BULLETIN (SB25-272)

VULNERABILITY SUMMARY FOR THE WEEK OF

22ND SEPTEMBER, 2025

Bulletin (SB25-272)
Vulnerability Summary for the Week of September 22, 2025

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.
The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by the division of high, medium and low severities correspond to the following scores:

High- Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0.
Medium - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0.6.9 -
Low - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9.

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis .
The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1000projects--Beauty Parlour Management System	A vulnerability was identified in 1000projects Beauty Parlour Management System 1.0. This affects an unknown function of the file /admin/bwdates-reports-details.php. The manipulation of the argument fromdate/todate leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	2025-09-03	7.3	CVE-2025-9919
1000projects--Beauty Parlour Management System	A security vulnerability has been detected in 1000projects Beauty Parlour Management System 1.0. This impacts an unknown function of the file /admin/contact-us.php. The manipulation of the argument mobnumber leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	2025-09-03	7.3	CVE-2025-9930
aakash1911--WP likes	Cross-Site Request Forgery (CSRF) vulnerability in aakash1911 WP likes allows Reflected XSS. This issue affects WP likes: from n/a through 3.1.1.	2025-09-05	7.1	CVE-2025-58848
Akinsoft--e-Mutabakat	Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft e-Mutabakat allows Authentication Bypass.This issue affects e-Mutabakat: from 2.02.06 before v2.02.06.	2025-09-04	8.6	CVE-2025-2417
Akinsoft--LimonDesk	Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft LimonDesk allows Authentication Bypass.This issue affects LimonDesk: from s1.02.14 before v1.02.17.	2025-09-03	8.6	CVE-2025-2416
Akinsoft--LimonDesk	Origin Validation Error vulnerability in Akinsoft LimonDesk allows Forceful Browsing.This issue affects LimonDesk: from s1.02.14 before v1.02.17.	2025-09-03	7.3	CVE-2024-13068
Akinsoft--MyRezzta	Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft MyRezzta allows Authentication Bypass, Password Recovery Exploitation, Brute Force.This issue affects MyRezzta: from s2.03.01 before v2.05.01.	2025-09-03	9.8	CVE-2025-1740
Akinsoft--MyRezzta	Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft MyRezzta allows Authentication Bypass.This issue affects MyRezzta: from s2.03.01 before v2.05.01.	2025-09-03	8.6	CVE-2025-2415
Akinsoft--OctoCloud	Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft OctoCloud allows Authentication Bypass.This issue affects OctoCloud: from s1.09.03 before v1.11.01.	2025-09-02	8.6	CVE-2025-2414
Akinsoft--ProKuafor	Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft ProKuafor allows Authentication Bypass.This issue affects ProKuafor: from s1.02.08 before v1.02.08.	2025-09-02	8.6	CVE-2025-2413
Akinsoft--QR Menu	Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft QR Menu allows Authentication Bypass.This issue affects QR Menu: from s1.05.07 before v1.05.12.	2025-09-01	8.6	CVE-2025-2412
Akinsoft--TaskPano	Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft TaskPano allows Authentication Bypass.This issue affects TaskPano: from s1.06.04 before v1.06.06.	2025-09-04	8.6	CVE-2025-2411
Aknsoft--QR Men	Cross-Site Request Forgery (CSRF) vulnerability in AkÄ±nsoft QR MenÃ¼ allows Cross Site Request Forgery.This issue affects QR MenÃ¼: from s1.05.06 before v1.05.12.	2025-09-01	8.6	CVE-2025-0610
Aknsoft--QR Men	Improper Validation of Certificate with Host Mismatch vulnerability in AkÄ±nsoft QR MenÃ¼ allows HTTP Response Splitting.This issue affects QR MenÃ¼: from s1.05.05 before v1.05.12.	2025-09-01	7.3	CVE-2024-12925
alaneuler--batteryKid	A weakness has been identified in alaneuler batteryKid up to 2.1 on macOS. The affected element is an unknown function of the file PrivilegeHelper/PrivilegeHelper.swift of the component NSXPCListener. This manipulation causes missing authentication. It is possible to launch the attack on the local host. The exploit has been made available to the public and could be exploited.	2025-09-02	7.8	CVE-2025-9815
AMD--AMD EPYC 9005 Series Processors	Improper cleanup in AMD CPU microcode patch loading could allow an attacker with local administrator privilege to load malicious CPU microcode, potentially resulting in loss of integrity of x86 instruction execution.	2025-09-06	7.2	CVE-2025-0032
AMD--AMD Radeon RX 7000 Series Graphics Products	Type confusion in the ASP could allow an attacker to pass a malformed argument to the Reliability, Availability, and Serviceability trusted application (RAS TA) potentially leading to a read or write to shared memory resulting in loss of confidentiality, integrity, or availability.	2025-09-06	8.7	CVE-2023-31322
AMD--AMD Ryzen 4000 Series Mobile Processors with Radeon Graphics	Improper input validation in the GPU driver could allow an attacker to exploit a heap overflow potentially resulting in arbitrary code execution.	2025-09-06	8.8	CVE-2024-36342
AMD--AMD Ryzen 4000 Series Mobile Processors with Radeon Graphics	Improper input validation in the AMD Graphics Driver could allow an attacker to supply a specially crafted pointer, potentially leading to arbitrary writes or denial of service.	2025-09-06	8.4	CVE-2024-36352

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
AMD--AMD Ryzen 5000 Series Mobile Processors with Radeon Graphics	Insufficient bounds checking in AMD TEE (Trusted Execution Environment) could allow an attacker with a compromised userspace to invoke a command with malformed arguments leading to out of bounds memory access, potentially resulting in loss of integrity or availability.	2025-09-05	7.9	CVE-2021-26383
AMD--AMD Ryzen 7040 Series Mobile Processors with Radeon Graphics	Missing authorization in AMD RomArmor could allow an attacker to bypass ROMArmor protections during system resume from a standby state, potentially resulting in a loss of confidentiality and integrity.	2025-09-06	8.4	CVE-2024-36326
AMD--AMD Ryzen 8000 Series Desktop Processors	Improper isolation of shared resources on System-on-a-chip (SOC) could a privileged attacker to tamper with the contents of the PSP reserved DRAM region potentially resulting in loss of confidentiality and integrity.	2025-09-06	7.2	CVE-2023-31325
AMD--AMD Ryzen Threadripper 3000 Processors	Improper input validation in the system management mode (SMM) could allow a privileged attacker to overwrite arbitrary memory potentially resulting in arbitrary code execution at the SMM level.	2025-09-06	7.5	CVE-2024-21947
AMD--AMD Ryzen Threadripper 3000 Processors	Improper input validation for DIMM serial presence detect (SPD) metadata could allow an attacker with physical access, ring0 access on a system with a non-compliant DIMM, or control over the Root of Trust for BIOS update, to bypass SMM isolation potentially resulting in arbitrary code execution at the SMM level.	2025-09-06	7.5	CVE-2024-36354
argoproj--argo-cd	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. In versions 2.13.0 through 2.13.8, 2.14.0 through 2.14.15, 3.0.0 through 3.0.12 and 3.1.0-rc1 through 3.1.1, API tokens with project-level permissions are able to retrieve sensitive repository credentials (usernames, passwords) through the project details API endpoint, even when the token only has standard application management permissions and no explicit access to secrets. This vulnerability does not only affect project-level permissions. Any token with project get permissions is also vulnerable, including global permissions such as: `p, role/user, projects, get, *, allow`. This issue is fixed in versions 2.13.9, 2.14.16, 3.0.14 and 3.1.2.	2025-09-04	10	CVE-2025-55190
aThemeArt Translations--eDS Responsive Menu	Deserialization of Untrusted Data vulnerability in aThemeArt Translations eDS Responsive Menu allows Object Injection. This issue affects eDS Responsive Menu: from n/a through 1.2.	2025-09-05	7.2	CVE-2025-58839
Brent Jett--Assistant	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brent Jett Assistant allows Reflected XSS. This issue affects Assistant: from n/a through 1.5.2.	2025-09-05	7.1	CVE-2025-53307
BuddyDev--MediaPress	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in BuddyDev MediaPress allows PHP Local File Inclusion. This issue affects MediaPress: from n/a through 1.5.9.1.	2025-09-03	7.5	CVE-2025-58608
Campcodes--Computer Sales and Inventory System	A flaw has been found in Campcodes Computer Sales and Inventory System 1.0. The affected element is an unknown function of the file /pages/pos_transac.php?action=add. Executing manipulation of the argument cash/firstname can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used. Other parameters might be affected as well.	2025-09-01	7.3	CVE-2025-9794
Campcodes--Courier Management System	A vulnerability was determined in Campcodes/SourceCodester Courier Management System 1.0. Affected is the function Login of the file /ajax.php. This manipulation of the argument email causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-01	7.3	CVE-2025-9757
Campcodes--Courier Management System	A security flaw has been discovered in Campcodes/SourceCodester Courier Management System 1.0. Affected by this issue is the function Signup of the file /ajax.php. Performing manipulation of the argument lastname results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	2025-09-01	7.3	CVE-2025-9759
Campcodes--Farm Management System	A vulnerability was found in Campcodes Farm Management System 1.0. This affects an unknown part of the file /reviewInput.php. Performing manipulation of the argument rating results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	2025-09-02	7.3	CVE-2025-9811
Campcodes--Grocery Sales and Inventory System	A weakness has been identified in Campcodes Grocery Sales and Inventory System 1.0. This issue affects some unknown processing of the file /ajax.php?action=save_receiving. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	2025-09-06	7.3	CVE-2025-10030
Campcodes--Grocery Sales and Inventory System	A security vulnerability has been detected in Campcodes Grocery Sales and Inventory System 1.0. Impacted is an unknown function of the file /ajax.php?action=delete_sales. The manipulation of the argument ID leads to sql	2025-09-06	7.3	CVE-2025-10031

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.			
Campcodes--Hospital Management System	A weakness has been identified in Campcodes Hospital Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/ of the component Admin Dashboard Login. This manipulation of the argument Password causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	2025-09-01	7.3	CVE-2025-9770
Campcodes--Online Feeds Product Inventory System	A security vulnerability has been detected in Campcodes Online Feeds Product Inventory System 1.0. This vulnerability affects unknown code of the file /feeds/index.php of the component Login. The manipulation of the argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	2025-09-01	7.3	CVE-2025-9761
Campcodes--Online Learning Management System	A vulnerability was detected in Campcodes Online Learning Management System 1.0. This issue affects some unknown processing of the file /student_signup.php. The manipulation of the argument Username results in sql injection. The attack can be launched remotely. The exploit is now public and may be used.	2025-09-01	7.3	CVE-2025-9763
Campcodes--Online Learning Management System	A vulnerability was found in Campcodes Online Learning Management System 1.0. Affected is an unknown function of the file /teacher_signup.php. Performing manipulation of the argument firstname results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used. Other parameters might be affected as well.	2025-09-01	7.3	CVE-2025-9786
charmbracelet--soft-serve	Soft Serve is a self-hostable Git server for the command line. In versions 0.9.1 and below, attackers can create or override arbitrary files with uncontrolled data through its SSH API. This issue is fixed in version 0.10.0.	2025-09-03	7.7	CVE-2025-58355
ChrisHurst--Bulk Watermark	Cross-Site Request Forgery (CSRF) vulnerability in ChrisHurst Bulk Watermark allows Reflected XSS. This issue affects Bulk Watermark: from n/a through 1.6.10.	2025-09-05	7.1	CVE-2025-58845
cloudinfrastructureservices--Cloud SAML SSO Single Sign On Login	The Cloud SAML SSO plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'set_organization_settings' action of the csso_handle_actions() function in all versions up to, and including, 1.0.19. The handler reads client-supplied POST parameters for organization settings and passes them directly to update_option() without any check of the user's capabilities or a CSRF nonce. This makes it possible for unauthenticated attackers to change critical configuration (including toggling signing and encryption), potentially breaking the SSO flow and causing a denial-of-service.	2025-09-06	8.2	CVE-2025-7040
coder--coder	Coder allows organizations to provision remote development environments via Terraform. In versions 2.22.0 through 2.24.3, 2.25.0 and 2.25.1, Coder can be compromised through insecure session handling in prebuilt workspaces. Coder automatically generates a session token for a user when a workspace is started. It is automatically exposed via coder_workspace_owner.session_token. Prebuilt workspaces are initially owned by a built-in prebuilds system user. When a prebuilt workspace is claimed, a new session token is generated for the user that claimed the workspace, but the previous session token for the prebuilds user was not expired. Any Coder workspace templates that persist this automatically generated session token are potentially impacted. This is fixed in versions 2.24.4 and 2.25.2.	2025-09-06	8.1	CVE-2025-58437
CreedAlly--Bulk Featured Image	Unrestricted Upload of File with Dangerous Type vulnerability in CreedAlly Bulk Featured Image allows Upload a Web Shell to a Web Server. This issue affects Bulk Featured Image: from n/a through 1.2.2.	2025-09-05	9.1	CVE-2025-58819
D-Link--DI-8400	A weakness has been identified in D-Link DI-8400 16.07.26A1. The affected element is the function yyxz_dlink_asp of the file /yyxz.asp. This manipulation of the argument ID 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.	2025-09-03	8.8	CVE-2025-9938
D-Link--DIR-825	A vulnerability was found in D-Link DIR-825 1.08.01. This impacts the function get_ping6_app_stat of the file ping6_response.cg of the component httpd. Performing manipulation of the argument ping6_ipaddr results in buffer overflow. It is possible to initiate the attack remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-09-06	8.8	CVE-2025-10034
D-Link--DIR-852	A security vulnerability has been detected in D-Link DIR-852 1.00CN B09. Impacted is the function soapcgi_main of the file soap.cgi of the component SOAP Service. Such manipulation of the argument service leads to os command injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-09-01	7.3	CVE-2025-9752

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
David Merinas--Add to Feedly	Cross-Site Request Forgery (CSRF) vulnerability in David Merinas Add to Feedly allows Stored XSS. This issue affects Add to Feedly: from n/a through 1.2.11.	2025-09-05	7.1	CVE-2025-58859
David Merinas--Auto Last Youtube Video	Cross-Site Request Forgery (CSRF) vulnerability in David Merinas Auto Last Youtube Video allows Stored XSS. This issue affects Auto Last Youtube Video: from n/a through 1.0.7.	2025-09-05	7.1	CVE-2025-58843
Deepak S--Hide Real Download Path	Cross-Site Request Forgery (CSRF) vulnerability in Deepak S Hide Real Download Path allows Stored XSS. This issue affects Hide Real Download Path: from n/a through 1.6.	2025-09-05	7.1	CVE-2025-58849
Dejan Markovic--WordPress Buffer HYPESocial. Social Media Auto Post, Social Media Auto Publish and Schedule	Cross-Site Request Forgery (CSRF) vulnerability in Dejan Markovic WordPress Buffer - HYPESocial. Social Media Auto Post, Social Media Auto Publish and Schedule allows Reflected XSS. This issue affects WordPress Buffer - HYPESocial. Social Media Auto Post, Social Media Auto Publish and Schedule: from n/a through 2020.1.0.	2025-09-05	7.1	CVE-2025-58846
Denis V (Artprima)--AP HoneyPot WordPress Plugin	Improper Neutralization of Formula Elements in a CSV File vulnerability in Denis V (Artprima) AP HoneyPot WordPress Plugin allows Reflected XSS. This issue affects AP HoneyPot WordPress Plugin: from n/a through 1.4.	2025-09-05	7.1	CVE-2025-58855
Digilent--DASYLab	There is an out of bounds write vulnerability due to improper bounds checking resulting in invalid data when parsing a DSB file with Digilent DASYLab. This vulnerability may result in arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted DSB file. The vulnerability affects all versions of DASYLab.	2025-09-02	7.8	CVE-2025-57774
Digilent--DASYLab	There is a heap-based Buffer Overflow vulnerability due to improper bounds checking when parsing a DSB file with Digilent DASYLab. This vulnerability may result in arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted DSB file. The vulnerability affects all versions of DASYLab.	2025-09-02	7.8	CVE-2025-57775
Digilent--DASYLab	There is an out of bounds write vulnerability due to improper bounds checking resulting in an invalid address when parsing a DSB file with Digilent DASYLab. This vulnerability may result in arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted DSB file. The vulnerability affects all versions of DASYLab.	2025-09-02	7.8	CVE-2025-57776
Digilent--DASYLab	There is an out of bounds write vulnerability due to improper bounds checking in displ2.dll when parsing a DSB file with Digilent DASYLab. This vulnerability may result in arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted DSB file. The vulnerability affects all versions of DASYLab.	2025-09-02	7.8	CVE-2025-57777
Digilent--DASYLab	There is an out of bounds write vulnerability due to improper bounds checking resulting in an invalid source address when parsing a DSB file with Digilent DASYLab. This vulnerability may result in arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted DSB file. The vulnerability affects all versions of DASYLab.	2025-09-02	7.8	CVE-2025-57778
Digilent--DASYLab	There is a deserialization of untrusted data vulnerability in Digilent DASYLab. This vulnerability may result in arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted DSB file. The vulnerability affects all versions of DASYLab.	2025-09-02	7.8	CVE-2025-9188
Digilent--DASYLab	There is an out of bounds write vulnerability due to improper bounds checking resulting in a large destination address when parsing a DSB file with Digilent DASYLab. This vulnerability may result in arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted DSB file. The vulnerability affects all versions of DASYLab.	2025-09-02	7.8	CVE-2025-9189
djangoproject--Django	An issue was discovered in Django 4.2 before 4.2.24, 5.1 before 5.1.12, and 5.2 before 5.2.6. FilteredRelation is subject to SQL injection in column aliases, using a suitably crafted dictionary, with dictionary expansion, as the **kwargs passed QuerySet.annotate() or QuerySet.alias().	2025-09-03	7.1	CVE-2025-57833
docjojo--atec Debug	The atec Debug plugin for WordPress is vulnerable to remote code execution in all versions up to, and including, 1.2.22 via the 'custom_log' parameter. This is due to insufficient sanitization when saving the custom log path. This makes it possible for authenticated attackers, with Administrator-level access and above, to execute code on the server.	2025-09-04	7.2	CVE-2025-9517
docjojo--atec Debug	The atec Debug plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation on the 'debug_path' parameter in all versions up to, and including, 1.2.22. This makes it possible for authenticated attackers, with Administrator-level access and above, to delete arbitrary files on the server, which	2025-09-04	7.2	CVE-2025-9518

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	can easily lead to remote code execution when the right file is deleted (such as wp-config.php).			
Dsingh--Purge Varnish Cache	Cross-Site Request Forgery (CSRF) vulnerability in Dsingh Purge Varnish Cache allows Stored XSS. This issue affects Purge Varnish Cache: from n/a through 2.6.	2025-09-05	7.1	CVE-2025-58807
ECOVACS--DEEBOT X1 Series	ECOVACS vacuum robot base stations do not validate firmware updates, so malicious over-the-air updates can be sent to base station via insecure connection between robot and base station.	2025-09-05	7.2	CVE-2025-30199
Endress+Hauser--Promag 10 with HART	A low-privileged attacker in bluetooth range may be able to access the password of a higher-privilege user (Maintenance) by viewing the device's event log. This vulnerability could allow the Operator to authenticate as the Maintenance user, thereby gaining unauthorized access to sensitive configuration settings and the ability to modify device parameters.	2025-09-02	7.4	CVE-2025-41690
eniturechnology--LTL Freight Quotes - TQL Edition	Deserialization of Untrusted Data vulnerability in eniturechnology LTL Freight Quotes - TQL Edition allows Object Injection. This issue affects LTL Freight Quotes - TQL Edition: from n/a through 1.2.6.	2025-09-03	7.2	CVE-2025-58644
eniturechnology--LTL Freight Quotes Day & Ross Edition	Deserialization of Untrusted Data vulnerability in eniturechnology LTL Freight Quotes - Day & Ross Edition allows Object Injection. This issue affects LTL Freight Quotes - Day & Ross Edition: from n/a through 2.1.11.	2025-09-03	7.2	CVE-2025-58642
eniturechnology--LTL Freight Quotes Daylight Edition	Deserialization of Untrusted Data vulnerability in eniturechnology LTL Freight Quotes - Daylight Edition allows Object Injection. This issue affects LTL Freight Quotes - Daylight Edition: from n/a through 2.2.7.	2025-09-03	7.2	CVE-2025-58643
envoyproxy--envoy	Envoy is an open source L7 proxy and communication bus designed for large modern service oriented architectures. Versions 1.34.0 through 1.34.4 and 1.35.0 contain a use-after-free (UAF) vulnerability in the DNS cache, causing abnormal process termination. The vulnerability is in Envoy's Dynamic Forward Proxy implementation, occurring when a completion callback for a DNS resolution triggers new DNS resolutions or removes existing pending resolutions. This condition may occur when the following conditions are met: dynamic Forwarding Filter is enabled, the `envoy.reloadable_features.dfp_cluster_resolves_hosts` runtime flag is enabled, and the Host header is modified between the Dynamic Forwarding Filter and Router filters. This issue is resolved in versions 1.34.5 and 1.35.1. To work around this issue, set the envoy.reloadable_features.dfp_cluster_resolves_hosts runtime flag to false.	2025-09-02	7.5	CVE-2025-54588
ericzane--Floating Window Music Player	Cross-Site Request Forgery (CSRF) vulnerability in ericzane Floating Window Music Player allows Stored XSS. This issue affects Floating Window Music Player: from n/a through 3.4.2.	2025-09-05	7.1	CVE-2025-48104
esphome--esphome	ESPHome is a system to control microcontrollers remotely through Home Automation systems. In version 2025.8.0 in the ESP-IDF platform, ESPHome's web_server authentication check can pass incorrectly when the client-supplied base64-encoded Authorization value is empty or is a substring of the correct value. This allows access to web_server functionality (including OTA, if enabled) without knowing any information about the correct username or password. This issue has been patched in version 2025.8.1.	2025-09-02	8.1	CVE-2025-57808
ExpressTech Systems--Quiz And Survey Master	Deserialization of Untrusted Data vulnerability in ExpressTech Systems Quiz And Survey Master allows Object Injection. This issue affects Quiz And Survey Master: from n/a through 10.2.5.	2025-09-05	9.8	CVE-2025-49401
flightphp--core	The mikecao/flight PHP framework in versions prior to v1.2 is vulnerable to Denial of Service (DoS) attacks due to eager loading of request bodies in the Request class constructor. The framework automatically reads the entire request body on every HTTP request, regardless of whether the application needs it. An attacker can exploit this by sending requests with large payloads, causing excessive memory consumption and potentially exhausting available server memory, leading to application crashes or service unavailability. The vulnerability was fixed in v1.2 by implementing lazy loading of request bodies.	2025-09-03	7.5	CVE-2014-125127
frappe--erpnext	ERP is a free and open source Enterprise Resource Planning tool. In versions below 14.89.2 and 15.0.0 through 15.75.1, lack of validation of parameters left certain endpoints vulnerable to error-based SQL Injection. Some information like version could be retrieved. This issue is fixed in versions 14.89.2 and 15.76.0.	2025-09-06	8.1	CVE-2025-58439
Fuji Electric--FRENIC-Loader 4	Fuji Electric FRENIC-Loader 4 is vulnerable to a deserialization of untrusted data when importing a file through a specified window, which may allow an attacker to execute arbitrary code.	2025-09-03	7.8	CVE-2025-9365

