf504c of 4 bytes by task 1102 on cpu 1: do_raw_write_lock+0x120/0x204 _raw_write_lock_irq do_exit call_usermodehelper_exec_async ret_from_fork read to 0xffff800009cf504c of 4 bytes by task 1103 on cpu 0: do_raw_write_lock+0x88/0x204 _raw_write_lock_irq do_exit call_usermodehelper_exec_async ret_from_fork value changed: 0xffffffff -> 0x00000001 Reported by Kernel Concurrency Sanitizer on: CPU: 0 PID: 1103 Comm: kworker/u4:1 6.1.111 Commit 1a365e822372 ("locking/spinlock/debug: Fix various data races") has adressed most of these races, but seems to be not consistent/not complete. >From do_raw_write_lock() only debug_write_lock_after() part has been converted to WRITE_ONCE(), but not debug_write_lock_before() part. Do it now.	N/A	More Details
CVE-2025-68337	In the Linux kernel, the following vulnerability has been resolved: jbd2: avoid bug_on in jbd2_journal_get_create_access() when file system corrupted There's issue when file system corrupted: ------------[cut here]------------ kernel BUG at fs/jbd2/transaction.c:1289! Oops: invalid opcode: 0000 [#1] SMP KASAN PTI CPU: 5 UID: 0 PID: 2031 Comm: mkdir Not tainted 6.18.0-rc1-next RIP: 0010:jbd2_journal_get_create_access+0x3b6/0x4d0 RSP: 0018:ffff888117aafa30 EFLAGS: 00010202 RAX: 0000000000000000 RBX: ffff88811a86b000 RCX: ffffffff89a63534 RDX: 1ffff110200ec602 RSI: 0000000000000004 RDI: ffff888100763010 RBP: ffff888100763000 R08: 0000000000000001 R09: ffff888100763028 R10: 0000000000000003 R11: 0000000000000000 R12: 0000000000000000 R13: ffff88812c432000 R14: ffff88812c608000 R15: ffff888120bfc000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f91d6970c99 CR3: 00000001159c4000 CR4: 00000000000006f0 Call Trace: <TASK> __ext4_journal_get_create_access+0x42/0x170 ext4_getblk+0x319/0x6f0 ext4_bread+0x11/0x100 ext4_append+0x1e6/0x4a0 ext4_init_new_dir+0x145/0x1d0 ext4_mkdir+0x326/0x920 vfs_mkdir+0x45c/0x740 do_mkdirat+0x234/0x2f0 __x64_sys_mkdir+0xd6/0x120 do_syscall_64+0x5f/0xfa0 entry_SYSCALL_64_after_hwframe+0x76/0x7e The above issue occurs with us in errors=continue mode when accompanied by storage failures. There have been many inconsistencies in the file system data. In the case of file system data inconsistency, for example, if the block bitmap of a referenced block is not set, it can lead to the situation where a block being committed is allocated and used again. As a result, the following condition will not be satisfied then trigger BUG_ON. Of course, it is entirely possible to construct a problematic image that can trigger this BUG_ON through specific operations. In fact, I have constructed such an image and easily reproduced this issue. Therefore, J_ASSERT() holds true only under ideal conditions, but it may not necessarily be satisfied in exceptional scenarios. Using J_ASSERT() directly in abnormal situations would cause the system to crash, which is clearly not what we want. So here we directly trigger a JBD abort instead of immediately invoking BUG_ON.	N/A	More Details
CVE-2025-34452	Streama versions 1.10.0 through 1.10.5 and prior to commit b7c8767 contain a combination of path traversal and server-side request forgery (SSRF) vulnerabilities in that allow an authenticated attacker to write arbitrary files to the server filesystem. The issue exists in the subtitle download functionality, where user-controlled parameters are used to fetch remote content and construct file paths without proper validation. By supplying a crafted subtitle download URL and a path traversal sequence in the file name, an attacker can write files to arbitrary locations on the server, potentially leading to remote code execution.	N/A	More Details
CVE-2025-34451	rofl0r/proxychains-ng versions up to and including 4.17 and prior to commit cc005b7 contain a stack-based buffer overflow vulnerability in the function proxy_from_string() located in src/libproxychains.c. When parsing crafted proxy configuration entries containing overly long username or password fields, the application may write beyond the bounds of fixed-size stack buffers, leading to memory corruption or crashes. This vulnerability may allow denial of service and, under certain conditions, could be leveraged for further exploitation depending on the execution environment and applied mitigations.	N/A	More Details
CVE-2025-34450	merbanan/rtl_433 versions up to and including 25.02 and prior to commit 25e47f8 contain a stack-based buffer overflow vulnerability in the function parse_rfraw() located in src/rfraw.c. When processing crafted or excessively large raw RF input data, the application may write beyond the bounds of a stack buffer, resulting in memory corruption or a crash. This vulnerability can be exploited to cause a denial of service and, under certain conditions, may be leveraged for further exploitation depending on the execution environment and available mitigations.	N/A	More Details
CVE-2025-34449	Genymobile/scrcpy versions up to and including 3.3.3, prior to commit 3e40b24, contain a buffer overflow vulnerability in the sc_device_msg_deserialize() function. A compromised device can send crafted messages that cause out-of-bounds reads, which may result in memory corruption or a denial-of-service condition. This vulnerability may allow further exploitation on the host system.	N/A	More Details

CVE-2025-13427	An authentication bypass vulnerability in Google Cloud Dialogflow CX Messenger allowed unauthenticated users to interact with restricted chat agents, gaining access to the agents' knowledge and the ability to trigger their intents, by manipulating initialization parameters or crafting specific API requests. All versions after August 20th, 2025 have been updated to protect from this vulnerability. No user action is required for this.	N/A	More Details
CVE-2025-68145	In mcp-server-git versions prior to 2025.12.17, when the server is started with the --repository flag to restrict operations to a specific repository path, it did not validate that repo_path arguments in subsequent tool calls were actually within that configured path. This could allow tool calls to operate on other repositories accessible to the server process. The fix adds path validation that resolves both the configured repository and the requested path (following symlinks) and verifies the requested path is within the allowed repository before executing any git operations. Users are advised to upgrade to 2025.12.17 upon release to remediate this issue.	N/A	More Details
CVE-2025-61738	Under certain circumstances, attacker can capture the network key, read or write encrypted packets on the PowerG network.	N/A	More Details
CVE-2025-48863	Rejected reason: This CVE id was assigned but later discarded.	N/A	More Details
CVE-2025-68144	In mcp-server-git versions prior to 2025.12.17, the git_diff and git_checkout functions passed user-controlled arguments directly to git CLI commands without sanitization. Flag-like values (e.g., `--output=/path/to/file` for `git_diff`) would be interpreted as command-line options rather than git refs, enabling arbitrary file overwrites. The fix adds validation that rejects arguments starting with - and verifies the argument resolves to a valid git ref via rev_parse before execution. Users are advised to update to 2025.12.17 resolve this issue when it is released.	N/A	More Details
CVE-2025-68491	Rejected reason: Not used	N/A	More Details
CVE-2025-68490	Rejected reason: Not used	N/A	More Details
CVE-2025-68489	Rejected reason: Not used	N/A	More Details
CVE-2025-68488	Rejected reason: Not used	N/A	More Details
CVE-2025-68487	Rejected reason: Not used	N/A	More Details
CVE-2025-68486	Rejected reason: Not used	N/A	More Details
CVE-2025-68485	Rejected reason: Not used	N/A	More Details
CVE-2025-68484	Rejected reason: Not used	N/A	More Details
CVE-2025-68483	Rejected reason: Not used	N/A	More Details
CVE-2025-14268	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-14597	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-12700	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-34290	Versa SASE Client for Windows versions released between 7.8.7 and 7.9.4 contain a local privilege escalation vulnerability in the audit log export functionality. The client communicates user-controlled file paths to a privileged service, which performs file system operations without impersonating the requesting user. Due to improper privilege handling and a time-of-check time-of-use race condition combined with symbolic link and mount point manipulation, a local authenticated attacker can coerce the service into deleting arbitrary directories with SYSTEM privileges. This can	N/A	More Details

	be exploited to delete protected system folders such as C:\\Config.msi and subsequently achieve execution as NT AUTHORITY\\SYSTEM via MSI rollback techniques.		