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gavias--Indutri	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in gavias Indutri allows PHP Local File Inclusion. This issue affects Indutri: from n/a through n/a.	2025-09-05	8.1	CVE-2025-58214
gopiplus--New Simple Gallery	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in gopiplus New Simple Gallery allows Blind SQL Injection. This issue affects New Simple Gallery: from n/a through 8.0.	2025-09-05	8.5	CVE-2025-58881
HCL Software--Compass	A security vulnerability in HCL Compass can allow attacker to gain unauthorized database access.	2025-09-03	7.5	CVE-2025-0280
honojs--hono	Hono is a Web application framework that provides support for any JavaScript runtime. Versions 4.8.0 through 4.9.5 contain a flaw in the getPath utility function which could allow path confusion and potential bypass of proxy-level ACLs (e.g. Nginx location blocks). The original implementation relied on fixed character offsets when parsing request URLs. Under certain malformed absolute-form Request-URIs, this could lead to incorrect path extraction depending on the application and environment. If proxy ACLs are used to protect sensitive endpoints such as /admin, this flaw could have allowed unauthorized access. The confidentiality impact depends on what data is exposed: if sensitive administrative data is exposed, the impact may be high, otherwise it may be moderate. This issue is fixed in version 4.9.6.	2025-09-04	7.5	CVE-2025-58362
Huawei--HarmonyOS	Vulnerability of exposing object heap addresses in the Ark eTS module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-09-05	8.4	CVE-2025-58280
Huawei--HarmonyOS	Out-of-bounds read vulnerability in the runtime interpreter module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-09-05	8.4	CVE-2025-58281
Huawei--HarmonyOS	Race condition vulnerability in the audio module. Impact: Successful exploitation of this vulnerability may affect function stability.	2025-09-05	7.5	CVE-2025-58296
IBM--Transformation Advisor	IBM Transformation Advisor 2.0.1 through 4.3.1 incorrectly assigns privileges to security critical files which could allow a local root escalation inside a container running the IBM Transformation Advisor Operator Catalog image.	2025-09-03	8.4	CVE-2025-36193
imjoehaines--WordPress Error Monitoring by Bugsnag	Cross-Site Request Forgery (CSRF) vulnerability in imjoehaines WordPress Error Monitoring by Bugsnag allows Stored XSS. This issue affects WordPress Error Monitoring by Bugsnag: from n/a through 1.6.3.	2025-09-05	7.1	CVE-2025-58806
immonex--immonex Kickstart	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in immonex immonex Kickstart allows PHP Local File Inclusion. This issue affects immonex Kickstart: from n/a through 1.11.6.	2025-09-03	7.5	CVE-2025-58637
InspiryThemes--RealHomes	Incorrect Privilege Assignment vulnerability in InspiryThemes RealHomes allows Privilege Escalation.This issue affects RealHomes: from n/a through 4.3.6.	2025-09-03	9.8	CVE-2024-32444
integromat--Make Connector	The Make Connector plugin for WordPress is vulnerable to arbitrary file uploads due to misconfigured file type validation in the 'upload_media' function in all versions up to, and including, 1.5.10. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2025-09-04	7.2	CVE-2025-6085
INVELITY--Invelity MyGLS connect	Cross-Site Request Forgery (CSRF) vulnerability in INVELITY Invelity MyGLS connect allows Object Injection. This issue affects Invelity MyGLS connect: from n/a through 1.1.1.	2025-09-05	8.8	CVE-2025-58833
itsourcecode--Apartment Management System	A security vulnerability has been detected in itsourcecode Apartment Management System 1.0. This issue affects some unknown processing of the file /e_dashboard/e_all_info.php. Such manipulation of the argument mid leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	2025-09-01	7.3	CVE-2025-9792
itsourcecode--Apartment Management System	A vulnerability was detected in itsourcecode Apartment Management System 1.0. Impacted is an unknown function of the file /setting/admin.php of the component Setting Handler. Performing manipulation of the argument ddlBranch results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2025-09-01	7.3	CVE-2025-9793
itsourcecode--Online Discussion Forum	A vulnerability has been found in itsourcecode Online Discussion Forum 1.0. This affects an unknown function of the file /admin. Such manipulation of the argument Username leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	2025-09-06	7.3	CVE-2025-10033
itsourcecode--Online Discussion Forum	A flaw has been found in itsourcecode Online Discussion Forum 1.0. This affects an unknown function of the file /admin/admin_forum/add_views.php. Executing manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	2025-09-07	7.3	CVE-2025-10068
itsourcecode--Sports	A flaw has been found in itsourcecode Sports Management System 1.0. Impacted is an unknown function of the file /Admin/resultdetails.php. This manipulation of the	2025-09-01	7.3	CVE-2025-9764

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	argument ID causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.			
itsourcecode--Sports Management System	A vulnerability has been found in itsourcecode Sports Management System 1.0. The affected element is an unknown function of the file /Admin/tournament_details.php. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2025-09-01	7.3	CVE-2025-9765
itsourcecode--Sports Management System	A vulnerability was found in itsourcecode Sports Management System 1.0. The impacted element is an unknown function of the file /Admin/facilitator.php. Performing manipulation of the argument code results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	2025-09-01	7.3	CVE-2025-9766
itsourcecode--Sports Management System	A vulnerability was determined in itsourcecode Sports Management System 1.0. This affects an unknown function of the file /Admin/sporttype.php. Executing manipulation of the argument code can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-01	7.3	CVE-2025-9767
itsourcecode--Student Information Management System	A vulnerability was determined in itsourcecode Student Information Management System 1.0. This affects an unknown part of the file /admin/login.php. Executing manipulation of the argument uname can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-06	7.3	CVE-2025-10062
itsourcecode--Student Information Management System	A vulnerability was determined in itsourcecode Student Information Management System 1.0. This issue affects some unknown processing of the file /admin/modules/student/index.php. This manipulation of the argument studentId causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-02	7.3	CVE-2025-9837
itsourcecode--Student Information Management System	A vulnerability was identified in itsourcecode Student Information Management System 1.0. Impacted is an unknown function of the file /admin/modules/subject/index.php. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	2025-09-02	7.3	CVE-2025-9838
itsourcecode--Student Information Management System	A security flaw has been discovered in itsourcecode Student Information Management System 1.0. The affected element is an unknown function of the file /admin/modules/course/index.php. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.	2025-09-02	7.3	CVE-2025-9839
KaizenCoders--Enable Latex	Cross-Site Request Forgery (CSRF) vulnerability in KaizenCoders Enable Latex allows Stored XSS. This issue affects Enable Latex: from n/a through 1.2.16.	2025-09-05	7.1	CVE-2025-58860
KaizenCoders--Table of content	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KaizenCoders Table of content allows Stored XSS. This issue affects Table of content: from n/a through 1.5.3.1.	2025-09-05	7.1	CVE-2025-58857
kamleshyadav--Miraculous	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in kamleshyadav Miraculous allows Blind SQL Injection. This issue affects Miraculous: from n/a through n/a.	2025-09-05	9.3	CVE-2025-58628
kleor--Easy Timer	The Easy Timer plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.2.1 via the plugin's shortcodes. This is due to insufficient restriction of shortcode attributes. This makes it possible for authenticated attackers, with Editor-level access and above, to execute code on the server.	2025-09-04	7.2	CVE-2025-9519
MarceloTessaro--promptcraft-forge-studio	Promptcraft Forge Studio is a toolkit for evaluating, optimizing, and maintaining LLM-powered applications. All versions contain an non-exhaustive URL scheme check that does not protect against XSS. User-controlled URLs pass through src/utils/validation.ts, but the check only strips `javascript:` and a few patterns. `data:` URLs (for example data:image/svg+xml,â€¦) still pass. If a sanitized value is used in href/src, an attacker can execute a script. There is currently no fix for this issue.	2025-09-04	9.3	CVE-2025-58361
MarceloTessaro--promptcraft-forge-studio	Promptcraft Forge Studio is a toolkit for evaluating, optimizing, and maintaining LLM-powered applications. All versions of Promptcraft Forge Studio sanitize user input using regex blacklists such as r`eplace(/javascript:/gi, '')`. Because the package uses multi-character tokens and each replacement is applied only once, removing one occurrence can create a new dangerous token due to overlap. The "sanitized" value may still contain an executable payload when used in href/src (or injected into the DOM). There is currently no fix for this issue.	2025-09-04	8.2	CVE-2025-58353

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Mark O'Donnell--MSTW League Manager	Cross-Site Request Forgery (CSRF) vulnerability in Mark O'Donnell MSTW League Manager allows Stored XSS. This issue affects MSTW League Manager: from n/a through 2.10.	2025-09-05	7.1	CVE-2025-58852
Microsoft--Azure Bot Service	Azure Bot Service Elevation of Privilege Vulnerability	2025-09-04	9	CVE-2025-55244
Microsoft--Dynamics 365 FastTrack Implementation	Dynamics 365 FastTrack Implementation Assets Information Disclosure Vulnerability	2025-09-04	7.5	CVE-2025-55238
Microsoft--Microsoft Entra	Azure Entra Elevation of Privilege Vulnerability	2025-09-04	9	CVE-2025-55241
Microsoft--Networking	Azure Networking Elevation of Privilege Vulnerability	2025-09-04	10	CVE-2025-54914
Mitsubishi Electric Corporation--MELSEC iQ-F Series FX5U-32MT/ES	Missing Authentication for Critical Function vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series CPU module allows a remote unauthenticated attacker to read or write the device values of the product and stop the operation of the programs, since MODBUS/TCP in the products does not have authentication features.	2025-09-01	7.3	CVE-2025-7405
Mitsubishi Electric Corporation--MELSEC iQ-F Series FX5U-32MT/ES	Cleartext Transmission of Sensitive Information vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series CPU module allows a remote unauthenticated attacker to obtain credential information by intercepting SLMP communication messages, and read or write the device values of the product and stop the operations of programs by using the obtained credential information.	2025-09-01	7.5	CVE-2025-7731
mondula2016--Multi Step Form	The Multi Step Form plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation via the import functionality in all versions up to, and including, 1.7.25. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2025-09-06	7.2	CVE-2025-9515
n/a--RemoteClinic	A vulnerability was detected in RemoteClinic up to 2.0. This affects an unknown part of the file /staff/edit.php. Performing manipulation of the argument image results in unrestricted upload. 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.	2025-09-01	7.3	CVE-2025-9772
n/a--RemoteClinic	A vulnerability was found in RemoteClinic up to 2.0. Impacted is an unknown function of the file /staff/edit-my-profile.php. The manipulation of the argument image results in unrestricted upload. The attack may be launched remotely. The exploit has been made public and could be used.	2025-09-01	7.3	CVE-2025-9775
N/A--smolagents	Incomplete validation of dunder attributes allows an attacker to escape from the Local Python execution environment sandbox, enforced by smolagents. The attack requires a Prompt Injection in order to trick the agent to create malicious code.	2025-09-03	7.6	CVE-2025-9959
nanbingxyz--5ire	5ire is a cross-platform desktop artificial intelligence assistant and model context protocol client. Version 0.13.2 contains a vulnerability in the chat page's script gadgets that enables content injection attacks through multiple vectors: malicious prompt injection pages, compromised MCP servers, and exploited tool integrations. This is fixed in version 0.14.0.	2025-09-04	9.7	CVE-2025-58357
Nick Ciske--To Lead For Salesforce	Cross-Site Request Forgery (CSRF) vulnerability in Nick Ciske To Lead For Salesforce allows Reflected XSS. This issue affects To Lead For Salesforce: from n/a through 2.7.3.9.	2025-09-05	7.1	CVE-2025-58809
NVIDIA--BlueField GA	NVIDIA BlueField contains a vulnerability in the management interface, where an attacker with local access could cause incorrect authorization to modify the configuration. A successful exploit of this vulnerability might lead to denial of service, escalation of privileges, information disclosure, and data tampering.	2025-09-04	8.7	CVE-2025-23256
NVIDIA--NVIDIA DOCA with collectx-clxapidev	NVIDIA DOCA contains a vulnerability in the collectx-clxapidev Debian package that could allow an actor with low privileges to escalate privileges. A successful exploit of this vulnerability might lead to escalation of privileges.	2025-09-04	7.3	CVE-2025-23257
NVIDIA--NVIDIA DOCA with collectx-dpeserver	NVIDIA DOCA contains a vulnerability in the collectx-dpeserver Debian package for arm64 that could allow an attacker with low privileges to escalate privileges. A successful exploit of this vulnerability might lead to escalation of privileges.	2025-09-04	7.3	CVE-2025-23258
OpenAgentPlatform--Dive	Dive is an open-source MCP Host Desktop Application that enables integration with function-calling LLMs. In versions 0.9.0 through 0.9.3, there is a one-click Remote Code Execution vulnerability triggered through a custom url value, `transport` in the JSON object. An attacker can exploit the vulnerability in the following two scenarios: a victim visits a malicious website controlled by the attacker and the website redirect to the URL automatically, or a victim clicks on such a crafted link embedded on a legitimate website (e.g., in user-generated content). In both cases,	2025-09-03	8.8	CVE-2025-58176

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the browser invokes Dive's custom URL handler (dive:), which launches the Dive app and processes the crafted URL, leading to arbitrary code execution on the victim's machine. This vulnerability is caused by improper processing of custom url. This is fixed in version 0.9.4.			
OTWthemes--Popping Sidebars and Widgets Light	Cross-Site Request Forgery (CSRF) vulnerability in OTWthemes Popping Sidebars and Widgets Light allows Reflected XSS. This issue affects Popping Sidebars and Widgets Light: from n/a through 1.27.	2025-09-05	7.1	CVE-2025-58853
pgadmin.org--pgAdmin 4	pgAdmin <= 9.7 is affected by a Cross-Origin Opener Policy (COOP) vulnerability. This vulnerability allows an attacker to manipulate the OAuth flow, potentially leading to unauthorised account access, account takeover, data breaches, and privilege escalation.	2025-09-04	7.9	CVE-2025-9636
PHPGurukul--Beauty Parlour Management System	A security flaw has been discovered in PHPGurukul Beauty Parlour Management System 1.1. Impacted is an unknown function of the file /admin/contact-us.php. The manipulation of the argument mobnumber results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	2025-09-02	7.3	CVE-2025-9814
PHPGurukul--Beauty Parlour Management System	A vulnerability was identified in PHPGurukul Beauty Parlour Management System 1.1. The impacted element is an unknown function of the file /signup.php. The manipulation of the argument mobilenumber leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. Other parameters might be affected as well.	2025-09-02	7.3	CVE-2025-9829
PHPGurukul--Beauty Parlour Management System	A security flaw has been discovered in PHPGurukul Beauty Parlour Management System 1.1. This affects an unknown function of the file /admin/add-customer-services.php. The manipulation of the argument sids[] results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	2025-09-02	7.3	CVE-2025-9830
PHPGurukul--Beauty Parlour Management System	A weakness has been identified in PHPGurukul Beauty Parlour Management System 1.1. This impacts an unknown function of the file /admin/edit-services.php. This manipulation of the argument sername causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	2025-09-02	7.3	CVE-2025-9831
PHPGurukul--Beauty Parlour Management System	A flaw has been found in PHPGurukul Beauty Parlour Management System 1.1. Affected by this vulnerability is an unknown functionality of the file /admin/update-image.php. This manipulation of the argument lid causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	2025-09-03	7.3	CVE-2025-9932
PHPGurukul--Beauty Parlour Management System	A vulnerability has been found in PHPGurukul Beauty Parlour Management System 1.1. Affected by this issue is some unknown functionality of the file /admin/view-appointment.php. Such manipulation of the argument viewid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2025-09-03	7.3	CVE-2025-9933
PHPGurukul--Online Course Registration	A vulnerability has been found in PHPGurukul Online Course Registration 3.1. Affected is an unknown function of the file /admin/semester.php. The manipulation of the argument semester leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2025-09-05	7.3	CVE-2025-10025
Progress Software Corporation--OpenEdge	It was possible to perform Remote Command Execution (RCE) via Java RMI interface in the OpenEdge AdminServer, allowing authenticated users to inject and execute OS commands under the delegated authority of the AdminServer process. An RMI interface permitted manipulation of a configuration property with inadequate input validation leading to OS command injection.	2025-09-04	8.4	CVE-2025-7388
projectworlds--Travel Management System	A vulnerability has been found in projectworlds Travel Management System 1.0. This vulnerability affects unknown code of the file /enquiry.php. The manipulation of the argument t2 leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	2025-09-03	7.3	CVE-2025-9924
projectworlds--Travel Management System	A vulnerability was found in projectworlds Travel Management System 1.0. This issue affects some unknown processing of the file /detail.php. The manipulation of the argument pid results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	2025-09-03	7.3	CVE-2025-9925
projectworlds--Travel Management System	A vulnerability was determined in projectworlds Travel Management System 1.0. Impacted is an unknown function of the file /viewsubcategory.php. This manipulation of the argument t1 causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-03	7.3	CVE-2025-9926
projectworlds--Travel	A vulnerability was identified in projectworlds Travel Management System 1.0. The affected element is an unknown function of the file /viewpackage.php. Such	2025-09-03	7.3	CVE-2025-9927

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	manipulation of the argument t1 leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.			
projectworlds--Travel Management System	A security flaw has been discovered in projectworlds Travel Management System 1.0. The impacted element is an unknown function of the file /viewcategory.php. Performing manipulation of the argument t1 results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	2025-09-03	7.3	CVE-2025-9928
PTZOptics--PT12X-SE-xx-G3	PTZOptics and possibly other ValueHD-based pan-tilt-zoom cameras use hard-coded, default administrative credentials. The passwords can readily be cracked. Many cameras have SSH or telnet listening on all interfaces. The passwords cannot be changed by the user, nor can the SSH or telnet service be disabled by the user.	2025-09-05	9.8	CVE-2025-35451
PTZOptics--PT12X-SE-xx-G3	PTZOptics and possibly other ValueHD-based pan-tilt-zoom cameras use default, shared credentials for the administrative web interface.	2025-09-05	9.8	CVE-2025-35452
RealMag777--InPost Gallery	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in RealMag777 InPost Gallery allows PHP Local File Inclusion. This issue affects InPost Gallery: from n/a through 2.1.4.5.	2025-09-05	7.5	CVE-2025-57889
Red Hat--Red Hat build of Apache Camel for Spring Boot 4	A flaw was found in Undertow where malformed client requests can trigger server-side stream resets without triggering abuse counters. This issue, referred to as the "MadeYouReset" attack, allows malicious clients to induce excessive server workload by repeatedly causing server-side stream aborts. While not a protocol bug, this highlights a common implementation weakness that can be exploited to cause a denial of service (DoS).	2025-09-02	7.5	CVE-2025-9784
Red Hat--Red Hat Enterprise Linux 10	There's a vulnerability in podman where an attacker may use the kube play command to overwrite host files when the kube file container a Secrete or a ConfigMap volume mount and such volume contains a symbolic link to a host file path. In a successful attack, the attacker can only control the target file to be overwritten but not the content to be written into the file. Binary-Affected: podman Upstream-version-introduced: v4.0.0 Upstream-version-fixed: v5.6.1	2025-09-05	8.1	CVE-2025-9566
RooCodeInc--Roo-Code	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. Versions below 3.26.0 contain a vulnerability in the command parsing logic where the Bash parameter expansion and indirect reference were not handled correctly. If the agent was configured to auto-approve execution of certain commands, an attacker able to influence prompts could abuse this weakness to execute additional arbitrary commands alongside the intended one. This is fixed in version 3.26.0.	2025-09-05	8.1	CVE-2025-58370
RooCodeInc--Roo-Code	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. Versions 3.25.23 and below contain a vulnerability where certain VS Code workspace configuration files (.code-workspace) are not protected in the same way as the .vscode folder. If the agent was configured to auto-approve file writes, an attacker able to influence prompts (for example via prompt injection) could cause malicious workspace settings or tasks to be written. These tasks could then be executed automatically when the workspace is reopened, resulting in arbitrary code execution. This issue is fixed in version 3.26.0.	2025-09-05	8.1	CVE-2025-58372
RooCodeInc--Roo-Code	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. Versions 3.25.23 and below contain a default list of allowed commands that do not need manual approval if auto-approve is enabled, and npm install is included in that list. Because npm install executes lifecycle scripts, if a repository's package.json file contains a malicious postinstall script, it would be executed automatically without user approval. This means that enabling auto-approved commands and opening a malicious repo could result in arbitrary code execution. This is fixed in version 3.26.0.	2025-09-06	7.8	CVE-2025-58374
Rubel Miah--Aitasi Coming Soon	Deserialization of Untrusted Data vulnerability in Rubel Miah Aitasi Coming Soon allows Object Injection. This issue affects Aitasi Coming Soon: from n/a through 2.0.2.	2025-09-05	7.2	CVE-2025-58815
Saad Iqbal--License Manager for WooCommerce	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saad Iqbal License Manager for WooCommerce allows Blind SQL Injection. This issue affects License Manager for WooCommerce: from n/a through 3.0.12.	2025-09-05	7.6	CVE-2025-58788
Samer Bechara--Ultimate AJAX Login	Cross-Site Request Forgery (CSRF) vulnerability in Samer Bechara Ultimate AJAX Login allows Reflected XSS. This issue affects Ultimate AJAX Login: from n/a through 1.2.1.	2025-09-05	7.1	CVE-2025-58854
Samsung Mobile--GoodLock	Improper export of component in GoodLock prior to version 2.2.04.95 allows local attackers to install arbitrary applications from Galaxy Store.	2025-09-04	7.7	CVE-2024-34598
Samsung Mobile--Samsung Mobile Devices	Out-of-bounds Write vulnerability in libaudiosaplus_sec.so library prior to SMR Apr-2023 Release 1 allows local attacker to execute arbitrary code.	2025-09-03	8	CVE-2023-21475