CVE-2025-14319	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-11540	Path Traversal vulnerability in Sharp Display Solutions projectors allows a attacker may access and read any files within the projector.	N/A	More Details
CVE-2025-11541	Stack-based Buffer Overflow vulnerability in Sharp Display Solutions projectors allows a attacker may execute arbitrary commands and programs.	N/A	More Details
CVE-2025-11542	Stack-based Buffer Overflow vulnerability in Sharp Display Solutions projectors allows a attacker may execute arbitrary commands and programs.	N/A	More Details
CVE-2025-11543	Improper Validation of Integrity Check Value vulnerability in Sharp Display Solutions projectors allows a attacker may create and run unauthorized firmware.	N/A	More Details
CVE-2025-12049	Missing Authentication for Critical Function vulnerability in Sharp Display Solutions Media Player MP-01 All Verisons allows a attacker may access to the web interface of the affected product without authentication and change settings or perform other operations, and deliver content from the authoring software to the affected product without authentication.	N/A	More Details
CVE-2025-14267	Incomplete removal of sensitive information before transfer vulnerability in M-Files Corporation M-Files Server allows data leak exposure affecting versions before 25.12.15491.7	N/A	More Details
CVE-2025-68143	Model Context Protocol Servers is a collection of reference implementations for the model context protocol (MCP). In mcp-server-git versions prior to 2025.9.25, the git_init tool accepted arbitrary filesystem paths and created Git repositories without validating the target location. Unlike other tools which required an existing repository, git_init could operate on any directory accessible to the server process, making those directories eligible for subsequent git operations. The tool was removed entirely, as the server is intended to operate on existing repositories only. Users are advised to upgrade to 2025.9.25 or newer to remediate this issue.	N/A	More Details
CVE-2025-11544	Improper Validation of Integrity Check Value vulnerability in Sharp Display Solutions projectors allows a attacker may create and run unauthorized firmware.	N/A	More Details
CVE-2025-11545	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Sharp Display Solutions projectors allows a attacker may improperly access the HTTP server and execute arbitrary actions.	N/A	More Details
CVE-2025-68161	The Socket Appender in Apache Log4j Core versions 2.0-beta9 through 2.25.2 does not perform TLS hostname verification of the peer certificate, even when the verifyHostName https://logging.apache.org/log4j/2.x/manual/appenders/network.html#SslConfiguration-attr-verifyHostName configuration attribute or the log4j2.sslVerifyHostName https://logging.apache.org/log4j/2.x/manual/systemproperties.html#log4j2.sslVerifyHostName system property is set to true. This issue may allow a man-in-the-middle attacker to intercept or redirect log traffic under the following conditions: * The attacker is able to intercept or redirect network traffic between the client and the log receiver. * The attacker can present a server certificate issued by a certification authority trusted by the Socket Appender’s configured trust store (or by the default Java trust store if no custom trust store is configured). Users are advised to upgrade to Apache Log4j Core version 2.25.3, which addresses this issue. As an alternative mitigation, the Socket Appender may be configured to use a private or restricted trust root to limit the set of trusted certificates.	N/A	More Details
CVE-2025-66524	Apache NiFi 1.20.0 through 2.6.0 include the GetAsanaObject Processor, which requires integration with a configurable Distribute Map Cache Client Service for storing and retrieving state information. The GetAsanaObject Processor used generic Java Object serialization and deserialization without filtering. Unfiltered Java object deserialization does not provide protection against crafted state information stored in the cache server configured for GetAsanaObject. Exploitation requires an Apache NiFi system running with the GetAsanaObject Processor, and direct access to the configured cache server. Upgrading to Apache NiFi 2.7.0 is the recommended mitigation, which replaces Java Object serialization with JSON serialization. Removing the GetAsanaObject Processor located in the nifi-asana-processors-nar bundle also prevents exploitation.	N/A	More Details
CVE-2025-14881	Multiple API endpoints allowed access to sensitive files from other users by knowing the UUID of the file that were not intended to be accessible by UUID only.	N/A	More Details
CVE-2025-14882	An API endpoint allowed access to sensitive files from other users by knowing the UUID of the file that were not intended to be accessible by UUID only.	N/A	More Details
CVE-2025-	An information disclosure vulnerability in M-Files Server before versions 25.12.15491.7, 25.8 LTS SR3, 25.2 LTS SR3 and 24.8 LTS SR5 allows an authenticated attacker using M-Files Web to capture session tokens of other active users.	N/A	More Details

13008			
CVE-2025-14739	Access of Uninitialized Pointer vulnerability in TP-Link WR940N and WR941ND allows local unauthenticated attackers the ability to execute DoS attack and potentially arbitrary code execution under the context of the ‘root’ user.This issue affects WR940N and WR941ND: ≤ WR940N v5 3.20.1 Build 200316, ≤ WR941ND v6 3.16.9 Build 151203.	N/A	More Details
CVE-2025-14738	Improper authentication vulnerability in TP-Link WA850RE (httpd modules) allows unauthenticated attackers to download the configuration file.This issue affects: ≤ WA850RE V2_160527, ≤ WA850RE V3_160922.	N/A	More Details
CVE-2025-14737	Command Injection vulnerability in TP-Link WA850RE (httpd modules) allows authenticated adjacent attacker to inject arbitrary commands.This issue affects: ≤ WA850RE V2_160527, ≤ WA850RE V3_160922.	N/A	More Details
CVE-2025-67045	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2025-67041. Reason: This record is a reservation duplicate of CVE-2025-67041. Notes: All CVE users should reference CVE-2025-67041 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-67046	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2025-67037. Reason: This record is a reservation duplicate of CVE-2025-67037. Notes: All CVE users should reference CVE-2025-67037 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-68469	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to version 7.1.1-14, ImageMagick crashes when processing a crafted TIFF file. Version 7.1.1-14 fixes the issue.	N/A	More Details
CVE-2025-68278	Tina is a headless content management system. In tinacms prior to version 3.1.1, tinacms uses the gray-matter package in an insecure way allowing attackers that can control the content of the processed markdown files, e.g., blog posts, to execute arbitrary code. tinacms version 3.1.1, @tinacms/cli version 2.0.4, and @tinacms/graphql version 2.0.3 contain a fix for the issue.	N/A	More Details
CVE-2025-68457	Orejime is a consent manager that focuses on accessibility. On HTML elements handled by Orejime prior to version 2.3.2, one could run malicious code by embedding `javascript:` code within data attributes. When consenting to the related purpose, Orejime would turn data attributes into unprefixed ones (i.e. `data-href` into `href`), thus executing the code. This shouldn't have any impact on most setups, as elements handled by Orejime are generally hardcoded. The problem would only arise if somebody could inject HTML code within pages. The problem has been patched in version 2.3.2. As a workaround, the problem can be fixed outside of Orejime by sanitizing attributes which could contain executable code.	N/A	More Details
CVE-2025-64724	Arduino IDE is an integrated development environment. Prior to version 2.3.7, Arduino IDE for macOS is installed with world-writable file permissions on sensitive application components, allowing any local user to replace legitimate files with malicious code. When another user launches the application, the malicious code executes with that user's privileges, enabling privilege escalation and unauthorized access to sensitive data. The fix is included starting from the `2.3.7` release.	N/A	More Details
CVE-2025-64723	Arduino IDE is an integrated development environment. Prior to version 2.3.7, Arduino IDE for macOS was configured with overly permissive security entitlements that could bypass macOS Hardened Runtime protections. This configuration allows attackers to inject malicious dynamic libraries into the application process, gaining access to all TCC (Transparency, Consent, and Control) permissions granted to the application. The fix is included starting from the `2.3.7 ` release.	N/A	More Details
CVE-2023-5092	Rejected reason: This CVE id was assigned to an issue which was later deemed not security relevant.	N/A	More Details
CVE-2023-5093	Rejected reason: This CVE id was assigned to an issue which was later deemed not security relevant.	N/A	More Details
CVE-2023-5094	Rejected reason: This CVE id was assigned to an issue which was later deemed not security relevant.	N/A	More Details
CVE-2025-67047	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2025-67036. Reason: This record is a reservation duplicate of CVE-2025-67036. Notes: All CVE users should reference CVE-2025-67036 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-68338	In the Linux kernel, the following vulnerability has been resolved: net: dsa: microchip: Don't free uninitialized ksz_irq If something goes wrong at setup, ksz_irq_free() can be called on uninitialized ksz_irq (for example when ksz_ptp_irq_setup() fails). It leads to freeing uninitialized IRQ numbers and/or domains. Use dsa_switch_for_each_user_port_continue_reverse() in the error path to iterate only over the fully initialized ports.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: atm/fore200e: Fix possible data race in fore200e_open() Protect access to fore200e->available_cell_rate with rate_mtx lock in the error handling path of fore200e_open() to prevent a data race. The field fore200e->available_cell_rate is a shared resource used to track available bandwidth. It is concurrently accessed by fore200e_open(), fore200e_close(), and fore200e_change_qos(). In fore200e_open(), the lock rate_mtx is correctly held when subtracting vcc->qos.txtp.max_pcr from available_cell_rate to reserve bandwidth. However, if the subsequent call to fore200e_activate_vcin() fails, the function restores the reserved		More