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Samsung Mobile--Samsung Mobile Devices	Out-of-bounds Write vulnerability in libaudiosaplus_sec.so library prior to SMR Apr-2023 Release 1 allows local attacker to execute arbitrary code.	2025-09-03	8	CVE-2023-21476
Samsung Mobile--Samsung Mobile Devices	Improper input validation vulnerability in CertByte prior to SMR Apr-2023 Release 1 allows local attackers to launch privileged activities.	2025-09-03	8.5	CVE-2023-21480
Samsung Mobile--Samsung Mobile Devices	Access of Memory Location After End of Buffer vulnerability in TIGERF trustlet prior to SMR Apr-2023 Release 1 allows local attackers to access protected data.	2025-09-03	7.9	CVE-2023-21477
ScienceLogic--SL1	index.em7 in ScienceLogic SL1 before 12.1.1 allows SQL Injection via a parameter in a request.	2025-09-05	7.2	CVE-2025-58780
ScriptAndTools--Real Estate Management System	A security vulnerability has been detected in ScriptAndTools Real Estate Management System 1.0. The affected element is an unknown function of the file /admin/userlist.php. Such manipulation leads to execution after redirect. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	2025-09-03	7.3	CVE-2025-9848
scriptsbundle--AdForest	The AdForest theme for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 6.0.9. This is due to the plugin not properly verifying a user's identity prior to authenticating them. This makes it possible for unauthenticated attackers to log in as other users, including administrators, without access to a password.	2025-09-06	9.8	CVE-2025-8359
Sitecore--Experience Manager (XM)	Deserialization of Untrusted Data vulnerability in Sitecore Experience Manager (XM), Sitecore Experience Platform (XP) allows Code Injection.This issue affects Experience Manager (XM): through 9.0; Experience Platform (XP): through 9.0.	2025-09-03	9	CVE-2025-53690
Sitecore--Experience Manager (XM)	Deserialization of Untrusted Data vulnerability in Sitecore Experience Manager (XM), Sitecore Experience Platform (XP) allows Remote Code Execution (RCE).This issue affects Experience Manager (XM): from 9.0 through 9.3, from 10.0 through 10.4; Experience Platform (XP): from 9.0 through 9.3, from 10.0 through 10.4.	2025-09-03	8.8	CVE-2025-53691
Sitecore--Sitecore Experience Manager (XM)	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in Sitecore Sitecore Experience Manager (XM), Sitecore Experience Platform (XP) allows Cache Poisoning.This issue affects Sitecore Experience Manager (XM): from 9.0 through 9.3, from 10.0 through 10.4; Experience Platform (XP): from 9.0 through 9.3, from 10.0 through 10.4.	2025-09-03	9.8	CVE-2025-53693
Sitecore--Sitecore Experience Manager (XM)	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Sitecore Sitecore Experience Manager (XM), Sitecore Experience Platform (XP).This issue affects Sitecore Experience Manager (XM): from 9.2 through 10.4; Experience Platform (XP): from 9.2 through 10.4.	2025-09-03	7.5	CVE-2025-53694
sizam--REHub - Price Comparison, Multi Vendor Marketplace Wordpress Theme	The The REHub - Price Comparison, Multi Vendor Marketplace Wordpress Theme theme for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 19.9.7. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	2025-09-06	7.3	CVE-2025-7366
smackcoders--WordPress Helpdesk Integration	The WordPress Helpdesk Integration plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 5.8.10 via the portal_type parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	2025-09-05	8.1	CVE-2025-9990
SolarWinds--Web Help Desk	SolarWinds Web Help Desk was found to be susceptible to a Java Deserialization Remote Code Execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. This vulnerability was found by the ZDI team after researching a previous vulnerability and providing this report. The ZDI team was able to discover an unauthenticated attack during their research. We recommend all Web Help Desk customers apply the patch, which is now available. We thank Trend Micro Zero Day Initiative (ZDI) for its ongoing partnership in coordinating with SolarWinds on responsible disclosure of this and other potential vulnerabilities.	2025-09-01	9.8	CVE-2024-28988
SonarSource--sonarqube-scan-action	SonarQube Server and Cloud is a static analysis solution for continuous code quality and security inspection. In versions 4 to 5.3.0, a command injection vulnerability was discovered in the SonarQube Scan GitHub Action that allows untrusted input arguments to be processed without proper sanitization. Arguments sent to the action are treated as shell expressions, allowing potential	2025-09-02	7.8	CVE-2025-58178

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution of arbitrary commands. A fix has been released in SonarQube Scan GitHub Action 5.3.1.			
SourceCodester--Eye Clinic Management System	A security vulnerability has been detected in SourceCodester Eye Clinic Management System 1.0. Affected by this issue is some unknown functionality of the file /main/search_index_Diagnosis.php. Such manipulation of the argument Search leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	2025-09-01	7.3	CVE-2025-9771
SourceCodester--Food Ordering Management System	A security vulnerability has been detected in SourceCodester Food Ordering Management System 1.0. Affected is an unknown function of the file /routers/register-router.php. Such manipulation of the argument phone leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	2025-09-02	7.3	CVE-2025-9832
SourceCodester--Hotel Reservation System	A security flaw has been discovered in SourceCodester Hotel Reservation System 1.0. This affects an unknown part of the file /admin/updateabout.php. The manipulation of the argument address results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be exploited.	2025-09-01	7.3	CVE-2025-9790
SourceCodester--Online Farm Management System	A vulnerability was detected in SourceCodester Online Farm Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /Login/login.php. Performing manipulation of the argument uname results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	2025-09-02	7.3	CVE-2025-9833
SourceCodester--Online Hotel Reservation System	A vulnerability was identified in SourceCodester Online Hotel Reservation System 1.0. Affected by this issue is some unknown functionality of the file /admin/edituser.php. The manipulation of the argument userid leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	2025-09-01	7.3	CVE-2025-9789
SourceCodester--School Log Management System	A vulnerability was determined in SourceCodester/Campcodes School Log Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/admin_class.php. Executing manipulation of the argument id_no can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-01	7.3	CVE-2025-9788
Stefan Keller--WooCommerce Payment Gateway for Saferpay	Path Traversal vulnerability in Stefan Keller WooCommerce Payment Gateway for Saferpay allows Path Traversal. This issue affects WooCommerce Payment Gateway for Saferpay: from n/a through 0.4.9.	2025-09-05	7.5	CVE-2025-48317
Subhash Kumar--Database to Excel	Cross-Site Request Forgery (CSRF) vulnerability in Subhash Kumar Database to Excel allows Stored XSS. This issue affects Database to Excel: from n/a through 1.0.	2025-09-05	7.1	CVE-2025-58844
SUSE--Rancher	Unauthorized disclosure of sensitive data: Any user with `GET` or `LIST` permissions on `BundleDeployment` resources could retrieve Helm values containing credentials or other secrets.	2025-09-02	7.7	CVE-2024-52284
SUSE--rancher	A vulnerability has been identified within Rancher Manager in which it did not enforce request body size limits on certain public (unauthenticated) and authenticated API endpoints. This allows a malicious user to exploit this by sending excessively large payloads, which are fully loaded into memory during processing, leading to Denial of Service (DoS).	2025-09-02	8.2	CVE-2024-58259
Tenda--AC20	A weakness has been identified in Tenda AC20 16.03.08.05. This vulnerability affects unknown code of the file /goform/fromAdvSetMacMtuWan. This manipulation of the argument wanMTU causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	2025-09-01	8.8	CVE-2025-9791
Tenda--CH22	A vulnerability was determined in Tenda CH22 1.0.0.1. This vulnerability affects the function formexeCommand of the file /goform/exeCommand. Executing manipulation of the argument cmdinput can lead to buffer overflow. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	2025-09-02	8.8	CVE-2025-9812
Tenda--CH22	A vulnerability was identified in Tenda CH22 1.0.0.1. This issue affects the function formSetSambaConf of the file /goform/SetSambaConf. The manipulation of the argument samba_userNameSda leads to buffer overflow. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	2025-09-02	8.8	CVE-2025-9813
Themeisle--WP Full Stripe Free	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeisle WP Full Stripe Free allows SQL Injection. This issue affects WP Full Stripe Free: from n/a through 8.3.0.	2025-09-05	7.6	CVE-2025-58789

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ThemeMove--MaxCoach	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in ThemeMove MaxCoach allows PHP Local File Inclusion. This issue affects MaxCoach: from n/a through 3.2.5.	2025-09-05	8.1	CVE-2025-58206
TOTOLINK--A702R	A vulnerability was detected in TOTOLINK A702R 4.0.0-B20211108.1423. Affected by this vulnerability is the function sub_4162DC of the file /boafrm/formFilter. The manipulation of the argument ip6addr results in buffer overflow. It is possible to launch the attack remotely. The exploit is now public and may be used.	2025-09-01	8.8	CVE-2025-9779
TOTOLINK--A702R	A flaw has been found in TOTOLINK A702R 4.0.0-B20211108.1423. Affected by this issue is the function sub_419BE0 of the file /boafrm/formIpQoS. This manipulation of the argument mac causes buffer overflow. The attack can be initiated remotely. The exploit has been published and may be used.	2025-09-01	8.8	CVE-2025-9780
TOTOLINK--A702R	A vulnerability has been found in TOTOLINK A702R 4.0.0-B20211108.1423. This affects the function sub_4162DC of the file /boafrm/formFilter. Such manipulation of the argument ip6addr leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2025-09-01	8.8	CVE-2025-9781
TOTOLINK--A702R	A vulnerability was found in TOTOLINK A702R 4.0.0-B20211108.1423. This vulnerability affects the function sub_4466F8 of the file /boafrm/formOneKeyAccessButton. Performing manipulation of the argument submit-url results in buffer overflow. The attack may be initiated remotely. The exploit has been made public and could be used.	2025-09-01	8.8	CVE-2025-9782
TOTOLINK--A702R	A vulnerability was determined in TOTOLINK A702R 4.0.0-B20211108.1423. This issue affects the function sub_418030 of the file /boafrm/formParentControl. Executing manipulation of the argument submit-url can lead to buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-01	8.8	CVE-2025-9783
TOTOLINK--N600R	A vulnerability was determined in TOTOLINK N600R 4.3.0cu.7866_B20220506. This vulnerability affects the function sub_4159F8 of the file /web_cste/cgi-bin/cstecgi.cgi. Executing manipulation can lead to command injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-03	7.3	CVE-2025-9935
Wireshark Foundation--Wireshark	SSH dissector crash in Wireshark 4.4.0 to 4.4.8 allows denial of service	2025-09-03	7.8	CVE-2025-9817
withastro--astro	Astro is a web framework for content-driven websites. Versions 11.0.3 through 12.6.5 are vulnerable to SSRF when using Astro's Cloudflare adapter. When configured with output: 'server' while using the default imageService: 'compile', the generated image optimization endpoint doesn't check the URLs it receives, allowing content from unauthorized third-party domains to be served. a A bug in impacted versions of the @astrojs/cloudflare adapter for deployment on Cloudflare's infrastructure, allows an attacker to bypass the third-party domain restrictions and serve any content from the vulnerable origin. This issue is fixed in version 12.6.6.	2025-09-04	7.2	CVE-2025-58179
WP Corner--Quick Event Calendar	Cross-Site Request Forgery (CSRF) vulnerability in WP Corner Quick Event Calendar allows Stored XSS. This issue affects Quick Event Calendar: from n/a through 1.4.9.	2025-09-05	7.1	CVE-2025-58861
WPFunnels--Mail Mint	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPFunnels Mail Mint allows SQL Injection. This issue affects Mail Mint: from n/a through 1.18.5.	2025-09-03	7.6	CVE-2025-58604
Yaidier--WN Flipbox Pro	Cross-Site Request Forgery (CSRF) vulnerability in Yaidier WN Flipbox Pro allows Reflected XSS. This issue affects WN Flipbox Pro: from n/a through 2.1.	2025-09-05	7.1	CVE-2025-58847
zcaceres--markdownify-mcp	Markdownify is a Model Context Protocol server for converting almost anything to Markdown. Versions below 0.0.2 contain a command injection vulnerability, caused by the unsanitized use of input parameters within a call to child_process.exec, enabling an attacker to inject arbitrary system commands. Successful exploitation can lead to remote code execution under the server process's privileges. The server constructs and executes shell commands using unvalidated user input directly within command-line strings. This introduces the possibility of shell metacharacter injection (|, >, &&, etc.). This issue is fixed in version 0.0.2.	2025-09-04	7.5	CVE-2025-58358
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30254, 20.005.30774, 25.001.20672 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file, and scope is unchanged.	2025-09-09	7.8	CVE-2025-54257
Adobe--Adobe Commerce	Adobe Commerce versions 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 and earlier are affected by an Improper Input Validation vulnerability. A successful attacker can abuse this to achieve session takeover, increasing the	2025-09-09	9.1	CVE-2025-54236

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	confidentiality, and integrity impact to high. Exploitation of this issue does not require user interaction.			
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Scope is changed	2025-09-09	7.7	CVE-2025-54248
Adobe--ColdFusion	ColdFusion versions 2025.3, 2023.15, 2021.21 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary code execution by an attacker. Scope is changed.	2025-09-09	9	CVE-2025-54261
Adobe--Dreamweaver Desktop	Dreamweaver Desktop versions 21.5 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must click on a malicious link, and scope is changed.	2025-09-09	8.6	CVE-2025-54256
Adobe--Premiere Pro	Premiere Pro versions 25.3, 24.6.5 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file, and scope is unchanged.	2025-09-09	7.8	CVE-2025-54242
Adobe--Substance3D - Modeler	Substance3D - Modeler versions 1.22.2 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is unchanged.	2025-09-09	7.8	CVE-2025-54258
Adobe--Substance3D - Modeler	Substance3D - Modeler versions 1.22.2 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is unchanged.	2025-09-09	7.8	CVE-2025-54259
Adobe--Substance3D - Modeler	Substance3D - Modeler versions 1.22.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is unchanged.	2025-09-09	7.8	CVE-2025-54260
Adobe--Substance3D - Viewer	Substance3D - Viewer versions 0.25.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-09-09	7.8	CVE-2025-54243
Adobe--Substance3D - Viewer	Substance3D - Viewer versions 0.25.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-09-09	7.8	CVE-2025-54244
Adobe--Substance3D - Viewer	Substance3D - Viewer versions 0.25.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-09-09	7.8	CVE-2025-54245
AMI--AptioV	APTIOV contains vulnerabilities in the BIOS where a privileged user may cause "Write-what-where Condition" and "Exposure of Sensitive Information to an Unauthorized Actor" through local access. The successful exploitation of these vulnerabilities can lead to information disclosure, arbitrary data writing, and impact Confidentiality, Integrity, and Availability.	2025-09-09	8.2	CVE-2025-33045
aurelienlws--LWS Cleaner	The LWS Cleaner plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the 'lws_cl_delete_file' function in all versions up to, and including, 2.4.1.3. This makes it possible for authenticated attackers, with Administrator-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	2025-09-12	7.2	CVE-2025-8575
axios--axios	Axios is a promise based HTTP client for the browser and Node.js. When Axios prior to version 1.11.0 runs on Node.js and is given a URL with the `data:` scheme, it does not perform HTTP. Instead, its Node http adapter decodes the entire payload into memory (`Buffer`/`Blob`) and returns a synthetic 200 response. This path ignores `maxContentLength` / `maxBodyLength` (which only protect HTTP responses), so an attacker can supply a very large `data:` URI and cause the process to allocate unbounded memory and crash (DoS), even if the caller requested `responseType: 'stream'`. Version 1.11.0 contains a patch for the issue.	2025-09-12	7.5	CVE-2025-58754
AxxonSoft--AxxonOne	Use of Unmaintained Third Party Components (CWE-1104) in the NuGet dependency components in AxxonSoft Axxon One VMS 2.0.0 through 2.0.4 on	2025-09-10	9.8	CVE-2025-10220

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Windows allows a remote attacker to execute arbitrary code or bypass security features via exploitation of vulnerable third-party packages such as Google.Protobuf, DynamicData, System.Runtime.CompilerServices.Unsafe, and others.			
AxxonSoft--AxxonOne	Dependency on Vulnerable Third-Party Component (CWE-1395) in the PostgreSQL backend in AxxonSoft Axxon One 2.0.8 and earlier on Windows and Linux allows a remote attacker to escalate privileges, execute arbitrary code, or cause denial-of-service via exploitation of multiple known CVEs present in PostgreSQL v10.x, which are resolved in PostgreSQL 17.4.	2025-09-10	9.8	CVE-2025-10226
AxxonSoft--AxxonOne	Improper Restriction of Operations within the Bounds of a Memory Buffer (CWE-119) in the OpenSSL-based session module in AxxonSoft Axxon One 2.0.6 and earlier on Windows allows a remote attacker under high load conditions to cause application crashes or unpredictable behavior via triggering memory reallocation errors when handling expired session keys.	2025-09-10	7.5	CVE-2025-10225
Baicells--NEUTRINO430	Use of Default Cryptographic Key (CWE-1394)	2025-09-09	9.1	CVE-2025-55049
Baicells--NEUTRINO430, NOVA436Q, NOVA430e/430i, NOVA846, NOVA246, NOVA243, NOVA233, NOVA227	Multiple CWE-78	2025-09-09	9.8	CVE-2025-55048
Baicells--NOVA430e/430i, NOVA436Q, NEUTRINO430, NOVA846	CWE-1392: Use of Default Credentials	2025-09-09	10	CVE-2025-55051
Baicells--NOVA430e/430i, NOVA436Q, NEUTRINO430, NOVA846	CWE-1242: Inclusion of Undocumented Features	2025-09-09	9.8	CVE-2025-55050
Baicells--SPECTRA LTE-U eNB	CWE-798 Use of Hard-coded Credentials	2025-09-09	8.4	CVE-2025-55047
Bearsthemes--Goza - Nonprofit Charity WordPress Theme	The Goza - Nonprofit Charity WordPress Theme theme for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the alone_import_pack_restore_data() function in all versions up to, and including, 3.2.2. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	2025-09-09	9.1	CVE-2025-10134
Beckhoff--TE1000 | TwinCAT 3 Enineering	An unauthenticated attacker can trick a local user into executing arbitrary commands by opening a deliberately manipulated project file with an affected engineering tool. These arbitrary commands are executed in the user context.	2025-09-09	7.8	CVE-2025-41701
Bender--CC612	An authenticated, low-privileged attacker can obtain credentials stored on the charge controller including the manufacturer password.	2025-09-08	8.8	CVE-2025-41682
Bender--CC612	Due to an unsecure default configuration HTTP is used instead of HTTPS for the web interface. An unauthenticated attacker on the same network could exploit this to learn sensitive data during transmission.	2025-09-08	7.4	CVE-2025-41708
beyondcart--BeyondCart Connector	The BeyondCart Connector plugin for WordPress is vulnerable to Privilege Escalation due to improper JWT secret management and authorization within the determine_current_user filter in versions 1.4.2 through 2.1.0. This makes it possible for unauthenticated attackers to craft valid tokens and assume any user's identity.	2025-09-11	9.8	CVE-2025-8570
Campcodes--Grocery Sales and Inventory System	A vulnerability has been found in Campcodes Grocery Sales and Inventory System 1.0. The affected element is an unknown function of the file /ajax.php?action=delete_customer. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	2025-09-14	7.3	CVE-2025-10413
Campcodes--Grocery Sales and Inventory System	A vulnerability was found in Campcodes Grocery Sales and Inventory System 1.0. The impacted element is an unknown function of the file /ajax.php?action=save_customer. Performing manipulation of the argument ID	2025-09-14	7.3	CVE-2025-10414