2025-68339	bandwidth by adding back to available_cell_rate without holding the lock. This introduces a race condition because available_cell_rate is a global device resource shared across all VCCs. If the error path in fore200e_open() executes concurrently with operations like fore200e_close() or fore200e_change_qos() on other VCCs, a read-modify-write race occurs. Specifically, the error path reads the rate without the lock. If another CPU acquires the lock and modifies the rate (e.g., releasing bandwidth in fore200e_close()) between this read and the subsequent write, the error path will overwrite the concurrent update with a stale value. This results in incorrect bandwidth accounting.	N/A	Details
CVE-2025-68340	In the Linux kernel, the following vulnerability has been resolved: team: Move team device type change at the end of team_port_add Attempting to add a port device that is already up will expectedly fail, but not before modifying the team device header_ops. In the case of the syzbot reproducer the gre0 device is already in state UP when it attempts to add it as a port device of team0, this fails but before that header_ops->create of team0 is changed from eth_header to ipgre_header in the call to team_dev_type_check_change. Later when we end up in ipgre_header() struct ip_tunnel* points to nonsense as the private data of the device still holds a struct team. Example sequence of iproute2 commands to reproduce the hang/BUG(): ip link add dev team0 type team ip link add dev gre0 type gre ip link set dev gre0 up ip link set dev gre0 master team0 ip link set dev team0 up ping -I team0 1.1.1.1 Move team_dev_type_check_change down where all other checks have passed as it changes the dev type with no way to restore it in case one of the checks that follow it fail. Also make sure to preserve the origial mtu assignment: - If port_dev is not the same type as dev, dev takes mtu from port_dev - If port_dev is the same type as dev, port_dev takes mtu from dev This is done by adding a conditional before the call to dev_set_mtu to prevent it from assigning port_dev->mtu = dev->mtu and instead letting team_dev_type_check_change assign dev->mtu = port_dev->mtu. The conditional is needed because the patch moves the call to team_dev_type_check_change past dev_set_mtu. Testing: - team device driver in-tree selftests - Add/remove various devices as slaves of team device - syzbot	N/A	More Details
CVE-2025-68341	In the Linux kernel, the following vulnerability has been resolved: veth: reduce XDP no_direct return section to fix race As explain in commit fa349e396e48 ("veth: Fix race with AF_XDP exposing old or uninitialized descriptors") for veth there is a chance after napi_complete_done() that another CPU can manage start another NAPI instance running veth_pool(). For NAPI this is correctly handled as the napi_schedule_prep() check will prevent multiple instances from getting scheduled, but for the remaining code in veth_pool() this can run concurrent with the newly started NAPI instance. The problem/race is that xdp_clear_return_frame_no_direct() isn't designed to be nested. Prior to commit 401cb7dae813 ("net: Reference bpf_redirect_info via task_struct on PREEMPT_RT.") the temporary BPF net context bpf_redirect_info was stored per CPU, where this wasn't an issue. Since this commit the BPF context is stored in 'current' task_struct. When running veth in threaded-NAPI mode, then the kthread becomes the storage area. Now a race exists between two concurrent veth_pool() function calls one exiting NAPI and one running new NAPI, both using the same BPF net context. Race is when another CPU gets within the xdp_set_return_frame_no_direct() section before exiting veth_pool() calls the clear-function xdp_clear_return_frame_no_direct().	N/A	More Details
CVE-2025-68342	In the Linux kernel, the following vulnerability has been resolved: can: gs_usb: gs_usb_receive_bulk_callback(): check actual_length before accessing data The URB received in gs_usb_receive_bulk_callback() contains a struct gs_host_frame. The length of the data after the header depends on the gs_host_frame hf::flags and the active device features (e.g. time stamping). Introduce a new function gs_usb_get_minimum_length() and check that we have at least received the required amount of data before accessing it. Only copy the data to that skb that has actually been received. [mkl: rename gs_usb_get_minimum_length() -> +gs_usb_get_minimum_rx_length()]	N/A	More Details