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.			
Campcodes--Grocery Sales and Inventory System	A vulnerability was determined in Campcodes Grocery Sales and Inventory System 1.0. This affects an unknown function of the file /ajax.php?action=save_supplier. Executing manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	2025-09-14	7.3	CVE-2025-10415
Campcodes--Grocery Sales and Inventory System	A vulnerability was identified in Campcodes Grocery Sales and Inventory System 1.0. This impacts an unknown function of the file /ajax.php?action=delete_supplier. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	2025-09-14	7.3	CVE-2025-10416
Campcodes--Online Loan Management System	A vulnerability was found in Campcodes Online Loan Management System 1.0. This vulnerability affects unknown code of the file /ajax.php?action=delete_loan. Performing manipulation of the argument ID results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	2025-09-08	7.3	CVE-2025-10108
Campcodes--Online Loan Management System	A vulnerability was determined in Campcodes Online Loan Management System 1.0. This issue affects some unknown processing of the file /ajax.php?action=delete_payment. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-08	7.3	CVE-2025-10109
Cisco--Cisco IOS XR Software	A vulnerability in the Address Resolution Protocol (ARP) implementation of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to trigger a broadcast storm, leading to a denial of service (DoS) condition on an affected device. This vulnerability is due to how Cisco IOS XR Software processes a high, sustained rate of ARP traffic hitting the management interface. Under certain conditions, an attacker could exploit this vulnerability by sending an excessive amount of traffic to the management interface of an affected device, overwhelming its ARP processing capabilities. A successful exploit could result in degraded device performance, loss of management connectivity, and complete unresponsiveness of the system, leading to a DoS condition.	2025-09-10	7.4	CVE-2025-20340
code-projects--Online Event Judging System	A security flaw has been discovered in code-projects Online Event Judging System 1.0. This affects an unknown function of the file /index.php. Performing manipulation of the argument Username results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.	2025-09-08	7.3	CVE-2025-10102
code-projects--Online Event Judging System	A weakness has been identified in code-projects Online Event Judging System 1.0. This impacts an unknown function of the file /home.php. Executing manipulation of the argument main_event can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be exploited.	2025-09-08	7.3	CVE-2025-10103
code-projects--Online Event Judging System	A security vulnerability has been detected in code-projects Online Event Judging System 1.0. Affected is an unknown function of the file /review_search.php. The manipulation of the argument txtsearch leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	2025-09-08	7.3	CVE-2025-10104
coredns--coredns	CoreDNS is a DNS server that chains plugins. Starting in version 1.2.0 and prior to version 1.12.4, the CoreDNS etcd plugin contains a TTL confusion vulnerability where lease IDs are incorrectly used as TTL values, enabling DNS cache pinning attacks. This effectively creates a DoS condition for DNS resolution of affected services. The `TTL()` function in `plugin/etcd/etcd.go` incorrectly casts etcd lease IDs (64-bit integers) to uint32 and uses them as TTL values. Large lease IDs become very large TTLs when cast to uint32. This enables cache pinning attacks. Version 1.12.4 contains a fix for the issue.	2025-09-09	7.1	CVE-2025-58063
Cristiano Zanca--WooCommerce Booking Bundle Hours	Cross-Site Request Forgery (CSRF) vulnerability in Cristiano Zanca WooCommerce Booking Bundle Hours allows Stored XSS. This issue affects WooCommerce Booking Bundle Hours: from n/a through 0.7.4.	2025-09-09	7.1	CVE-2025-58991
D-Link--DIR-823X	A vulnerability was determined in D-Link DIR-823X up to 250416. Affected by this vulnerability is the function sub_415028 of the file /goform/set_static_leases. Executing manipulation of the argument Hostname can lead to command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-09	7.3	CVE-2025-10123

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Daikin--Security Gateway	Daikin Security Gateway is vulnerable to an authorization bypass through a user-controlled key vulnerability that could allow an attacker to bypass authentication. An unauthorized attacker could access the system without prior credentials.	2025-09-11	7.3	CVE-2025-10127
dasinfomedia--WPGYM - Wordpress Gym Management System	The WPGYM - Wordpress Gym Management System plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 67.7.0 via the 'MJ_gmgt_gmgt_add_user' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change the email, password, and other details of any user, including Administrator users.	2025-09-10	8.8	CVE-2025-7049
Dell--PowerProtect Data Manager	Dell PowerProtect Data Manager, version(s) 19.19 and 19.20, Hyper-V contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution.	2025-09-10	8.2	CVE-2025-43884
Dell--PowerProtect Data Manager	Dell PowerProtect Data Manager, Hyper-V, version(s) 19.19 and 19.20, contain(s) an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access.	2025-09-10	8.8	CVE-2025-43888
Dell--PowerProtect Data Manager	Dell PowerProtect Data Manager, Generic Application Agent, version(s) 19.19 and 19.20, contain(s) an Incorrect Default Permissions vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2025-09-10	7.8	CVE-2025-43725
Dell--PowerProtect Data Manager	Dell PowerProtect Data Manager, version(s) 19.19 and 19.20, Hyper-V contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution.	2025-09-10	7.8	CVE-2025-43885
Dell--PowerProtect Data Manager	Dell PowerProtect Data Manager, version(s) 19.19 and 19.20, Hyper-V contain(s) an Incorrect Default Permissions vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2025-09-10	7	CVE-2025-43887
Delta Electronics--DIALink	Delta Electronics DIALink has an Directory Traversal Authentication Bypass Vulnerability.	2025-09-11	10	CVE-2025-58321
Delta Electronics--DIALink	Delta Electronics DIALink has an Directory Traversal Authentication Bypass Vulnerability.	2025-09-11	7.3	CVE-2025-58320
Digiever--DS-1200	Certain models of NVR developed by Digiever has an Exposure of Sensitive Information vulnerability, allowing unauthenticated remoter attackers to access the system configuration file and obtain plaintext credentials of the NVR and its connected cameras.	2025-09-12	10	CVE-2025-10264
Digiever--DS-1200	Certain models of NVR developed by Digiever has an OS Command Injection vulnerability, allowing authenticated remote attackers to inject arbitrary OS commands and execute them on the device.	2025-09-12	8.8	CVE-2025-10265
dreamstechnologies--Doccure	The Doccure theme for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'doccure_temp_upload_to_media' function in all versions up to, and including, 1.4.8. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	2025-09-08	9.8	CVE-2025-9113
dreamstechnologies--Doccure	The Doccure theme for WordPress is vulnerable to Arbitrary User Password Change in versions up to, and including, 1.4.8. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for unauthenticated attackers to change user passwords and potentially take over administrator accounts.	2025-09-08	9.8	CVE-2025-9114
dreamstechnologies--Doccure	The Doccure theme for WordPress is vulnerable to arbitrary file uploads due to incorrect file type validation in the 'doccure_temp_file_uploader' function in all versions up to, and including, 1.4.8. This makes it possible for authenticated attackers, with subscriber-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2025-09-08	8.8	CVE-2025-9112
eCharge Hardy Barth--Salia PLCC	A security flaw has been discovered in eCharge Hardy Barth Salia PLCC 2.2.0. This issue affects some unknown processing of the file /api.php. The manipulation of the argument setrfidlist results in unrestricted upload. The attack may be performed from remote. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-13	7.3	CVE-2025-10371
fassionstorage--Propovoice: All-in-One Client Management System	The Propovoice: All-in-One Client Management System plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 1.7.6.7 via the send_email() function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	2025-09-11	7.5	CVE-2025-8422

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
FlowiseAI--Flowise	Flowise is a drag & drop user interface to build a customized large language model flow. In version 3.0.5 and earlier, the `forgot-password` endpoint in Flowise returns sensitive information including a valid password reset `tempToken` without authentication or verification. This enables any attacker to generate a reset token for arbitrary users and directly reset their password, leading to a complete account takeover (ATO). This vulnerability applies to both the cloud service (`cloud.flowiseai.com`) and self-hosted/local Flowise deployments that expose the same API. Commit 9e178d68873eb876073846433a596590d3d9c863 in version 3.0.6 secures password reset endpoints. Several recommended remediation steps are available. Do not return reset tokens or sensitive account details in API responses. Tokens must only be delivered securely via the registered email channel. Ensure `forgot-password` responds with a generic success message regardless of input, to avoid user enumeration. Require strong validation of the `tempToken` (e.g., single-use, short expiry, tied to request origin, validated against email delivery). Apply the same fixes to both cloud and self-hosted/local deployments. Log and monitor password reset requests for suspicious activity. Consider multi-factor verification for sensitive accounts.	2025-09-12	9.8	CVE-2025-58434
Frenify--Mow	Cross-Site Request Forgery (CSRF) vulnerability in Frenify Mow allows Code Injection. This issue affects Mow: from n/a through 4.10.	2025-09-09	9.6	CVE-2025-58997
FWDesign--Ultimate Video Player	Server-Side Request Forgery (SSRF) vulnerability in FWDesign Ultimate Video Player allows Server Side Request Forgery. This issue affects Ultimate Video Player: from n/a through 10.1.	2025-09-09	7.2	CVE-2025-49430
gavias--Ziston	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in gavias Ziston allows PHP Local File Inclusion. This issue affects Ziston: from n/a through n/a.	2025-09-09	8.1	CVE-2025-58215
germanpearls--Time Tracker	The Time Tracker plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check on the 'tt_update_table_function' and 'tt_delete_record_function' functions in all versions up to, and including, 3.1.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update options such as user registration and default role, allowing anyone to register as an Administrator, and to delete limited data from the database.	2025-09-11	8.8	CVE-2025-9018
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 16.11 before 18.1.6, 18.2 before 18.2.6, and 18.3 before 18.3.2 that could have allowed authenticated users to make unintended internal requests through proxy environments by injecting crafted sequences.	2025-09-12	8.5	CVE-2025-6454
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 7.12 before 18.1.6, 18.2 before 18.2.6, and 18.3 before 18.3.2 that could have allowed unauthorized users to render the GitLab instance unresponsive to legitimate users by sending multiple concurrent large SAML responses.	2025-09-12	7.5	CVE-2025-2256
highwarden--Super Store Finder	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in highwarden Super Store Finder. This issue affects Super Store Finder: from n/a through 6.9.7.	2025-09-09	7.5	CVE-2025-47571
Hossein--Material Dashboard	Weak Password Recovery Mechanism for Forgotten Password vulnerability in Hossein Material Dashboard. This issue affects Material Dashboard: from n/a through 1.4.6.	2025-09-09	9.8	CVE-2025-32486
IBM--Fusion	IBM Fusion 2.2.0 through 2.10.1, IBM Fusion HCI 2.2.0 through 2.10.0, and IBM Fusion HCI for watsonx 2.8.2 through 2.10.0 uses insecure default configurations that could expose AMQStreams without client authentication that could allow an attacker to perform unauthorized actions.	2025-09-11	8.7	CVE-2025-36222
idiatech--Catalog Importer, Scraper & Crawler	The Catalog Importer, Scraper & Crawler plugin for WordPress is vulnerable to PHP code injection in all versions up to, and including, 5.1.4. This is due to reliance on a guessable numeric token (e.g. ?key= 900001705) without proper authentication, combined with the unsafe use of eval() on user-supplied input. This makes it possible for unauthenticated attackers to execute arbitrary PHP code on the server via a forged request granted they can guess or brute-force the numeric key.	2025-09-11	8.1	CVE-2025-8417
ISC--Stork	If an unauthenticated user sends a large amount of data to the Stork UI, it may cause memory and disk use problems for the system running the Stork server. This issue affects Stork versions 1.0.0 through 2.3.0.	2025-09-10	7.5	CVE-2025-8696
itsourcecode--Baptism Information Management System	A vulnerability was found in itsourcecode Baptism Information Management System 1.0. This impacts an unknown function of the file /rptbaptismal.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	2025-09-14	7.3	CVE-2025-10404

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
itsourcecode--Baptism Information Management System	A vulnerability was determined in itsourcecode Baptism Information Management System 1.0. Affected is an unknown function of the file /listbaptism.php. This manipulation of the argument bapt_id causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-14	7.3	CVE-2025-10405
itsourcecode--E-Logbook with Health Monitoring System for COVID-19	A security vulnerability has been detected in itsourcecode E-Logbook with Health Monitoring System for COVID-19 1.0. The affected element is an unknown function of the file /login.php. The manipulation of the argument Username leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	2025-09-09	7.3	CVE-2025-10118
itsourcecode--Student Information Management System	A security flaw has been discovered in itsourcecode Student Information Management System 1.0. The affected element is an unknown function of the file /admin/modules/instructor/index.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.	2025-09-08	7.3	CVE-2025-10111
itsourcecode--Student Information Management System	A weakness has been identified in itsourcecode Student Information Management System 1.0. The impacted element is an unknown function of the file /admin/modules/department/index.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	2025-09-08	7.3	CVE-2025-10112
itsourcecode--Student Information Management System	A security vulnerability has been detected in itsourcecode Student Information Management System 1.0. This affects an unknown function of the file /admin/modules/room/index.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	2025-09-09	7.3	CVE-2025-10113
Ivanti--Connect Secure	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure authentication related settings.	2025-09-09	8.8	CVE-2025-55141
Ivanti--Connect Secure	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure authentication related settings.	2025-09-09	8.8	CVE-2025-55142
Ivanti--Connect Secure	CSRF in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote unauthenticated attacker to execute sensitive actions on behalf of the victim user. User interaction is required	2025-09-09	8.8	CVE-2025-55147
Ivanti--Connect Secure	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure restricted settings.	2025-09-09	7.6	CVE-2025-55148
Ivanti--Connect Secure 22.7R2.9	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker to hijack existing HTML5 connections.	2025-09-09	8.9	CVE-2025-55145
Ivanti--Endpoint Manager	Insufficient filename validation in Ivanti Endpoint Manager before 2024 SU3 SR1 and 2022 SU8 SR2 allows a remote unauthenticated attacker to achieve remote code execution. User interaction is required.	2025-09-09	8.8	CVE-2025-9712
Ivanti--Endpoint Manager	Insufficient filename validation in Ivanti Endpoint Manager before 2024 SU3 SR1 and 2022 SU8 SR2 allows a remote unauthenticated attacker to achieve remote code execution. User interaction is required.	2025-09-09	8.8	CVE-2025-9872
Jinher--OA	A flaw has been found in Jinher OA up to 1.2. The impacted element is an unknown function of the file /C6/Jhsoft.Web.departments/GetTreeDate.aspx. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	2025-09-08	7.3	CVE-2025-10090
Jinher--OA	A vulnerability has been found in Jinher OA up to 1.2. This affects an unknown function of the file /c6/Jhsoft.Web.projectmanage/ProjectManage/XmlHttp.aspx/?Type=add of the component XML Handler. The manipulation leads to xml external entity reference. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	2025-09-08	7.3	CVE-2025-10091

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Jinher--OA	A vulnerability was found in Jinher OA up to 1.2. This impacts an unknown function of the file /c6/Jhsoft.Web.projectmanage/TaskManage/AddTask.aspx/?Type=add of the component XML Handler. The manipulation results in xml external entity reference. The attack can be executed remotely. The exploit has been made public and could be used.	2025-09-08	7.3	CVE-2025-10092
khaledsaikat--User Meta User Profile Builder and User management plugin	The User Meta - User Profile Builder and User management plugin plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the postInsertUserProcess function in all versions up to, and including, 3.1.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	2025-09-11	8	CVE-2025-9693
LabRedesCefetRJ--WeGIA	WeGIA is a Web manager for charitable institutions. The fix for CVE-2025-22133 was not enough to remediate the arbitrary file upload vulnerability. The WeGIA only check MIME types for Excel files at endpoint `/html/socio/sistema/controller/controla_xlsx.php`, which can be bypassed by using magic bytes of Excel file in a PHP file. As a result, attacker can upload webshell to the server for remote code execution. Version 3.4.11 contains an updated fix.	2025-09-08	10	CVE-2025-58745
Lenovo--Browser	A potential DLL hijacking vulnerability was discovered in Lenovo Browser during an internal security assessment that could allow a local user to execute code with elevated privileges.	2025-09-11	7.8	CVE-2025-9201
Lenovo--Dispatcher 3.0 Driver	A potential insufficient access control vulnerability was reported in the Lenovo Dispatcher 3.0 and Dispatcher 3.1 drivers used by some Lenovo consumer notebooks that could allow an authenticated local user to execute code with elevated privileges. The Lenovo Dispatcher 3.2 driver is not affected. This vulnerability does not affect systems when the Windows feature Core Isolation Memory Integrity is enabled. Lenovo systems preloaded with Windows 11 have this feature enabled by default.	2025-09-11	7	CVE-2025-8061
Lenovo--Wallpaper Client	A potential vulnerability was reported in the Lenovo Wallpaper Client that could allow arbitrary code execution under certain conditions.	2025-09-11	7.5	CVE-2025-9319
Lenovo--XClarity Orchestrator (LXCO)	An internal product security audit of Lenovo XClarity Orchestrator (LXCO) discovered the below vulnerability: An attacker with access to a device on the local Lenovo XClarity Orchestrator (LXCO) network segment may be able to manipulate the local device to create an alternate communication channel which could allow the attacker, under certain conditions, to directly interact with backend LXCO API services typically inaccessible to users. While access controls may limit the scope of interaction, this could result in unauthorized access to internal functionality or data. This issue is not exploitable from remote networks.	2025-09-11	8.8	CVE-2025-8557
lmsys--sglang	A security flaw has been discovered in lmsys sglang 0.4.6. Affected by this vulnerability is the function main of the file /update_weights_from_tensor. The manipulation of the argument serialized_named_tensors results in deserialization. The attack can be launched remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-09	7.3	CVE-2025-10164
maheshmthorat--All in one Minifier	The All in one Minifier plugin for WordPress is vulnerable to SQL Injection via the 'post_id' parameter in all versions up to, and including, 3.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-11	7.5	CVE-2025-9073
Mercury--KM08-708H GiGA WiFi Wave2	A vulnerability was detected in Mercury KM08-708H GiGA WiFi Wave2 1.1.14. This affects an unknown function of the component HTTP Header Handler. The manipulation of the argument Host results in stack-based buffer overflow. The attack can be executed remotely. The exploit is now public and may be used.	2025-09-14	9.8	CVE-2025-10392
Mercury--KM08-708H GiGA WiFi Wave2	A vulnerability has been found in Mercury KM08-708H GiGA WiFi Wave2 1.1. Affected by this issue is the function sub_450B2C of the file /goform/mcr_setSysAdm. The manipulation of the argument ChgUserId leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2025-09-14	8.8	CVE-2025-10385
Microsoft--.NET 6.0	A vulnerability (CVE-2024-38229 https://www.cve.org/CVERecord) exists in EOL ASP.NET when closing an HTTP/3 stream while application code is writing to the response body, a race condition may lead to use-after-free, resulting in Remote Code Execution. Per CWE-416: Use After Free https://cwe.mitre.org/data/definitions/416.html , Use After Free is when a product reuses or references memory after it has been freed. At some point afterward, the	2025-09-08	8.1	CVE-2025-36854

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	memory may be allocated again and saved in another pointer, while the original pointer references a location somewhere within the new allocation. Any operations using the original pointer are no longer valid because the memory "belongs" to the code that operates on the new pointer. This issue affects EOL ASP.NET 6.0.0 <= 6.0.36 as represented in this CVE, as well as 8.0.0 <= 8.0.8, 9.0.0-preview.1.24081.5 <= 9.0.0.RC.1 as represented in CVE-2024-38229 https://www.cve.org/CVERecord . Additionally, if you've deployed self-contained applications https://docs.microsoft.com/dotnet/core/deploying/#self-contained-deployments-scd targeting any of the impacted versions, these applications are also vulnerable and must be recompiled and redeployed. NOTE: This CVE only represents End Of Life (EOL) software components. The vendor, Microsoft, has indicated there will be no future updates nor support provided upon inquiry.			
Microsoft--.NET 6.0	A vulnerability (CVE-2025-21176 https://www.cve.org/CVERecord) exists in DiaSymReader.dll due to buffer over-read. Per CWE-126: Buffer Over-read https://cwe.mitre.org/data/definitions/126.html , Buffer Over-read is when a product reads from a buffer using buffer access mechanisms such as indexes or pointers that reference memory locations after the targeted buffer. This issue affects EOL ASP.NET 6.0.0 <= 6.0.36 as represented in this CVE, as well as 8.0.0 <= 8.0.11 & <= 9.0.0 as represented in CVE-2025-21176. Additionally, if you've deployed self-contained applications https://docs.microsoft.com/dotnet/core/deploying/#self-contained-deployments-scd targeting any of the impacted versions, these applications are also vulnerable and must be recompiled and redeployed. NOTE: This CVE affects only End Of Life (EOL) software components. The vendor, Microsoft, has indicated there will be no future updates nor support provided upon inquiry.	2025-09-08	8.8	CVE-2025-36855
Microsoft--.NET 6.0	A vulnerability (CVE-2025-21172) exists in msdia140.dll due to integer overflow and heap-based overflow. Per CWE-122: Heap-based Buffer Overflow, a heap overflow condition is a buffer overflow, where the buffer that can be overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a routine such as malloc().â€• Per CWE-190: Integer Overflow or Wraparound, is when a product performs a calculation that can produce an integer overflow or wraparound when the logic assumes that the resulting value will always be larger than the original value. This occurs when an integer value is incremented to a value that is too large to store in the associated representation. When this occurs, the value may become a very small or negative number. NOTE: This CVE affects only End Of Life (EOL) software components. The vendor, Microsoft, has indicated there will be no future updates nor support provided upon inquiry.	2025-09-08	7.5	CVE-2025-36853
Microsoft--Azure Connected Machine Agent	Improper access control in Azure Windows Virtual Machine Agent allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-49692
Microsoft--Azure Connected Machine Agent	External control of file name or path in Azure Arc allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-55316
Microsoft--Microsoft AutoUpdate for Mac	Improper link resolution before file access ('link following') in Microsoft AutoUpdate (MAU) allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-55317
Microsoft--Microsoft HPC Pack 2019	Deserialization of untrusted data in Microsoft High Performance Compute Pack (HPC) allows an unauthorized attacker to execute code over a network.	2025-09-09	9.8	CVE-2025-55232
Microsoft--Microsoft Office 2019	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-09-09	8.4	CVE-2025-54910
Microsoft--Microsoft Office 2019	Free of memory not on the heap in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8	CVE-2025-54899
Microsoft--Microsoft Office 2019	Heap-based buffer overflow in Microsoft Office Visio allows an unauthorized attacker to execute code locally.	2025-09-09	7.8	CVE-2025-54907
Microsoft--Microsoft Office 2019	Use after free in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.	2025-09-09	7.8	CVE-2025-54908

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Microsoft OfficePLUS	Exposure of sensitive information to an unauthorized actor in Microsoft Office Plus allows an unauthorized attacker to perform spoofing over a network.	2025-09-09	7.5	CVE-2025-55243
Microsoft--Microsoft SharePoint Enterprise Server 2016	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2025-09-09	8.8	CVE-2025-54897
Microsoft--Microsoft SharePoint Enterprise Server 2016	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2025-09-09	7.1	CVE-2025-54905
Microsoft--Microsoft SharePoint Enterprise Server 2016	Free of memory not on the heap in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-09-09	7.8	CVE-2025-54906
Microsoft--Microsoft SQL Server 2017 (GDR)	Improper neutralization of special elements used in a command ('command injection') in SQL Server allows an authorized attacker to elevate privileges over a network.	2025-09-09	8.8	CVE-2025-55227
Microsoft--Office Online Server	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8	CVE-2025-54896
Microsoft--Office Online Server	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8	CVE-2025-54898
Microsoft--Office Online Server	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8	CVE-2025-54900
Microsoft--Office Online Server	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8	CVE-2025-54902
Microsoft--Office Online Server	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8	CVE-2025-54903
Microsoft--Office Online Server	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8	CVE-2025-54904
Microsoft--Visual Studio Code	Ai command injection in Agentic AI and Visual Studio Code allows an unauthorized attacker to execute code over a network.	2025-09-12	8.8	CVE-2025-55319
Microsoft--Windows 10 Version 1809	Integer overflow or wraparound in Windows Kernel allows an authorized attacker to elevate privileges locally.	2025-09-09	8.8	CVE-2025-54110
Microsoft--Windows 10 Version 1809	Improper authentication in Windows NTLM allows an authorized attacker to elevate privileges over a network.	2025-09-09	8.8	CVE-2025-54918
Microsoft--Windows 10 Version 1809	SMB Server might be susceptible to relay attacks depending on the configuration. An attacker who successfully exploited these vulnerabilities could perform relay attacks and make the users subject to elevation of privilege attacks. The SMB Server already supports mechanisms for hardening against relay attacks: SMB Server signing SMB Server Extended Protection for Authentication (EPA) Microsoft is releasing this CVE to provide customers with audit capabilities to help them to assess their environment and to identify any potential device or software incompatibility issues before deploying SMB Server hardening measures that protect against relay attacks. If you have not already enabled SMB Server hardening measures, we advise customers to take the following actions to be protected from these relay attacks: Assess your environment by utilizing the audit capabilities that we are exposing in the September 2025 security updates. See Support for Audit Events to deploy SMB Server Hardening-SMB Server Signing & SMB Server EPA. Adopt appropriate SMB Server hardening measures.	2025-09-09	8.8	CVE-2025-55234
Microsoft--Windows 10 Version 1809	Improper restriction of communication channel to intended endpoints in Windows PowerShell allows an authorized attacker to elevate privileges locally.	2025-09-09	7	CVE-2025-49734
Microsoft--Windows 10 Version 1809	No cwe for this issue in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-53800
Microsoft--Windows 10 Version 1809	Untrusted pointer dereference in Windows DWM allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-53801

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2025-09-09	7	CVE-2025-53807
Microsoft--Windows 10 Version 1809	Integer overflow or wraparound in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-54091
Microsoft--Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-54092
Microsoft--Windows 10 Version 1809	Time-of-check time-of-use (toctou) race condition in Windows TCP/IP allows an authorized attacker to elevate privileges locally.	2025-09-09	7	CVE-2025-54093
Microsoft--Windows 10 Version 1809	Improper access control in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-54098
Microsoft--Windows 10 Version 1809	Stack-based buffer overflow in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2025-09-09	7	CVE-2025-54099
Microsoft--Windows 10 Version 1809	Use after free in Windows Connected Devices Platform Service allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-54102
Microsoft--Windows 10 Version 1809	Use after free in Windows UI XAML Phone DatePickerFlyout allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-54111
Microsoft--Windows 10 Version 1809	Use after free in Microsoft Virtual Hard Drive allows an authorized attacker to elevate privileges locally.	2025-09-09	7	CVE-2025-54112
Microsoft--Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	2025-09-09	7	CVE-2025-54115
Microsoft--Windows 10 Version 1809	Improper access control in Windows MultiPoint Services allows an authorized attacker to elevate privileges locally.	2025-09-09	7.3	CVE-2025-54116
Microsoft--Windows 10 Version 1809	Local Security Authority Subsystem Service Elevation of Privilege Vulnerability	2025-09-09	7.8	CVE-2025-54894
Microsoft--Windows 10 Version 1809	Integer overflow or wraparound in Windows SPNEGO Extended Negotiation allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-54895
Microsoft--Windows 10 Version 1809	Use after free in Windows BitLocker allows an authorized attacker to elevate privileges locally.	2025-09-09	7.3	CVE-2025-54911
Microsoft--Windows 10 Version 1809	Use after free in Windows BitLocker allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-54912
Microsoft--Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows UI XAML Maps MapControlSettings allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-54913
Microsoft--Windows 10 Version 1809	Stack-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.	2025-09-09	7.8	CVE-2025-54916
Microsoft--Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to execute code locally.	2025-09-09	7.5	CVE-2025-54919
Microsoft--Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Graphics Kernel allows an authorized attacker to elevate privileges locally.	2025-09-09	7	CVE-2025-55223
Microsoft--Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to execute code locally.	2025-09-09	7.8	CVE-2025-55224
Microsoft--Windows 10 Version 1809	Time-of-check time-of-use (toctou) race condition in Graphics Kernel allows an authorized attacker to execute code locally.	2025-09-09	7.3	CVE-2025-55236

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 21H2	Use after free in Windows Management Services allows an unauthorized attacker to elevate privileges locally.	2025-09-09	7.4	CVE-2025-54103
Microsoft--Windows Server 2019	Integer overflow or wraparound in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	2025-09-09	8.8	CVE-2025-54106
Microsoft--Windows Server 2019	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	2025-09-09	8.8	CVE-2025-54113
Microsoft--Windows Server 2022	Use after free in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	2025-09-09	7	CVE-2025-53802
Microsoft--Windows Server 2022	Out-of-bounds read in Windows Internet Information Services allows an unauthorized attacker to deny service over a network.	2025-09-09	7.5	CVE-2025-53805
Microsoft--Windows Server 2022	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Connected Devices Platform Service allows an authorized attacker to deny service locally.	2025-09-09	7	CVE-2025-54114
Microsoft--Windows Server 2022	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to execute code locally.	2025-09-09	7.8	CVE-2025-55228
Microsoft--Windows Server 2025 (Server Core installation)	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	2025-09-09	7	CVE-2025-54105
Microsoft--Windows Server 2025 (Server Core installation)	Concurrent execution using shared resource with improper synchronization ('race condition') in Capability Access Management Service (camsvc) allows an authorized attacker to elevate privileges locally.	2025-09-09	7	CVE-2025-54108
Microsoft--Xbox Gaming Services	Improper link resolution before file access ('link following') in Xbox allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8	CVE-2025-55245
mockoon--mockoon	Mockoon provides way to design and run mock APIs. Prior to version 9.2.0, a mock API configuration for static file serving follows the same approach presented in the documentation page, where the server filename is generated via templating features from user input is vulnerable to Path Traversal and LFI, allowing an attacker to get any file in the mock server filesystem. The issue may be particularly relevant in cloud hosted server instances. Version 9.2.0 fixes the issue.	2025-09-10	7.5	CVE-2025-59049
moeru-ai--airi	AIRI is a self-hosted, artificial intelligence based Grok Companion. In v0.7.2-beta.2 in the `packages/stage-ui/src/components/MarkdownRenderer.vue` path, the Markdown content is processed using the useMarkdown composable, and the processed HTML is rendered directly into the DOM using v-html. An attacker creates a card file containing malicious HTML/JavaScript, then simply processes it using the highlightTagToHtml function (which simply replaces template tags without HTML escaping), and then directly renders it using v-html, leading to cross-site scripting (XSS). The project also exposes the Tauri API, which can be called from the frontend. The MCP plugin exposes a command execution interface function in `crates/tauri-plugin-mcp/src/lib.rs`. This allows arbitrary command execution. `connect_server` directly passes the user-supplied `command` and `args` parameters to `Command::new(command).args(args)` without any input validation or whitelisting. Thus, the previous XSS exploit could achieve command execution through this interface. v0.7.2-beta.3 fixes the issue.	2025-09-11	9.7	CVE-2025-59053
mythemeshop--My WP Translate	The My WP Translate plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the ajax_import_strings() function in all versions up to, and including, 1.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	2025-09-11	8.8	CVE-2025-8425
N-able--N-central	An Incorrect File Handling Permission bug exists on the N-central Windows Agent and Probe that, in the right circumstances, can allow a local low-level user to run commands with elevated permissions.	2025-09-10	7	CVE-2025-10231
n/a--SiempreCMS	A vulnerability was determined in SiempreCMS up to 1.3.6. This affects an unknown part of the file user_search_ajax.php. This manipulation of the argument name/userName causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-09	7.3	CVE-2025-10115

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--SiempreCMS	A vulnerability was identified in SiempreCMS up to 1.3.6. This vulnerability affects unknown code of the file /docs/admin/file_upload.php. Such manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit is publicly available and might be used.	2025-09-09	7.3	CVE-2025-10116
NewType Infortech--NUP Portal	NUP Pro developed by NewType Infortech has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.	2025-09-12	9.8	CVE-2025-10266
nik00726--Responsive Filterable Portfolio	The Responsive Filterable Portfolio plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation via the HdnMediaSelection_image field in all versions up to, and including, 1.0.24. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2025-09-10	7.2	CVE-2025-10049
ninofiliu--interactive-git-checkout	The npm package `interactive-git-checkout` is an interactive command-line tool that allows users to checkout a git branch while it prompts for the branch name on the command-line. It is available as an npm package and can be installed via `npm install -g interactive-git-checkout`. Versions up to and including 1.1.4 of the `interactive-git-checkout` tool are vulnerable to a command injection vulnerability because the software passes the branch name to the `git checkout` command using the Node.js child process module's `exec()` function without proper input validation or sanitization. Commit 8dd832dd302af287a61611f4f85e157cd1c6bb41 fixes the issue.	2025-09-09	9.8	CVE-2025-59046
NVIDIA--NVDebug tool	The NVIDIA NVDebug tool contains a vulnerability that may allow an actor to gain access to a privileged account . A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure and data tampering.	2025-09-09	8.2	CVE-2025-23342
NVIDIA--NVDebug tool	The NVIDIA NVDebug tool contains a vulnerability that may allow an actor to write files to restricted components. A successful exploit of this vulnerability may lead to information disclosure, denial of service, and data tampering.	2025-09-09	7.6	CVE-2025-23343
NVIDIA--NVDebug tool	The NVIDIA NVDebug tool contains a vulnerability that may allow an actor to run code on the platform host as a non-privileged user. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure and data tampering.	2025-09-09	7.3	CVE-2025-23344
One Identity--OneLogin	In One Identity OneLogin before 2025.3.0, a request returns the OIDC client secret with GET Apps API v2 (even though this secret should only be returned when an App is first created),	2025-09-14	7.7	CVE-2025-59363
OpenPrinting--cups	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. In versions 2.4.12 and earlier, when the `AuthType` is set to anything but `Basic`, if the request contains an `Authorization: Basic ...` header, the password is not checked. This results in authentication bypass. Any configuration that allows an `AuthType` that is not `Basic` is affected. Version 2.4.13 fixes the issue.	2025-09-11	8	CVE-2025-58060
OPEXUS--FOIAXpress Public Access Link (PAL)	OPEXUS FOIAXpress Public Access Link (PAL) before version 11.13.1.0 allows SQL injection via SearchPopularDocs.aspx. A remote, unauthenticated attacker could read, write, or delete any content in the underlying database.	2025-09-09	9.8	CVE-2025-58462
PHPGurukul--Beauty Parlour Management System	A flaw has been found in PHPGurukul Beauty Parlour Management System 1.1. The impacted element is an unknown function of the file /admin/readenq.php. Executing manipulation of the argument delid can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	2025-09-14	7.3	CVE-2025-10402
PHPGurukul--Beauty Parlour Management System	A vulnerability has been found in PHPGurukul Beauty Parlour Management System 1.1. This affects an unknown function of the file /admin/view-enquiry.php. The manipulation of the argument viewid leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	2025-09-14	7.3	CVE-2025-10403
PHPGurukul--Small CRM	A flaw has been found in PHPGurukul Small CRM 4.0. Affected by this vulnerability is an unknown functionality of the file /get-quote.php. Executing manipulation of the argument Contact can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	2025-09-08	7.3	CVE-2025-10079
PHPGurukul--Small CRM	A vulnerability was found in PHPGurukul Small CRM 4.0. Affected by this issue is some unknown functionality of the file /profile.php. The manipulation of the argument Name results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	2025-09-09	7.3	CVE-2025-10114
pixel_prime--Resideo Plugin for Resideo - Real	The Resideo Plugin for Resideo - Real Estate WordPress Theme plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.5.4. This is due to the plugin not properly validating a user's	2025-09-10	8.8	CVE-2025-7718

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Estate WordPress Theme	identity prior to updating their details like email. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change arbitrary user's email addresses, including administrators, and leverage that to reset the user's password and gain access to their account.			
PressTigers--ZIP Code Based Content Protection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in PressTigers ZIP Code Based Content Protection allows SQL Injection. This issue affects ZIP Code Based Content Protection: from n/a through 1.0.0.	2025-09-09	7.6	CVE-2025-59008
Project-MONAI--MONAI	MONAI (Medical Open Network for AI) is an AI toolkit for health care imaging. The extractall function `zip_file.extractall(output_dir)` is used directly to process compressed files. It is used in many places in the project. In versions up to and including 1.5.0, when the Zip file containing malicious content is decompressed, it overwrites the system files. In addition, the project allows the download of the zip content through the link, which increases the scope of exploitation of this vulnerability. As of time of publication, no known fixed versions are available.	2025-09-08	8.8	CVE-2025-58755
Project-MONAI--MONAI	MONAI (Medical Open Network for AI) is an AI toolkit for health care imaging. In versions up to and including 1.5.0, in `model_dict = torch.load(full_path, map_location=torch.device(device), weights_only=True)` in monai/bundle/scripts.py , `weights_only=True` is loaded securely. However, insecure loading methods still exist elsewhere in the project, such as when loading checkpoints. This is a common practice when users want to reduce training time and costs by loading pre-trained models downloaded from other platforms. Loading a checkpoint containing malicious content can trigger a deserialization vulnerability, leading to code execution. As of time of publication, no known fixed versions are available.	2025-09-08	8.8	CVE-2025-58756
Project-MONAI--MONAI	MONAI (Medical Open Network for AI) is an AI toolkit for health care imaging. In versions up to and including 1.5.0, the `pickle_operations` function in `monai/data/utils.py` automatically handles dictionary key-value pairs ending with a specific suffix and deserializes them using `pickle.loads()` . This function also lacks any security measures. The deserialization may lead to code execution. As of time of publication, no known fixed versions are available.	2025-09-08	8.8	CVE-2025-58757
rathena--rathena	rAthena is an open-source cross-platform massively multiplayer online role playing game (MMORPG) server. Versions prior to commit 2f5248b have a heap-based buffer overflow in the login server, remote attacker to overwrite adjacent session fields by sending a crafted `CA_SSO_LOGIN_REQ` with an oversized token length. This leads to immediate denial of service (crash) and it is possible to achieve remote code execution via heap corruption. Commit 2f5248b fixes the issue.	2025-09-09	9.8	CVE-2025-58447
rathena--rathena	rAthena is an open-source cross-platform massively multiplayer online role playing game (MMORPG) server. Versions prior to commit 0d89ae0 have a SQL Injection in the PartyBooking component via `WorldName` parameter. Commit 0d89ae0 fixes the issue.	2025-09-09	9.1	CVE-2025-58448
rathena--rathena	rAthena is an open-source cross-platform massively multiplayer online role playing game (MMORPG) server. Versions prior to commit 0cc348b are missing a bound check in `chclif_parse_moveCharSlot` that can result in reading and writing out of bounds using input from the user. The problem has been fixed in commit 0cc348b.	2025-09-09	8.2	CVE-2025-58750
rubengc--AutomatorWP Automator plugin for no-code automations, webhooks & custom integrations in WordPress	The AutomatorWP - Automator plugin for no-code automations, webhooks & custom integrations in WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the automatorwp_ajax_import_automation_from_url function in all versions up to, and including, 5.3.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create arbitrary automations, which can lead to Remote Code Execution or Privilege escalation once such automation is activated by the administrator	2025-09-09	8	CVE-2025-9539
Samsung Mobile--Samsung Mobile Devices	Out-of-bounds write in libimagecodec.quram.so prior to SMR Apr-2025 Release 1 allows remote attackers to execute arbitrary code.	2025-09-12	8.8	CVE-2025-21042
Samsung Mobile--Samsung Mobile Devices	Out-of-bounds write in libimagecodec.quram.so prior to SMR Sep-2025 Release 1 allows remote attackers to execute arbitrary code.	2025-09-12	8.8	CVE-2025-21043
SAP_SE--SAP Business One (SLD)	When a user logs in via SAP Business One native client, the SLD backend service fails to enforce proper encryption of certain APIs. This leads to exposure of sensitive credentials within http response body. As a result, it has a high impact on the confidentiality, integrity, and availability of the application.	2025-09-09	8.8	CVE-2025-42933

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SAP_SE--SAP Landscape Transformation Replication Server	Due to missing input validation, an attacker with high privilege access to ABAP reports could delete the content of arbitrary database tables, if the tables are not protected by an authorization group. This leads to a high impact on integrity and availability of the database.	2025-09-09	8.1	CVE-2025-42929
SAP_SE--SAP NetWeaver	Due to a missing authentication check in the SAP NetWeaver application on IBM i-series, the application allows high privileged unauthorized users to read, modify, or delete sensitive information, as well as access administrative or privileged functionalities. This results in a high impact on the confidentiality, integrity, and availability of the application.	2025-09-09	9.1	CVE-2025-42958
SAP_SE--SAP Netweaver (RMI-P4)	Due to a deserialization vulnerability in SAP NetWeaver, an unauthenticated attacker could exploit the system through the RMI-P4 module by submitting malicious payload to an open port. The deserialization of such untrusted Java objects could lead to arbitrary OS command execution, posing a high impact to the application's confidentiality, integrity, and availability.	2025-09-09	10	CVE-2025-42944
SAP_SE--SAP NetWeaver AS Java (Deploy Web Service)	SAP NetWeaver AS Java allows an attacker authenticated as a non-administrative user to use a flaw in an available service to upload an arbitrary file. This file when executed can lead to a full compromise of confidentiality, integrity and availability of the system.	2025-09-09	9.9	CVE-2025-42922
SAP_SE--SAP S/4HANA (Private Cloud or On-Premise)	Due to missing input validation, an attacker with high privilege access to ABAP reports could delete the content of arbitrary database tables, if the tables are not protected by an authorization group. This leads to a high impact on integrity and availability of the database but no impact on confidentiality.	2025-09-09	8.1	CVE-2025-42916
Shanghai Lingdang Information Technology--Lingdang CRM	A vulnerability was detected in Shanghai Lingdang Information Technology Lingdang CRM up to 8.6.5.4. This affects an unknown function of the file crm/WeiXinApp/dingtalk/index_event.php. The manipulation of the argument corpurl results in server-side request forgery. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-09	7.3	CVE-2025-5005
Shenzhen Sixun--Business Management System	A security flaw has been discovered in Shenzhen Sixun Business Management System 7/11. This affects an unknown part of the file /Adm/OperatorStop. Performing manipulation 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.	2025-09-13	7.3	CVE-2025-10374
Siemens--SIMATIC PCS neo V4.1	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a stack-based buffer overflow vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to execute arbitrary code or to cause a denial of service condition.	2025-09-09	9.8	CVE-2025-40795
Siemens--SIMATIC PCS neo V4.1	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a out-of-bounds read vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to cause a denial of service condition.	2025-09-09	7.5	CVE-2025-40796
Siemens--SIMATIC PCS neo V4.1	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a out-of-bounds read vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to cause a denial of service condition.	2025-09-09	7.5	CVE-2025-40797
Siemens--SIMATIC PCS neo V4.1	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a out-of-bounds read vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to cause a denial of service condition.	2025-09-09	7.5	CVE-2025-40798
Siemens--SIMATIC Virtualization as a Service (SIVaaS)	A vulnerability has been identified in SIMATIC Virtualization as a Service (SIVaaS) (All versions). The affected application exposes a network share without any authentication. This could allow an attacker to access or alter sensitive data without proper authorization.	2025-09-09	9.1	CVE-2025-40804
smackcoders--WP Import Ultimate CSV XML Importer for WordPress	The WP Import - Ultimate CSV XML Importer for WordPress plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'get_ftp_details' AJAX action in all versions up to, and including, 7.27. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve a configured set of SFTP/FTP credentials.	2025-09-10	7.7	CVE-2025-10040
solwin--Blog Designer PRO	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in solwin Blog Designer PRO. This issue affects Blog Designer PRO: from n/a through 3.4.7.	2025-09-09	7.1	CVE-2025-47694