CVE-2025-68343	In the Linux kernel, the following vulnerability has been resolved: can: gs_usb: gs_usb_receive_bulk_callback(): check actual_length before accessing header The driver expects to receive a struct gs_host_frame in gs_usb_receive_bulk_callback(). Use struct_group to describe the header of the struct gs_host_frame and check that we have at least received the header before accessing any members of it. To resubmit the URB, do not dereference the pointer chain "dev->parent->hf_size_rx" but use "parent->hf_size_rx" instead. Since "urb->context" contains "parent", it is always defined, while "dev" is not defined if the URB it too short.	N/A	More Details
CVE-2024-10398	Rejected reason: This CVE id was assigned but later discarded.	N/A	More Details
CVE-2025-58053	Galette is a membership management web application for non profit organizations. Prior to version 1.2.0, while updating any existing account with a self forged POST request, one can gain higher privileges. Version 1.2.0 fixes the issue.	N/A	More Details
CVE-2025-58935	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in axiomthemes Lunna lunna allows PHP Local File Inclusion.This issue affects Lunna: from n/a through <= 1.15.	N/A	More Details
CVE-2025-67044	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2025-67035. Reason: This record is a reservation duplicate of CVE-2025-67035. Notes: All CVE users should reference CVE-2025-67035 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-61736	Successful exploitation of this vulnerability could result in the product failing to re-establish communication once the certificate expires.	N/A	More Details
CVE-2025-43873	Successful exploitation of these vulnerabilities could allow an attacker to modify firmware and gain full access to the device.	N/A	More Details
CVE-2025-	A buffer overflow vulnerability exists in the ONVIF XML parser of Tapo C200 V3. An unauthenticated attacker on the same local network segment can send specially crafted SOAP XML requests, causing memory overflow and device	N/A	More Details

8065	crash, resulting in denial-of-service (DoS).		
CVE-2025-14300	The HTTPS service on Tapo C200 V3 exposes a connectAP interface without proper authentication. An unauthenticated attacker on the same local network segment can exploit this to modify the device’s Wi-Fi configuration, resulting in loss of connectivity and denial-of-service (DoS).	N/A	More Details
CVE-2025-14299	The HTTPS server on Tapo C200 V3 does not properly validate the Content-Length header, which can lead to an integer overflow. An unauthenticated attacker on the same local network segment can send crafted HTTPS requests to trigger excessive memory allocation, causing the device to crash and resulting in denial-of-service (DoS).	N/A	More Details
CVE-2025-14828	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-14318	Improper access checks in M-Files Server before 25.12.15491.7 allows users to download files through M-Files Web using Web Companion despite Print and Download Prevention module being enabled.	N/A	More Details
CVE-2025-66647	RIOT is an open-source microcontroller operating system, designed to match the requirements of Internet of Things (IoT) devices and other embedded devices. A vulnerability was discovered in the IPv6 fragmentation reassembly implementation of RIOT OS v2025.07. When copying the contents of the first fragment (offset=0) into the reassembly buffer, no size check is performed. It is possible to force the creation of a small reassembly buffer by first sending a shorter fragment (also with offset=0). Overflowing the reassembly buffer corrupts the state of other packet buffers which an attacker might be able to used to achieve further memory corruption (potentially resulting in remote code execution). To trigger the vulnerability, the `gnrc_ipv6_ext_frag` module must be included and the attacker must be able to send arbitrary IPv6 packets to the victim. Version 2025.10 fixes the issue.	N/A	More Details
CVE-2025-26381	Successful exploitation of this vulnerability could allow an attacker to gain unauthorized access to sensitive information.	N/A	More Details
CVE-2025-34433	AVideo versions 14.3.1 prior to 20.1 contain an unauthenticated remote code execution vulnerability caused by predictable generation of an installation salt using PHP uniqid(). The installation timestamp is exposed via a public endpoint, and a derived hash identifier is accessible through unauthenticated API responses, allowing attackers to brute-force the remaining entropy. The recovered salt can then be used to encrypt a malicious payload supplied to a notification API endpoint that evaluates attacker-controlled input, resulting in arbitrary code execution as the web server user.	N/A	More Details
CVE-2025-53922	Galette is a membership management web application for non profit organizations. Starting in version 1.1.4 and prior to version 1.2.0, a user who is logged in as group manager may bypass intended restrictions on Contributions and Transactions. Version 1.2.0 fixes the issue.	N/A	More Details