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
solwin--Blog Designer PRO	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in solwin Blog Designer PRO. This issue affects Blog Designer PRO: from n/a through 3.4.7.	2025-09-09	7.5	CVE-2025-47695
Sophos--AP6 Series Wireless Access Points	An authentication bypass vulnerability allows remote attackers to gain administrative privileges on Sophos AP6 Series Wireless Access Points older than firmware version 1.7.2563 (MR7).	2025-09-09	9.8	CVE-2025-10159
SourceCodester--Online Polling System	A weakness has been identified in SourceCodester Online Polling System 1.0. This affects an unknown function of the file /manage-profile.php. This manipulation of the argument email causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	2025-09-08	7.3	CVE-2025-10076
SourceCodester--Online Polling System	A security vulnerability has been detected in SourceCodester Online Polling System 1.0. This impacts an unknown function of the file /registeracc.php. Such manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	2025-09-08	7.3	CVE-2025-10077
SourceCodester--Online Polling System	A vulnerability was detected in SourceCodester Online Polling System 1.0. Affected is an unknown function of the file /admin/candidates.php. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	2025-09-08	7.3	CVE-2025-10078
SourceCodester--Online Polling System	A vulnerability has been found in SourceCodester Online Polling System 1.0. Affected is an unknown function of the file /admin/manage-admins.php. Such manipulation of the argument email leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	2025-09-08	7.3	CVE-2025-10082
SourceCodester--Pet Grooming Management Software	A vulnerability was determined in SourceCodester Pet Grooming Management Software 1.0. Affected by this issue is some unknown functionality of the file /admin/edit_role.php. Executing manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-14	7.3	CVE-2025-10396
SourceCodester--Simple Forum Discussion System	A vulnerability was detected in SourceCodester Simple Forum Discussion System 1.0. This impacts an unknown function of the file /admin_class.php?action=login. Performing manipulation of the argument Username results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	2025-09-08	7.3	CVE-2025-10100
SpectoLabs--hoverfly	Hoverfly is an open source API simulation tool. In versions 1.11.3 and prior, the middleware functionality in Hoverfly is vulnerable to command injection vulnerability at `/api/v2/hoverfly/middleware` endpoint due to insufficient validation and sanitization in user input. The vulnerability exists in the middleware management API endpoint `/api/v2/hoverfly/middleware`. This issue is born due to combination of three code level flaws: Insufficient Input Validation in middleware.go line 94-96; Unsafe Command Execution in local_middleware.go line 14-19; and Immediate Execution During Testing in hoverfly_service.go line 173. This allows an attacker to gain remote code execution (RCE) on any system running the vulnerable Hoverfly service. Since the input is directly passed to system commands without proper checks, an attacker can upload a malicious payload or directly execute arbitrary commands (including reverse shells) on the host server with the privileges of the Hoverfly process. Commit 17e60a9bc78826deb4b782dca1c1abd3dbe60d40 in version 1.12.0 disables the set middleware API by default, and subsequent changes to documentation make users aware of the security changes of exposing the set middleware API.	2025-09-10	9.8	CVE-2025-54123
Tautulli--Tautulli	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. In Tautulli v2.15.3 and earlier, an attacker with administrative access can use the `pms_image_proxy` endpoint to write arbitrary python scripts into the application filesystem. This leads to remote code execution when combined with the `Script` notification agent. If an attacker with administrative access changes the URL of the PMS to a server they control, they can then abuse the `pms_image_proxy` to obtain a file write into the application filesystem. This can be done by making a `pms_image_proxy` request with a URL in the `img` parameter and the desired file name in the `img_format` parameter. Tautulli then uses a hash of the desired metadata together with the `img_format` in order to construct a file path. Since the attacker controls `img_format` which occupies the end of the file path, and `img_format` is not sanitised, the attacker can then use path traversal characters to specify filename of their choosing. If the specified file does not exist, Tautaulli will then attempt to fetch the image from the configured PMS. Since the attacker controls the PMS, they can return arbitrary content in response to this request, which will then be written into the specified file. An attacker can write an arbitrary python script into a location on the application file system. The attacker can then make use of the built-in `Script` notification agent to run the local script, obtaining	2025-09-09	9.1	CVE-2025-58762

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote code execution on the application server. Users should upgrade to version 2.16.0 to receive a patch.			
Tautulli--Tautulli	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. The `/image` API endpoint in Tautulli v2.15.3 and earlier is vulnerable to path traversal, allowing unauthenticated attackers to read arbitrary files from the application server's filesystem. In Tautulli, the `/image` API endpoint is used to serve static images from the application's data directory to users. This endpoint can be accessed without authentication, and its intended purpose is for server background images and icons within the user interface. Attackers can exfiltrate files from the application file system, including the `tautulli.db` SQLite database containing active JWT tokens, as well as the `config.ini` file which contains the hashed admin password, the JWT token secret, and the Plex Media Server token and connection details. If the password is cracked, or if a valid JWT token is present in the database, an unauthenticated attacker can escalate their privileges to obtain administrative control over the application. Version 2.16.0 contains a fix for the issue.	2025-09-09	8.6	CVE-2025-58760
Tautulli--Tautulli	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. The `real_pms_image_proxy` endpoint in Tautulli v2.15.3 and prior is vulnerable to path traversal, allowing unauthenticated attackers to read arbitrary files from the application server's filesystem. The `real_pms_image_proxy` is used to fetch an image directly from the backing Plex Media Server. The image to be fetched is specified through an `img` URL parameter, which can either be a URL or a file path. There is some validation ensuring that `img` begins with the prefix `interfaces/default/images` in order to be served from the local filesystem. However this can be bypassed by passing an `img` parameter which begins with a valid prefix, and then adjoining path traversal characters in order to reach files outside of intended directories. An attacker can exfiltrate files on the application file system, including the `tautulli.db` SQLite database containing active JWT tokens, as well as the `config.ini` file which contains the hashed admin password, the JWT token secret, and the Plex Media Server token and connection details. If the password is cracked, or if a valid JWT token is present in the database, an unauthenticated attacker can escalate their privileges to obtain administrative control over the application. Version 2.16.0 contains a fix for the issue.	2025-09-09	8.6	CVE-2025-58761
Tautulli--Tautulli	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. A command injection vulnerability in Tautulli v2.15.3 and prior allows attackers with administrative privileges to obtain remote code execution on the application server. This vulnerability requires the application to have been cloned from GitHub and installed manually. When Tautulli is cloned directly from GitHub and installed manually, the application manages updates and versioning through calls to the `git` command. In the code, this is performed through the `runGit` function in `versioncheck.py`. Since `shell=True` is passed to `subproces.Popen`, this call is vulnerable to subject to command injection, as shell characters within arguments will be passed to the underlying shell. A concrete location where this can be triggered is in the `checkout_git_branch` endpoint. This endpoint stores a user-supplied remote and branch name into the `GIT_REMOTE` and `GIT_BRANCH` configuration keys without sanitization. Downstream, these keys are then fetched and passed directly into `runGit` using a format string. Hence, code execution can be obtained by using `$()` interpolation in a command. Version 2.16.0 contains a fix for the issue.	2025-09-09	8.1	CVE-2025-58763
TecCom--TecConnect	A blind XML External Entity (XXE) injection in the OpenMessaging webservice in TecCom TecConnect 4.1 allows an unauthenticated attacker to exfiltrate arbitrary files to an attacker-controlled server. TecConnect 4.1 is considered end-of-life as of December 2023. Users are advised to upgrade to TecCom Connect 5.	2025-09-09	9.1	CVE-2025-10183
Tenda--AC20	A vulnerability was detected in Tenda AC20 up to 16.03.08.12. The impacted element is the function strcpy of the file /goform/GetParentControlInfo. The manipulation of the argument mac results in buffer overflow. The attack may be performed from remote. The exploit is now public and may be used.	2025-09-09	8.8	CVE-2025-10120
theeventscalendar--The Events Calendar	The The Events Calendar plugin for WordPress is vulnerable to time-based SQL Injection via the 's' parameter in all versions up to, and including, 6.15.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-12	7.5	CVE-2025-9807
Theme-Spirit--Spirit Framework	The Spirit Framework plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.2.13. This makes it possible for authenticated	2025-09-12	7.5	CVE-2025-10269

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers, with Subscriber-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.			
ThemeGoods--Photography	Deserialization of Untrusted Data vulnerability in ThemeGoods Photography. This issue affects Photography: from n/a through 7.5.2.	2025-09-09	9	CVE-2025-47579
ThemeMove--ThemeMove Core	Deserialization of Untrusted Data vulnerability in ThemeMove ThemeMove Core allows Object Injection. This issue affects ThemeMove Core: from n/a through 1.4.2.	2025-09-09	8.8	CVE-2025-53303
ThemesGrove--WP SmartPay	Improper Validation of Specified Quantity in Input vulnerability in ThemesGrove WP SmartPay. This issue affects WP SmartPay: from n/a through 2.7.13.	2025-09-09	7.5	CVE-2025-32689
Themeum--Tutor LMS	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Tutor LMS allows SQL Injection. This issue affects Tutor LMS: from n/a through 3.7.4.	2025-09-09	7.6	CVE-2025-58993
ThinkInAIXYZ--deepchat	DeepChat is a smart assistant uses artificial intelligence. Prior to version 0.3.5, in the Mermaid chart rendering component, there is a risky operation of directly using `innerHTML` to set user content. Therefore, any malicious content rendered via Mermaid will directly trigger the exploit chain, leading to command execution. This vulnerability is primarily caused by a failure to fully address the existing XSS issue in the project, leading to another exploit chain. The exploit chain is consistent with the report GHSA-hqr4-4gfc-5p2j, executing arbitrary JavaScript code via XSS and arbitrary commands via exposed IPC. Version 0.3.5 contains an updated fix.	2025-09-09	9.7	CVE-2025-58768
tvcnet--The Hack Repair Guy's Plugin Archiver	The The Hack Repair Guy's Plugin Archiver plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the prepare_items function in all versions up to, and including, 2.0.4. This makes it possible for authenticated attackers, with Administrator-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	2025-09-12	7.2	CVE-2025-10176
UTT--1200GW	A weakness has been identified in UTT 1200GW up to 3.0.0-170831. Affected by this issue is some unknown functionality of the file /goform/ConfigWirelessBase. This manipulation of the argument ssid causes buffer overflow. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-09	8.8	CVE-2025-10169
UTT--1200GW	A security vulnerability has been detected in UTT 1200GW up to 3.0.0-170831. This affects the function sub_4B48F8 of the file /goform/formApLbConfig. Such manipulation of the argument loadBalanceNameOld leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-09	8.8	CVE-2025-10170
UTT--1250GW	A vulnerability was detected in UTT 1250GW up to 3.2.2-200710. This vulnerability affects the function sub_453DC of the file /goform/formConfigApConfTemp. Performing manipulation results in buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-09	8.8	CVE-2025-10171
UTT--750W	A flaw has been found in UTT 750W up to 3.2.2-191225. This issue affects some unknown processing of the file /goform/formPictureUrl. Executing manipulation of the argument importpictureurl can lead to buffer overflow. The attack can be executed remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-09	8.8	CVE-2025-10172
uxper--Sala	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in uxper Sala. This issue affects Sala: from n/a through 1.1.6.	2025-09-09	8.1	CVE-2025-54709
villatheme--WooCommerce Photo Reviews	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in villatheme WooCommerce Photo Reviews. This issue affects WooCommerce Photo Reviews: from n/a through 1.3.13.	2025-09-09	7.1	CVE-2025-47570
VolkovLabs--business-links	The Volkov Labs Business Links panel for Grafana provides an interface to navigate using external links, internal dashboards, time pickers, and dropdown menus. Prior to version 2.4.0, a malicious actor with Editor privileges can escalate their privileges to Administrator and perform arbitrary administrative actions. This is possible because the plugin allows arbitrary JavaScript code injection in the [Layout] â†’ [Link] â†’ [URL] field. Version 2.4.0 contains a fix for the issue.	2025-09-08	9.1	CVE-2025-58746
WAGO--Coupler 0750-0362	A low-privileged remote attacker could gain unauthorized access to critical resources, such as firmware and certificates, due to improper permission handling	2025-09-08	7.5	CVE-2025-41664

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	during the runtime of services (e.g., FTP/SFTP). This access could allow the attacker to escalate privileges and modify firmware.			
Wavlink--WL-WN578W2	A vulnerability was found in Wavlink WL-WN578W2 221110. The impacted element is the function sub_409184 of the file /wizard_rep.shtml. The manipulation of the argument sel_EncrypTyp results in command injection. The attack may be performed from remote. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	7.3	CVE-2025-10323
Wavlink--WL-WN578W2	A vulnerability was determined in Wavlink WL-WN578W2 221110. This affects the function sub_401C5C of the file firewall.cgi. This manipulation of the argument pingFrmWANFilterEnabled/blockSynFloodEnabled/blockPortScanEnabled/remoteManagementEnabled causes command injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	7.3	CVE-2025-10324
Wavlink--WL-WN578W2	A security vulnerability has been detected in Wavlink WL-WN578W2 221110. This affects the function sub_404850 of the file /cgi-bin/wireless.cgi. The manipulation of the argument delete_list leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-13	7.3	CVE-2025-10358
Wavlink--WL-WN578W2	A vulnerability was detected in Wavlink WL-WN578W2 221110. This impacts the function sub_404DBC of the file /cgi-bin/wireless.cgi. The manipulation of the argument macAddr results in os command injection. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-13	7.3	CVE-2025-10359
webcodingplace--Ultimate Classified Listings	The Ultimate Classified Listings plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.6 via the 'uclwp_dashboard' shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	2025-09-11	7.5	CVE-2025-9874
webdevstudios--Constant Contact for WordPress	Deserialization of Untrusted Data vulnerability in webdevstudios Constant Contact for WordPress allows Object Injection. This issue affects Constant Contact for WordPress: from n/a through 4.1.1.	2025-09-09	8.8	CVE-2025-48101
webrecorder--wabac.js	wabac.js provides a full web archive replay system, or 'wayback machine', using Service Workers. A Reflected Cross-Site Scripting (XSS) vulnerability exists in the 404 error handling logic of wabac.js v2.23.10 and below. The parameter `requestURL` (derived from the original request target) is directly embedded into an inline `<script>` block without sanitization or escaping. This allows an attacker to craft a malicious URL that executes arbitrary JavaScript in the victim's browser. The scope may be limited by CORS policies, depending on the situation in which wabac.js is used. The vulnerability is fixed in wabac.js v2.23.11.	2025-09-09	7.1	CVE-2025-58765
Welotec--SmartEMS Web Application	The upload endpoint insufficiently validates the 'Upload-Key' request header. By supplying path traversal sequences, an authenticated attacker can cause the server to create upload-related artifacts outside the intended storage location. In certain configurations this enables arbitrary file write and may be leveraged to achieve remote code execution.	2025-09-10	8.8	CVE-2025-41714
wpallimport--Import any XML, CSV or Excel File to WordPress	The Import any XML, CSV or Excel File to WordPress plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the import functionality in all versions up to, and including, 3.9.3. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload unsafe files like .phar files on the affected site's server which may make remote code execution possible.	2025-09-10	7.2	CVE-2025-10001
WPSwings--WooCommerce Ultimate Gift Card - Create, Sell and Manage Gift Cards with Customized Email Templates	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPSwings WooCommerce Ultimate Gift Card - Create, Sell and Manage Gift Cards with Customized Email Templates. This issue affects WooCommerce Ultimate Gift Card - Create, Sell and Manage Gift Cards with Customized Email Templates: from n/a through 2.8.10.	2025-09-09	9.3	CVE-2025-47569
xwikisas--xwiki-pro-macros	XWiki Remote Macros provides XWiki rendering macros that are useful when migrating content from Confluence. Starting in version 1.0 and prior to version 1.26.5, missing escaping of the width parameter in the column macro allows remote code execution for any user who can edit any page or who can access the CKEditor converter. The width parameter is used without escaping in XWiki syntax,	2025-09-09	10	CVE-2025-55727

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	thus allowing XWiki syntax injection which enables remote code execution when the macro has been installed by a user with programming right, or it at least allows executing Velocity code as the wiki admin. Version 1.26.5 contains a patch for the issue.			
xwikisas--xwiki-pro-macros	XWiki Remote Macros provides XWiki rendering macros that are useful when migrating content from Confluence. Starting in version 1.0 and prior to version 1.26.5, missing escaping of the classes parameter in the panel macro allows remote code execution for any user who can edit any page The classes parameter is used without escaping in XWiki syntax, thus allowing XWiki syntax injection which enables remote code execution. Version 1.26.5 contains a patch for the issue.	2025-09-09	10	CVE-2025-55728
xwikisas--xwiki-pro-macros	XWiki Remote Macros provides XWiki rendering macros that are useful when migrating content from Confluence. Starting in version 1.0 and prior to version 1.26.5, missing escaping of the ac:type in the ConfluenceLayoutSection macro allows remote code execution for any user who can edit any page The classes parameter is used without escaping in XWiki syntax, thus allowing XWiki syntax injection which enables remote code execution. Version 1.26.5 has a fix for the issue.	2025-09-09	10	CVE-2025-55729
xwikisas--xwiki-pro-macros	XWiki Remote Macros provides XWiki rendering macros that are useful when migrating content from Confluence. Starting in version 1.0 and prior to version 1.26.5, missing escaping of the title in the confluence paste code macro allows remote code execution for any user who can edit any page. The classes parameter is used without escaping in XWiki syntax, thus allowing XWiki syntax injection which enables remote code execution. Version 1.26.5 has a fix for the issue.	2025-09-09	10	CVE-2025-55730
Zoom Communications, Inc--Zoom Workplace for Windows on ARM	Missing authorization in the installer for Zoom Workplace for Windows on ARM before version 6.5.0 may allow an authenticated user to conduct an escalation of privilege via local access.	2025-09-09	7.8	CVE-2025-49459
1000projects--Online Student Project Report Submission and Evaluation System	A vulnerability was determined in 1000projects Online Student Project Report Submission and Evaluation System 1.0. The affected element is an unknown function of the file /admin/controller/faculty_controller.php. This manipulation of the argument new_image causes unrestricted upload. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-15	7.3	CVE-2025-10424
1000projects--Online Student Project Report Submission and Evaluation System	A vulnerability was identified in 1000projects Online Student Project Report Submission and Evaluation System 1.0. The impacted element is an unknown function of the file /admin/controller/student_controller.php. Such manipulation of the argument new_image leads to unrestricted upload. The attack may be performed from remote. The exploit is publicly available and might be used.	2025-09-15	7.3	CVE-2025-10425
ABB--FLXEON	Use of a One-Way Hash with a Predictable Salt vulnerability in ABB FLXEON.This issue affects FLXEON: through 9.3.5. and newer versions	2025-09-17	8.8	CVE-2025-10205
ABB--FLXEON	Use of Hard-coded Credentials vulnerability in ABB FLXEON.This issue affects FLXEON: through 9.3.5 and newer versions	2025-09-17	7	CVE-2024-48842
ABB--FLXEON	Improper Validation of Specified Type of Input vulnerability in ABB FLXEON.A remote code execution is possible due to an improper input validation. This issue affects FLXEON: through 9.3.5.	2025-09-18	7.2	CVE-2024-48851
ABB--FLXEON	Improper Validation of Specified Type of Input vulnerability in ABB FLXEON.This issue affects FLXEON: through 9.3.5.	2025-09-18	7.2	CVE-2025-10207
Adobe--Substance3D - Stager	Substance3D - Stager versions 3.1.3 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-09-16	7.8	CVE-2025-54262
aliasvault--aliasvault	AliasVault is a privacy-first password manager with built-in email aliasing. A server-side request forgery (SSRF) vulnerability exists in the favicon extraction feature of AliasVault API versions 0.23.0 and lower. The extractor fetches a user-supplied URL, parses the returned HTML, and follows <link rel="icon" href="..."> . Although the initial URL is validated to allow only HTTP/HTTPS with default ports, the extractor automatically follows redirects and does not block requests to loopback or internal IP ranges. An authenticated, low-privileged user can exploit this behavior to coerce the backend into making HTTP(S) requests to arbitrary internal hosts and non-default ports. If the target host serves a favicon or any other valid image, the response is returned to the attacker in Base64 form. Even when no data is returned, timing and error behavior can be abused to map internal services. This vulnerability only affects self-hosted AliasVault instances that are reachable from the public internet with public user registration enabled. Private/internal	2025-09-19	7.7	CVE-2025-59344

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	deployments without public sign-ups are not directly exploitable. This issue has been fixed in AliasVault release 0.23.1.			
aonetheme--Service Finder Bookings	The Service Finder Bookings plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 6.0. This is due to the plugin not properly validating a user's identity prior to claiming a business when using the claim_business AJAX action. This makes it possible for unauthenticated attackers to login as any user including admins. Please note that subscriber privileges or brute-forcing are needed when completing the business takeover. The claim_id is needed to takeover the admin account, but brute-forcing is a practical approach to obtaining valid IDs.	2025-09-19	9.8	CVE-2025-5948
aonetheme--Service Finder SMS System	The Service Finder SMS System plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 2.0.0. This is due to the plugin not verifying a user's phone number before logging them in. This makes it possible for unauthenticated attackers to login as arbitrary users.	2025-09-19	8.1	CVE-2025-5955
Arma Store--Armalife	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), CWE - 200 - Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Arma Store Armalife allows SQL Injection.This issue affects Armalife: through 20250916. NOTE: The vendor did not inform about the completion of the fixing process within the specified time. The CVE will be updated when new information becomes available.	2025-09-16	9.8	CVE-2024-13149
Autodesk--Revit	A maliciously crafted PDF file, when parsed through certain Autodesk products, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.	2025-09-16	7.8	CVE-2025-8893
Autodesk--Revit	A maliciously crafted PDF file, when parsed through certain Autodesk products, can force a Heap-Based Overflow vulnerability. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	2025-09-16	7.8	CVE-2025-8894
Bearsthemes--Goza - Nonprofit Charity WordPress Theme	The Goza - Nonprofit Charity WordPress Theme theme for WordPress is vulnerable to unauthorized arbitrary file uploads due to a missing capability check on the 'beplus_import_pack_install_plugin' function in all versions up to, and including, 3.2.2. This makes it possible for unauthenticated attackers to upload zip files containing webshells disguised as plugins from remote locations to achieve remote code execution.	2025-09-19	9.8	CVE-2025-10690
Beyaz Computer--CityPlus	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Beyaz Computer CityPlus allows Path Traversal.This issue affects CityPlus: before 24.29375.	2025-09-19	7.5	CVE-2025-10468
BGS Interactive--SINAV.LINK Exam Result Module	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BGS Interactive SINAV.LINK Exam Result Module allows SQL Injection.This issue affects SINAV.LINK Exam Result Module: before 1.2.	2025-09-16	9.8	CVE-2025-4688
BMC--Control-M/Agent	An authentication bypass vulnerability exists in the out-of-support Control-M/Agent versions 9.0.18 to 9.0.20 and potentially earlier unsupported versions when using an empty or default kdb keystore or a default PKCS#12 keystore. A remote attacker with access to a signed third-party or demo certificate for client authentication can bypass the need for a certificate signed by the certificate authority of the organization during authentication on the Control-M/Agent. The Control-M/Agent contains hardcoded certificates which are only trusted as fallback if an empty kdb keystore is used; they are never trusted if a PKCS#12 keystore is used. All of these certificates are now expired. In addition, the Control-M/Agent default kdb and PKCS#12 keystores contain trusted third-party certificates (external recognized CAs and default self-signed demo certificates) which are trusted for client authentication.	2025-09-16	9	CVE-2025-55109
BMC--Control-M/Agent	If the Access Control List is enforced by the Control-M/Agent and the C router is in use (default in Out-of-support Control-M/Agent versions 9.0.18 to 9.0.20 and potentially earlier unsupported versions; non-default but configurable using the JAVA_AR setting in newer versions), the verification stops at the first NULL byte encountered in the email address referenced in the client certificate. An attacker could bypass configured ACLs by using a specially crafted certificate.	2025-09-16	9	CVE-2025-55113
BMC--Control-M/Agent	A path traversal in the Control-M/Agent can lead to a local privilege escalation when an attacker has access to the system running the Agent. This vulnerability impacts the out-of-support Control-M/Agent versions 9.0.18 to 9.0.20 and potentially earlier unsupported versions. This vulnerability was fixed in 9.0.20.100 and above.	2025-09-16	8.8	CVE-2025-55115
BMC--Control-M/Agent	A buffer overflow in the Control-M/Agent can lead to a local privilege escalation when an attacker has access to the system running the Agent. This vulnerability	2025-09-16	8.8	CVE-2025-55116

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	impacts the out-of-support Control-M/Agent versions 9.0.18 to 9.0.20 and potentially earlier unsupported versions.			
BMC--Control-M/Agent	Memory corruptions can be remotely triggered in the Control-M/Agent when SSL/TLS communication is configured. The issue occurs in the following cases: * Control-M/Agent 9.0.20: SSL/TLS configuration is set to the non-default setting "use_openssl=n"; * Control-M/Agent 9.0.21 and 9.0.22: Agent router configuration uses the non-default settings "JAVA_AR=N" and "use_openssl=n".	2025-09-16	8.9	CVE-2025-55118
BMC--Control-M/Agent	Out-of-support Control-M/Agent versions 9.0.18 to 9.0.20 (and potentially earlier unsupported versions) that are configured to use the non-default Blowfish cryptography algorithm use a hardcoded key. An attacker with access to network traffic and to this key could decrypt network traffic between the Control-M/Agent and Server.	2025-09-16	7.4	CVE-2025-55112
Campcodes--Computer Sales and Inventory System	A security flaw has been discovered in Campcodes Computer Sales and Inventory System 1.0. The affected element is an unknown function of the file /pages/cust_edit1.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be exploited.	2025-09-15	7.3	CVE-2025-10435
Campcodes--Computer Sales and Inventory System	A weakness has been identified in Campcodes Computer Sales and Inventory System 1.0. The impacted element is an unknown function of the file /pages/sup_searchfrm.php?action=edit. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	2025-09-15	7.3	CVE-2025-10436
Campcodes--Computer Sales and Inventory System	A weakness has been identified in Campcodes Computer Sales and Inventory System 1.0. Impacted is an unknown function of the file /pages/us_transac.php?action=add. Executing manipulation of the argument Username can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be exploited.	2025-09-15	7.3	CVE-2025-10445
Campcodes--Computer Sales and Inventory System	A security vulnerability has been detected in Campcodes Computer Sales and Inventory System 1.0. The affected element is an unknown function of the file /pages/cust_searchfrm.php?action=edit. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	2025-09-15	7.3	CVE-2025-10446
Campcodes--Grocery Sales and Inventory System	A security flaw has been discovered in Campcodes Grocery Sales and Inventory System 1.0. Affected is an unknown function of the file /ajax.php?action=delete_product. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	2025-09-15	7.3	CVE-2025-10417
Campcodes--Grocery Sales and Inventory System	A flaw has been found in Campcodes Grocery Sales and Inventory System 1.0. This affects an unknown function of the file /ajax.php?action=save_product. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	2025-09-16	7.3	CVE-2025-10562
Campcodes--Grocery Sales and Inventory System	A vulnerability has been found in Campcodes Grocery Sales and Inventory System 1.0. This impacts an unknown function of the file /ajax.php?action=save_category. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	2025-09-16	7.3	CVE-2025-10563
Campcodes--Grocery Sales and Inventory System	A vulnerability was found in Campcodes Grocery Sales and Inventory System 1.0. Affected is an unknown function of the file /ajax.php?action=delete_category. Performing manipulation of the argument ID results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	2025-09-16	7.3	CVE-2025-10564
Campcodes--Grocery Sales and Inventory System	A vulnerability was determined in Campcodes Grocery Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=delete_receiving. Executing manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	2025-09-16	7.3	CVE-2025-10565
Campcodes--Online Job Finder System	A security flaw has been discovered in Campcodes Online Job Finder System 1.0. This issue affects some unknown processing of the file /advancesearch.php. Performing manipulation of the argument Username results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.	2025-09-15	7.3	CVE-2025-10444
Campcodes--Online Job Finder System	A vulnerability was detected in Campcodes Online Job Finder System 1.0. The impacted element is an unknown function of the file /eris/applicationform.php. The manipulation of the argument picture results in unrestricted upload. It is possible to launch the attack remotely. The exploit is now public and may be used.	2025-09-15	7.3	CVE-2025-10447

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Campcodes--Online Job Finder System	A flaw has been found in Campcodes Online Job Finder System 1.0. This affects an unknown function of the file /index.php?q=result&searchfor=bycompany. This manipulation of the argument Search causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	2025-09-15	7.3	CVE-2025-10448
catchthemes--Catch Dark Mode	The Catch Dark Mode plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.0 via the 'catch_dark_mode' shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	2025-09-17	7.5	CVE-2025-10143
centos-webpanel--CentOS Web Panel	CWP (aka Control Web Panel or CentOS Web Panel) before 0.9.8.1205 allows unauthenticated remote code execution via shell metacharacters in the t_total parameter in a filemanager changePerm request. A valid non-root username must be known.	2025-09-19	9	CVE-2025-48703
Chaos Mesh—Chaos Controller Manager	The cleanTcs mutation in Chaos Controller Manager is vulnerable to OS command injection. In conjunction with CVE-2025-59358, this allows unauthenticated in-cluster attackers to perform remote code execution across the cluster.	2025-09-15	9.8	CVE-2025-59359
Chaos Mesh—Chaos Controller Manager	The killProcesses mutation in Chaos Controller Manager is vulnerable to OS command injection. In conjunction with CVE-2025-59358, this allows unauthenticated in-cluster attackers to perform remote code execution across the cluster.	2025-09-15	9.8	CVE-2025-59360
Chaos Mesh—Chaos Controller Manager	The cleanIptables mutation in Chaos Controller Manager is vulnerable to OS command injection. In conjunction with CVE-2025-59358, this allows unauthenticated in-cluster attackers to perform remote code execution across the cluster.	2025-09-15	9.8	CVE-2025-59361
Chaos Mesh—Chaos Controller Manager	The Chaos Controller Manager in Chaos Mesh exposes a GraphQL debugging server without authentication to the entire Kubernetes cluster, which provides an API to kill arbitrary processes in any Kubernetes pod, leading to cluster-wide denial of service.	2025-09-15	7.5	CVE-2025-59358
Cognex--In-Sight 2000 series	Cognex In-Sight Explorer and In-Sight Camera Firmware expose a telnet-based service on port 23 to allow management operations such as firmware upgrades and device reboots, which require authentication. A user with protected privileges can successfully invoke the SetSystemConfig functionality to modify relevant device properties (such as network settings), contradicting the security model proposed in the user manual.	2025-09-18	8.1	CVE-2025-52873
Cognex--In-Sight 2000 series	Cognex In-Sight Explorer and In-Sight Camera Firmware expose a service implementing a proprietary protocol on TCP port 1069 to allow the client-side software, such as the In-Sight Explorer tool, to perform management operations such as changing network settings or modifying users' access to the device.	2025-09-18	8.8	CVE-2025-53969
Cognex--In-Sight 2000 series	Cognex In-Sight Explorer and In-Sight Camera Firmware expose a telnet-based service on port 23 to allow management operations such as firmware upgrades and device reboots, which require authentication. A user with protected privileges can successfully invoke the SetSerialPort functionality to modify relevant device properties (such as serial interface settings), contradicting the security model proposed in the user manual.	2025-09-18	8.1	CVE-2025-54497
Cognex--In-Sight 2000 series	An attacker with adjacent access, without authentication, can exploit this vulnerability to retrieve a hard-coded password embedded in publicly available software. This password can then be used to decrypt sensitive network traffic, affecting the Cognex device.	2025-09-18	8	CVE-2025-54754
Cognex--In-Sight 2000 series	Cognex In-Sight Explorer and In-Sight Camera Firmware expose a proprietary protocol on TCP port 1069 to perform management operations such as modifying system properties. The user management functionality handles sensitive data such as registered usernames and passwords over an unencrypted channel, allowing an adjacent attacker to intercept valid credentials to gain access to the device.	2025-09-18	8	CVE-2025-54810
Cognex--In-Sight 2000 series	Cognex In-Sight Explorer and In-Sight Camera Firmware expose a proprietary protocol on TCP port 1069 to perform management operations such as modifying system properties. The user management functionality handles sensitive data such as registered usernames and passwords over an unencrypted channel, allowing an adjacent attacker to intercept valid credentials to gain access to the device.	2025-09-18	8	CVE-2025-54818
Cognex--In-Sight 2000 series	A local attacker with low privileges on the Windows system where the software is installed can exploit this vulnerability to corrupt sensitive data. A data folder is created with very weak privileges, allowing any user logged into the Windows system to modify its content.	2025-09-18	7.7	CVE-2025-53947

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cognex--In-Sight 2000 series	Cognex In-Sight Explorer and In-Sight Camera Firmware expose a telnet-based service on port 23 in order to allow management operations on the device such as firmware upgrades and device reboot requiring an authentication. A wrong management of login failures of the service allows a denial-of-service attack, leaving the telnet service into an unreachable state.	2025-09-18	7.7	CVE-2025-54860
cyberlord92--Miniorange OTP Verification with Firebase	The Miniorange OTP Verification with Firebase plugin for WordPress is vulnerable to privilege escalation due to a missing capability check on the 'handle_mofirebase_form_options' function in versions 3.1.0 to 3.6.2. This makes it possible for unauthenticated attackers to update the default role to Administrator. Premium features must be enabled in order to exploit the vulnerability.	2025-09-19	8.1	CVE-2025-7665
D-Link--DIR-825	A security flaw has been discovered in D-Link DIR-825 up to 2.10. Affected by this vulnerability is the function sub_4106d4 of the file apply.cgi. The manipulation of the argument countdown_time results in buffer overflow. The attack can be executed remotely. The exploit has been released to the public and may be exploited. This vulnerability only affects products that are no longer supported by the maintainer.	2025-09-18	8.8	CVE-2025-10666
Dassault Systmes--SOLIDWORKS eDrawings	An Out-Of-Bounds Read vulnerability affecting the PAR file reading procedure in SOLIDWORKS eDrawings on Release SOLIDWORKS Desktop 2025 could allow an attacker to execute arbitrary code while opening a specially crafted PAR file.	2025-09-17	7.8	CVE-2025-9447
Dassault Systmes--SOLIDWORKS eDrawings	A Use After Free vulnerability affecting the PAR file reading procedure in SOLIDWORKS eDrawings on Release SOLIDWORKS Desktop 2025 could allow an attacker to execute arbitrary code while opening a specially crafted PAR file.	2025-09-17	7.8	CVE-2025-9449
Dassault Systmes--SOLIDWORKS eDrawings	A Use of Uninitialized Variable vulnerability affecting the JT file reading procedure in SOLIDWORKS eDrawings on Release SOLIDWORKS Desktop 2025 could allow an attacker to execute arbitrary code while opening a specially crafted JT file.	2025-09-17	7.8	CVE-2025-9450
Digilent--WaveForms	Relative path traversal vulnerability due to improper input validation in Digilent WaveForms that may result in arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted .DWF3WORK file. This vulnerability affects Digilent WaveForms 3.24.3 and prior versions.	2025-09-15	7.8	CVE-2025-10203
Dokuzsoft Technology--E-Commerce Web Design Product	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Dokuzsoft Technology E-Commerce Web Design Product allows XSS Through HTTP Headers.This issue affects E-Commerce Web Design Product: before 11.08.2025.	2025-09-17	7.1	CVE-2025-8411
dolfinus--3DAlloy	3DAlloy is a lightWeight 3D-viewer for MediaWiki. From 1.0 through 1.8, the <3d> parser tag and the {{#3d}} parser function allow users to provide custom attributes that are then appended to the canvas HTML element that is being output by the extension. The attributes are not sanitized, which means that arbitrary JavaScript can be inserted and executed.	2025-09-15	8.6	CVE-2025-59332
Dolusoft--Omaspot	Cleartext Transmission of Sensitive Information vulnerability in Dolusoft Omaspot allows Interception, Privilege Escalation.This issue affects Omaspot: before 12.09.2025.	2025-09-16	9.6	CVE-2025-7743
Dolusoft--Omaspot	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Dolusoft Omaspot allows SQL Injection.This issue affects Omaspot: before 12.09.2025.	2025-09-16	9.8	CVE-2025-7744
Dover Fueling Solutions--ProGauge MagLink LX 4	Dover Fueling Solutions ProGauge MagLink LX4 Devices have default root credentials that cannot be changed through standard administrative means. An attacker with network access to the device can gain administrative access to the system.	2025-09-18	9.8	CVE-2025-30519
Dover Fueling Solutions--ProGauge MagLink LX 4	The secret used for validating authentication tokens is hardcoded in device firmware for affected versions. An attacker who obtains the signing key can bypass authentication, gaining complete access to the system.	2025-09-18	9.8	CVE-2025-54807
Dover Fueling Solutions--ProGauge MagLink LX 4	Dover Fueling Solutions ProGauge MagLink LX4 Devices fail to handle Unix time values beyond a certain point. An attacker can manually change the system time to exploit this limitation, potentially causing errors in authentication and leading to a denial-of-service condition.	2025-09-18	8.2	CVE-2025-55068
dyad-sh--dyad	Dyad is a local AI app builder. A critical security vulnerability has been discovered that affected Dyad v0.19.0 and earlier versions that allows attackers to execute arbitrary code on users' systems. The vulnerability affects the application's preview window functionality and can bypass Docker container protections. An attacker can craft web content that automatically executes when the preview loads. The malicious content can break out of the application's security boundaries and gain control of the system. This has been fixed in Dyad v0.20.0 and later.	2025-09-17	9.1	CVE-2025-58766
E1 Informatics--Web Application	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in E1 Informatics Web Application allows SQL Injection.This	2025-09-16	8.6	CVE-2024-13174

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	issue affects Web Application: through 20250916. NOTE: The vendor did not inform about the completion of the fixing process within the specified time. The CVE will be updated when new information becomes available.			
executeautomation--mcp-database-server	The mcp-database-server (MCP Server) 1.1.0 and earlier, as distributed via the npm package @executeautomation/database-server, fails to implement adequate security controls to properly enforce a "read-only" mode. This vulnerability affects only the npm distribution; other distributions are not impacted. As a result, the server is susceptible to abuse and attacks on affected database systems such as PostgreSQL, and potentially others that expose elevated functionalities. These attacks may lead to denial of service and other unexpected behaviors.	2025-09-16	8.1	CVE-2025-59333
Fortra--GoAnywhere MFT	A deserialization vulnerability in the License Servlet of Fortra's GoAnywhere MFT allows an actor with a validly forged license response signature to deserialize an arbitrary actor-controlled object, possibly leading to command injection.	2025-09-18	10	CVE-2025-10035
Gen Digital--CCleaner	Elevation of Privileges in the cleaning feature of Gen Digital CCleaner version 6.33.11465 on Windows allows a local user to gain SYSTEM privileges via exploiting insecure file delete operations. Reported in CCleaner v. 6.33.11465. This issue affects CCleaner: before < 6.36.11508.	2025-09-15	7.3	CVE-2025-3025
Gotac--Statistical Database System	Statistical Database System developed by Gotac has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read, modify, and delete database contents with high-level privileges.	2025-09-15	9.8	CVE-2025-10452
greenshot--greenshot	Greenshot is an open source Windows screenshot utility. Greenshot 1.3.300 and earlier deserializes attacker-controlled data received in a WM_COPYDATA message using BinaryFormatter.Deserialize without prior validation or authentication, allowing a local process at the same integrity level to trigger arbitrary code execution inside the Greenshot process. The vulnerable logic resides in a WinForms WndProc handler for WM_COPYDATA (message 74) that copies the supplied bytes into a MemoryStream and invokes BinaryFormatter.Deserialize, and only afterward checks whether the specified channel is authorized. Because the authorization check occurs after deserialization, any gadget chain embedded in the serialized payload executes regardless of channel membership. A local attacker who can send WM_COPYDATA to the Greenshot main window can achieve in-process code execution, which may aid evasion of application control policies by running payloads within the trusted, signed Greenshot.exe process. This issue is fixed in version 1.3.301. No known workarounds exist.	2025-09-16	8.4	CVE-2025-59050
Hewlett Packard Enterprise (HPE)--HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability in the command-line interface of HPE Aruba Networking EdgeConnect SD-WAN Gateways could allow an authenticated remote attacker to escalate privileges. Successful exploitation of this vulnerability may enable the attacker to execute arbitrary system commands with root privileges on the underlying operating system.	2025-09-16	8.8	CVE-2025-37123
Hewlett Packard Enterprise (HPE)--HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability in the HPE Aruba Networking SD-WAN Gateways could allow an unauthenticated remote attacker to bypass firewall protections. Successful exploitation could allow an attacker to route potentially harmful traffic through the internal network, leading to unauthorized access or disruption of services.	2025-09-16	8.6	CVE-2025-37124
Hewlett Packard Enterprise (HPE)--HPE Aruba Networking EdgeConnect SD-WAN Gateway	A broken access control vulnerability exists in HPE Aruba Networking EdgeConnect OS (ECOS). Successful exploitation could allow an attacker to bypass firewall protections, potentially leading to unauthorized traffic being handled improperly	2025-09-16	7.5	CVE-2025-37125
Hewlett Packard Enterprise (HPE)--HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability exists in the HPE Aruba Networking EdgeConnect SD-WAN Gateways Command Line Interface that allows remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of this vulnerability will result in the ability to execute arbitrary commands as root on the underlying operating system.	2025-09-16	7.2	CVE-2025-37126
Hewlett Packard Enterprise (HPE)--HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability in the cryptographic logic used by HPE Aruba Networking EdgeConnect SD-WAN Gateways could allow an authenticated remote attacker to gain shell access. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system, potentially leading to unauthorized access and control over the affected systems.	2025-09-16	7.2	CVE-2025-37127