CVE-2025-68118	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to version 3.20.0, a vulnerability exists in FreeRDP’s certificate handling code on Windows platforms. The function `freerdp_certificate_data_hash_ uses` the Microsoft-specific `_snprintf` function to format certificate cache filenames without guaranteeing NUL termination when truncation occurs. According to Microsoft documentation, `_snprintf` does not append a terminating NUL byte if the formatted output exceeds the destination buffer size. If an attacker controls the hostname value (for example via server redirection or a crafted .rdp file), the resulting filename buffer may not be NUL-terminated. Subsequent string operations performed on this buffer may read beyond the allocated memory region, resulting in a heap-based out-of-bounds read. In default configurations, the connection is typically terminated before sensitive data can be meaningfully exposed, but unintended memory read or a client crash may still occur under certain conditions. Version 3.20.0 has a patch for the issue.	N/A	More Details
CVE-2025-12874	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') vulnerability in Quest Coexistence Manager for Notes (Free/Busy Connector modules) allows HTTP Request Smuggling via the Content-Length-Transfer-Encoding (CL.TE) attack vector. This could allow an attacker to bypass access controls, poison web caches, hijack sessions, or trigger unintended internal requests. This issue affects Coexistence Manager for Notes 3.8.2045. Other versions may also be affected.	N/A	More Details
CVE-2025-68655	Rejected reason: Not used	N/A	More Details
CVE-2025-34457	wb2osz/direwolf (Dire Wolf) versions up to and including 1.8, prior to commit 694c954, contain a stack-based buffer overflow vulnerability in the function kiss_rec_byte() located in src/kiss_frame.c. When processing crafted KISS frames that reach the maximum allowed frame length (MAX_KISS_LEN), the function appends a terminating FEND byte without reserving sufficient space in the stack buffer. This results in an out-of-bounds write followed by an out-of-bounds read during the subsequent call to kiss_unwrap(), leading to stack memory corruption or application crashes. This vulnerability may allow remote unauthenticated attackers to trigger a denial-of-service condition.	N/A	More Details
CVE-2025-34458	wb2osz/direwolf (Dire Wolf) versions up to and including 1.8, prior to commit 3658a87, contain a reachable assertion vulnerability in the APRS MIC-E decoder function aprs_mic_e() located in src/decode_aprs.c. When processing a specially crafted AX.25 frame containing a MIC-E message with an empty or truncated comment field, the application triggers an unhandled assertion checking for a non-empty comment. This assertion failure causes immediate process termination, allowing a remote, unauthenticated attacker to cause a denial of service by sending malformed APRS traffic.	N/A	More Details
CVE-2025-	CSRF in Ercom Cryptobox administration console allows attacker to trigger some actions on behalf of a Cryptobox administrator. The attack requires the administrator to browse a malicious web site or to click a link while he has an	N/A	More Details

14266	open session on the administration console.		
CVE-2025-67043	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2025-67038. Reason: This record is a reservation duplicate of CVE-2025-67038. Notes: All CVE users should reference CVE-2025-67038 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-68476	KEDA is a Kubernetes-based Event Driven Autoscaling component. Prior to versions 2.17.3 and 2.18.3, an Arbitrary File Read vulnerability has been identified in KEDA, potentially affecting any KEDA resource that uses TriggerAuthentication to configure HashiCorp Vault authentication. The vulnerability stems from an incorrect or insufficient path validation when loading the Service Account Token specified in spec.hashiCorpVault.credential.serviceAccount. An attacker with permissions to create or modify a TriggerAuthentication resource can exfiltrate the content of any file from the node's filesystem (where the KEDA pod resides) by directing the file's content to a server under their control, as part of the Vault authentication request. The potential impact includes the exfiltration of sensitive system information, such as secrets, keys, or the content of files like /etc/passwd. This issue has been patched in versions 2.17.3 and 2.18.3.	N/A	More Details
CVE-2025-68650	Rejected reason: Not used	N/A	More Details
CVE-2025-68651	Rejected reason: Not used	N/A	More Details
CVE-2025-68652	Rejected reason: Not used	N/A	More Details
CVE-2025-68653	Rejected reason: Not used	N/A	More Details
CVE-2025-68654	Rejected reason: Not used	N/A	More Details
CVE-2025-68696	httparty is an API tool. In versions 0.23.2 and prior, httparty is vulnerable to SSRF. This issue can pose a risk of leaking API keys, and it can also allow third parties to issue requests to internal servers. This issue has been patched via commit 0529bcd.	N/A	More Details