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
HubSpot--jinjava	jinjava is a Java-based template engine based on django template syntax, adapted to render jinja templates. Priori to 2.8.1, by using mapper.getTypeFactory().constructFromCanonical(), it is possible to instruct the underlying ObjectMapper to deserialize attacker-controlled input into arbitrary classes. This enables the creation of semi-arbitrary class instances without directly invoking restricted methods or class literals. As a result, an attacker can escape the sandbox and instantiate classes such as java.net.URL, opening up the ability to access local files and URLs(e.g., file:///etc/passwd). With further chaining, this primitive can potentially lead to remote code execution (RCE). This vulnerability is fixed in 2.8.1.	2025-09-17	9.8	CVE-2025-59340
I-O DATA DEVICE, INC.--WN-7D36QR	Improper neutralization of special elements used in an OS command ('OS Command Injection') issue exists in WN-7D36QR and WN-7D36QR/UE. If this vulnerability is exploited, an arbitrary OS command may be executed by a remote authenticated attacker.	2025-09-17	7.2	CVE-2025-58116
IBM--AIX	IBM AIX 7.2, 7.3, IBM VIOS 3.1, and 4.1, when configured to use Kerberos network authentication, could allow a local user to write to files on the system with root privileges due to improper initialization of critical variables.	2025-09-16	7.4	CVE-2025-36244
itsourcecode--E-Logbook with Health Monitoring System for COVID-19	A flaw has been found in itsourcecode E-Logbook with Health Monitoring System for COVID-19 1.0. This issue affects some unknown processing of the file /check_profile.php. Executing manipulation of the argument profile_id can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	2025-09-18	7.3	CVE-2025-10670
itsourcecode--Online Discussion Forum	A weakness has been identified in itsourcecode Online Discussion Forum 1.0. Affected by this issue is some unknown functionality of the file /members/compose_msg.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	2025-09-18	7.3	CVE-2025-10667
itsourcecode--Online Discussion Forum	A security vulnerability has been detected in itsourcecode Online Discussion Forum 1.0. This affects an unknown part of the file /members/compose_msg_admin.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	2025-09-18	7.3	CVE-2025-10668
itsourcecode--Online Laundry Management System	A security flaw has been discovered in itsourcecode Online Laundry Management System 1.0. This affects an unknown function of the file /login.php. Performing manipulation of the argument Username results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	2025-09-15	7.3	CVE-2025-10426
itsourcecode--Student Information Management System	A vulnerability was determined in itsourcecode Student Information Management System 1.0. The impacted element is an unknown function of the file /admin/modules/class/index.php. This manipulation of the argument classId causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-18	7.3	CVE-2025-10673
itsourcecode--Web-Based Internet Laboratory Management System	A security flaw has been discovered in itsourcecode Web-Based Internet Laboratory Management System 1.0. Impacted is the function User::AuthenticateUser of the file login.php. Performing manipulation of the argument user_email results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.	2025-09-17	7.3	CVE-2025-10599
JetBrains--Junie	In JetBrains Junie before 252.284.66, 251.284.66, 243.284.66, 252.284.61, 251.284.61, 243.284.61, 252.284.50, 252.284.54, 251.284.54, 251.284.50, 243.284.54, 243.284.50 code execution was possible due to improper command validation	2025-09-17	8.3	CVE-2025-59458
JetBrains--TeamCity	In JetBrains TeamCity before 2025.07.2 missing Git URL validation allowed credential leakage on Windows	2025-09-17	7.7	CVE-2025-59457
kidaze--CourseSelectionSystem	A vulnerability was determined in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. This vulnerability affects unknown code of the file /Profilers/PriProfile/COUNT2.php. This manipulation of the argument cname causes sql injection. The attack may be initiated remotely. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available.	2025-09-17	7.3	CVE-2025-10597
kodezen--StoreEngine Powerful WordPress eCommerce Plugin for Payments,	The StoreEngine - Powerful WordPress eCommerce Plugin for Payments, Memberships, Affiliates, Sales & More plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the import() function in all versions up to, and including, 1.5.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2025-09-17	8.8	CVE-2025-9216

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Memberships, Affiliates, Sales & More				
Kovah--LinkAce	LinkAce is a self-hosted archive to collect website links. Prior to 2.3.1, a Stored Cross-Site Scripting (XSS) vulnerability has been identified on the /system/audit page. The application fails to properly sanitize the username field before it is rendered in the audit log. An authenticated attacker can set a malicious JavaScript payload as their username. When an action performed by this user is recorded (e.g., generate or revoke an API token), the payload is stored in the database. The script is then executed in the browser of any user, particularly administrators, who views the /system/audit page. This vulnerability is fixed in 2.3.1.	2025-09-18	7.3	CVE-2025-59424
lemonldap-ng--LemonLDAP::NG	In LemonLDAP::NG before 2.16.7 and 2.17 through 2.21 before 2.21.3, OS command injection can occur in the Safe jail. It does not Localize _ during rule evaluation. Thus, an administrator who can edit a rule evaluated by the Safe jail can execute commands on the server.	2025-09-17	8	CVE-2025-59518
libexpat project--libexpat	libexpat in Expat before 2.7.2 allows attackers to trigger large dynamic memory allocations via a small document that is submitted for parsing.	2025-09-15	7.5	CVE-2025-59375
Logo Software--Diva	Authorization Bypass Through User-Controlled SQL Primary Key, CWE - 89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Logo Software Diva allows SQL Injection, CAPEC - 7 - Blind SQL Injection.This issue affects Diva: through 4.56.00.00.	2025-09-18	10	CVE-2024-13151
Mattermost--Mattermost	Mattermost versions 10.8.x <= 10.8.3, 10.5.x <= 10.5.8, 9.11.x <= 9.11.17, 10.10.x <= 10.10.1, 10.9.x <= 10.9.3 fail to validate import directory path configuration which allows admin users to execute arbitrary code via malicious plugin upload to prepackaged plugins directory	2025-09-19	8	CVE-2025-9079
Mattermost--Mattermost	Mattermost versions 10.10.x <= 10.10.1, 10.5.x <= 10.5.9, 10.9.x <= 10.9.4 fail to validate the redirect_to parameter, allowing an attacker to craft a malicious link that, once a user authenticates with their SAML provider, could post the user's cookies to an attacker-controlled URL.	2025-09-15	7.6	CVE-2025-9072
Megatek Communication System--Azora Wireless Network Management	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Megatek Communication System Azora Wireless Network Management allows SQL Injection.This issue affects Azora Wireless Network Management: through 20250916. NOTE: The vendor did not inform about the completion of the fixing process within the specified time. The CVE will be updated when new information becomes available.	2025-09-16	8.8	CVE-2024-12913
Microsoft--Windows Server 2022	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	2025-09-18	7	CVE-2025-59220
Microsoft--Windows Server 2025 (Server Core installation)	Use after free in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2025-09-18	7	CVE-2025-59215
Microsoft--Windows Server 2025 (Server Core installation)	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2025-09-18	7	CVE-2025-59216
mohammadzain2008--Linkr	Linkr is a lightweight file delivery system that downloads files from a webserver. Linkr versions through 2.0.0 do not verify the integrity or authenticity of .linkr manifest files before using their contents, allowing a tampered manifest to inject arbitrary file entries into a package distribution. An attacker can modify a generated .linkr manifest (for example by adding a new entry with a malicious URL) and when a user runs the extract command the client downloads the attacker-supplied file without verification. This enables arbitrary file injection and creates a potential path to remote code execution if a downloaded malicious binary or script is later executed. Version 2.0.1 adds a manifest integrity check that compares the checksum of the original author-created manifest to the one being extracted and aborts on mismatch, warning if no original manifest is hosted. Users should update to 2.0.1 or later. As a workaround prior to updating, use only trusted .linkr manifests, manually verify manifest integrity, and host manifests on trusted servers.	2025-09-16	9.7	CVE-2025-59334
MongoDB Inc--MongoDB Server	The MongoDB Windows installation MSI may leave ACLs unset on custom installation directories allowing a local attacker to introduce executable code to MongoDB's process via DLL hijacking. This issue affects MongoDB Server v6.0 version prior to 6.0.25, MongoDB Server v7.0 version prior to 7.0.21 and MongoDB Server v8.0 version prior to 8.0.5	2025-09-15	7.8	CVE-2025-10491

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
N-Partner--N-Reporter	The N-Reporter, N-Cloud, and N-Probe developed by N-Partner has an OS Command Injection vulnerability, allowing authenticated remote attackers to inject arbitrary OS commands and execute them on the server.	2025-09-17	8.8	CVE-2025-10589
n/a--07FLYCMS	A vulnerability was found in 07FLYCMS, 07FLY-CMS and 07FlyCRM up to 20250831. This issue affects some unknown processing of the file /index.php/Login/login. Performing manipulation of the argument Username results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used. This product is published under multiple names. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-19	7.3	CVE-2025-10712
NetApp--StorageGRID	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8.0.15 and 11.9.0.8 without Single Sign-on enabled are susceptible to a Server-Side Request Forgery (SSRF) vulnerability. Successful exploit could allow an unauthenticated attacker to change the password of any Grid Manager or Tenant Manager non-federated user.	2025-09-19	7.5	CVE-2025-26515
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability in the Python backend, where an attacker could cause a remote code execution by manipulating the model name parameter in the model control APIs. A successful exploit of this vulnerability might lead to remote code execution, denial of service, information disclosure, and data tampering.	2025-09-17	9.8	CVE-2025-23316
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server contains a vulnerability in the DALI backend where an attacker may cause an improper input validation issue. A successful exploit of this vulnerability may lead to code execution.	2025-09-17	8	CVE-2025-23268
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where an attacker could cause an out-of-bounds write through a specially crafted input. A successful exploit of this vulnerability might lead to denial of service.	2025-09-17	7.5	CVE-2025-23328
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where an attacker could cause memory corruption by identifying and accessing the shared memory region used by the Python backend. A successful exploit of this vulnerability might lead to denial of service.	2025-09-17	7.5	CVE-2025-23329
PHPGurukul--Beauty Parlour Management System	A security flaw has been discovered in PHPGurukul Beauty Parlour Management System 1.1. This affects an unknown part of the file /admin/all-appointment.php. The manipulation of the argument delid results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	2025-09-15	7.3	CVE-2025-10459
PHPGurukul--Online Course Registration	A vulnerability was found in PHPGurukul Online Course Registration 3.1. This affects an unknown function of the file /my-profile.php. Performing manipulation of the argument cgpa results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	2025-09-18	7.3	CVE-2025-10663
PHPGurukul--Online Discussion Forum	A vulnerability was determined in PHPGurukul Online Discussion Forum 1.0. Affected by this issue is some unknown functionality of the file /admin/admin_forum/search_result.php. Executing manipulation of the argument Search can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-17	7.3	CVE-2025-10603
PHPGurukul--Online Discussion Forum	A vulnerability was identified in PHPGurukul Online Discussion Forum 1.0. This affects an unknown part of the file /admin/edit_member.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	2025-09-17	7.3	CVE-2025-10604
PHPGurukul--Small CRM	A vulnerability was determined in PHPGurukul Small CRM 4.0. This impacts an unknown function of the file /create-ticket.php. Executing manipulation of the argument subject can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-18	7.3	CVE-2025-10664
PHPGurukul--User Management System	A security flaw has been discovered in PHPGurukul User Management System 1.0. This affects an unknown function of the file /login.php. Performing manipulation of the argument emailid results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	2025-09-17	7.3	CVE-2025-10624
Planet Technology--ICG-2510WG-LTE (EU/US)	Certain models of Industrial Cellular Gateway developed by Planet Technology have a Missing Authentication vulnerability, allowing unauthenticated remote attackers to manipulate the device via a specific functionality.	2025-09-17	9.8	CVE-2025-9971
Planet Technology--ICG-2510WG-LTE (EU/US)	The N-Reporter, N-Cloud, and N-Probe developed by N-Partner has an OS Command Injection vulnerability, allowing authenticated remote attackers to inject arbitrary OS commands and execute them on the server.	2025-09-17	9.8	CVE-2025-9972
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in Podman. In a Containerfile or Podman, data written to RUN --mount=type=bind mounts during the podman build is not discarded. This issue can lead to files created within the container appearing in the temporary build context directory on the host, leaving the created files accessible.	2025-09-16	7.4	CVE-2025-4953

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
salzano--Embed PDF for WPForms	The Embed PDF for WPForms plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the ajax_handler_download_pdf_media function in all versions up to, and including, 1.1.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2025-09-19	8.8	CVE-2025-10647
Sitecore--Sitecore Experience Manager (XM)	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Sitecore Sitecore Experience Manager (XM), Sitecore Experience Platform (XP) allows Cross-Site Scripting (XSS).This issue affects Sitecore Experience Manager (XM): from 9.2 through 10.4; Experience Platform (XP): from 9.2 through 10.4.	2025-09-21	7.1	CVE-2025-53692
smackcoders--WP Import Ultimate CSV XML Importer for WordPress	The WP Import - Ultimate CSV XML Importer for WordPress plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 7.28. This is due to the write_to_customfile() function writing unfiltered PHP code to a file. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject the customFunction.php file with PHP code that can be accessed to trigger remote code execution.	2025-09-17	8.8	CVE-2025-10057
smackcoders--WP Import Ultimate CSV XML Importer for WordPress	The WP Import - Ultimate CSV XML Importer for WordPress plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the upload_function() function in all versions up to, and including, 7.27. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	2025-09-17	8.1	CVE-2025-10058
SmartVista Suite -- 2.2.22	Cross Site Request Forgery (CSRF) vulnerability in Smartvista BackOffice SmartVista Suite 2.2.22 via crafted GET request.	2025-09-18	7.8	CVE-2025-50255
SourceCodester--Hotel Reservation System	A vulnerability was determined in SourceCodester Hotel Reservation System 1.0. The affected element is an unknown function of the file editroomimage.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.	2025-09-17	7.3	CVE-2025-10621
SourceCodester--Hotel Reservation System	A vulnerability was identified in SourceCodester Hotel Reservation System 1.0. The impacted element is an unknown function of the file deleteuser.php. 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.	2025-09-17	7.3	CVE-2025-10623
SourceCodester--Online Exam Form Submission	A vulnerability was found in SourceCodester Online Exam Form Submission 1.0. This affects an unknown part of the file /index.php. The manipulation of the argument usn results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	2025-09-17	7.3	CVE-2025-10596
SourceCodester--Online Exam Form Submission	A flaw has been found in SourceCodester Online Exam Form Submission 1.0. This impacts an unknown function of the file /register.php. This manipulation of the argument img causes unrestricted upload. It is possible to initiate the attack remotely. The exploit has been published and may be used.	2025-09-17	7.3	CVE-2025-10600
SourceCodester--Online Exam Form Submission	A vulnerability has been found in SourceCodester Online Exam Form Submission 1.0. Affected is an unknown function of the file /admin/index.php. Such manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2025-09-17	7.3	CVE-2025-10601
SourceCodester--Online Student File Management System	A security flaw has been discovered in SourceCodester Online Student File Management System 1.0. The impacted element is an unknown function of the file /index.php. Performing manipulation of the argument stud_no results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	2025-09-15	7.3	CVE-2025-10479
SourceCodester--Online Student File Management System	A vulnerability was detected in SourceCodester Online Student File Management System 1.0. Affected is an unknown function of the file /admin/index.php. The manipulation of the argument Username results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	2025-09-15	7.3	CVE-2025-10482
SourceCodester--Pet Grooming Management Software	A vulnerability was identified in SourceCodester Pet Grooming Management Software 1.0. This issue affects some unknown processing of the file /admin/search_product.php. Such manipulation of the argument group_id leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	2025-09-17	7.3	CVE-2025-10598
SourceCodester--Pet Grooming Management Software	A vulnerability was determined in SourceCodester Pet Grooming Management Software 1.0. This vulnerability affects unknown code of the file /admin/operation/paid.php. This manipulation of the argument inv_no/insta_amt causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-18	7.3	CVE-2025-10688

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SourceCodester--Responsive E-Learning System	A vulnerability was found in SourceCodester Responsive E-Learning System 1.0. This affects an unknown part of the file /admin/add_teacher.php. The manipulation of the argument Username results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	2025-09-18	7.3	CVE-2025-10687
Spring--Cloud Gateway	Spring Cloud Gateway Server Webflux may be vulnerable to Spring Environment property modification. An application should be considered vulnerable when all the following are true: * The application is using Spring Cloud Gateway Server Webflux (Spring Cloud Gateway Server WebMVC is not vulnerable). * Spring Boot actuator is a dependency. * The Spring Cloud Gateway Server Webflux actuator web endpoint is enabled via management.endpoints.web.exposure.include=gateway. * The actuator endpoints are available to attackers. * The actuator endpoints are unsecured.	2025-09-16	10	CVE-2025-41243
SUSE--neuvector	A vulnerability exists in NeuVector versions up to and including 5.4.5, where a fixed string is used as the default password for the built-in `admin` account. If this password is not changed immediately after deployment, any workload with network access within the cluster could use the default credentials to obtain an authentication token. This token can then be used to perform any operation via NeuVector APIs.	2025-09-17	9.8	CVE-2025-8077
Tenda--AC1206	A vulnerability was found in Tenda AC1206 15.03.06.23. This vulnerability affects the function check_param_changed of the file /goform/AdvSetMacMtuWa of the component HTTP Request Handler. Performing manipulation of the argument wanMTU results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	2025-09-15	9.8	CVE-2025-10432
Tenda--AC9	A vulnerability was identified in Tenda AC9 and AC15 15.03.05.14/15.03.05.18. This vulnerability affects the function formexeCommand of the file /goform/exeCommand. Such manipulation of the argument cmdinput leads to buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used.	2025-09-15	8.8	CVE-2025-10443
UTT--1200GW	A weakness has been identified in UTT 1200GW up to 3.0.0-170831. The affected element is an unknown function of the file /goform/formConfigDnsFilterGlobal. This manipulation of the argument GroupName causes buffer overflow. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-20	8.8	CVE-2025-10757
UTT--HiPER 840G	A security flaw has been discovered in UTT HiPER 840G up to 3.1.1-190328. Impacted is an unknown function of the file /goform/getOneApConfTempEntry. The manipulation of the argument tempName results in buffer overflow. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-20	8.8	CVE-2025-10756
Vegagrup Software--Vega Master	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Vegagrup Software Vega Master allows Directory Indexing.This issue affects Vega Master: from v.1.12.35 through 20250916. NOTE: The vendor did not inform about the completion of the fixing process within the specified time. The CVE will be updated when new information becomes available.	2025-09-16	8.6	CVE-2024-12367
Vizly Web Design--Real Estate Packages	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Vizly Web Design Real Estate Packages allows Content Spoofing, CAPEC - 593 - Session Hijacking, CAPEC - 591 - Reflected XSS.This issue affects Real Estate Packages: before 5.1.	2025-09-19	7.1	CVE-2025-9969
VMware--Spring Framework	The Spring Framework annotation detection mechanism may not correctly resolve annotations on methods within type hierarchies with a parameterized super type with unbounded generics. This can be an issue if such annotations are used for authorization decisions. Your application may be affected by this if you are using Spring Security's @EnableMethodSecurity feature. You are not affected by this if you are not using @EnableMethodSecurity or if you do not use security annotations on methods in generic superclasses or generic interfaces. This CVE is published in conjunction with CVE-2025-41248 https://spring.io/security/cve-2025-41248 .	2025-09-16	7.5	CVE-2025-41249
VMware--Spring Security	The Spring Security annotation detection mechanism may not correctly resolve annotations on methods within type hierarchies with a parameterized super type with unbounded generics. This can be an issue when using @PreAuthorize and other method security annotations, resulting in an authorization bypass. Your application may be affected by this if you are using Spring Security's @EnableMethodSecurity feature. You are not affected by this if you are not using @EnableMethodSecurity or if you do not use security annotations on methods in	2025-09-16	7.5	CVE-2025-41248

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	generic superclasses or generic interfaces. This CVE is published in conjunction with CVE-2025-41249 https://spring.io/security/cve-2025-41249 .			
whuan132--AIBattery	A vulnerability was found in whuan132 AIBattery up to 1.0.9. The affected element is an unknown function of the file AIBatteryHelper/XPC/BatteryXPCService.swift of the component com.collweb.AIBatteryHelper. The manipulation results in missing authentication. The attack requires a local approach. The exploit has been made public and could be used.	2025-09-18	7.8	CVE-2025-10672
wplegalpages--Privacy Policy Generator, Terms & Conditions Generator WordPress Plugin : WP Legal Pages	The Privacy Policy Generator, Terms & Conditions Generator WordPress Plugin : WP Legal Pages plugin for WordPress is vulnerable to unauthorized access of functionality due to a missing capability check on the wplp_gdpr_install_plugin_ajax_handler() function in all versions up to, and including, 3.4.3. This makes it possible for authenticated attackers, with Contributor-level access and above, to install arbitrary repository plugins.	2025-09-18	8.1	CVE-2025-8565
Yordam Informatics--Yordam Library Automation System	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Yordam Informatics Yordam Library Automation System allows SQL Injection.This issue affects Yordam Library Automation System: from 21.5 & 21.6 before 21.7.	2025-09-17	9.8	CVE-2025-10439
zephyrproject-rtos--Zephyr	A vulnerability was identified in the handling of Bluetooth Low Energy (BLE) fixed channels (such as SMP or ATT). Specifically, an attacker could exploit a flaw that causes the BLE target (i.e., the device under attack) to attempt to disconnect a fixed channel, which is not allowed per the Bluetooth specification. This leads to undefined behavior, including potential assertion failures, crashes, or memory corruption, depending on the BLE stack implementation.	2025-09-19	7.1	CVE-2025-10456
zephyrproject-rtos--Zephyr	Parameters are not validated or sanitized, and are later used in various internal operations.	2025-09-19	7.6	CVE-2025-10458
zephyrproject-rtos--Zephyr	Unsafe handling in bt_conn_tx_processor causes a use-after-free, resulting in a write-before-zero. The written 4 bytes are attacker-controlled, enabling precise memory corruption.	2025-09-19	7.6	CVE-2025-7403
1000projects--Bookstore Management System	A vulnerability was determined in 1000projects Bookstore Management System 1.0. The impacted element is an unknown function of the file /login.php. This manipulation of the argument unm causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-23	7.3	CVE-2025-10833
Aftabul Islam--Stock Message	Cross-Site Request Forgery (CSRF) vulnerability in Aftabul Islam Stock Message allows Stored XSS. This issue affects Stock Message: from n/a through 1.1.0.	2025-09-22	7.1	CVE-2025-58267
Airship AI--Acropolis	Airship AI Acropolis includes a default administrative account that uses the same credentials on every installation. Instances of Airship AI that do not change this account password are vulnerable to a remote attacker logging in and gaining the privileges of this account. Fixed in 10.2.35, 11.0.21, and 11.1.9.	2025-09-22	9.8	CVE-2025-35042
Airship AI--Acropolis	Airship AI Acropolis allows unlimited MFA attempts for 15 minutes after a user has logged in with valid credentials. A remote attacker with valid credentials could brute-force the 6-digit MFA code. Fixed in 10.2.35, 11.0.21, and 11.1.9.	2025-09-22	7.5	CVE-2025-35041
Anps--Constructo	Cross-Site Request Forgery (CSRF) vulnerability in Anps Constructo allows Object Injection. This issue affects Constructo: from n/a through 4.3.9.	2025-09-22	8.8	CVE-2025-58244
apollographql--embeddable-explorer	Apollo Studio Embeddable Explorer & Embeddable Sandbox are website embeddable software solutions from Apollo GraphQL. Prior to Apollo Sandbox version 2.7.2 and Apollo Explorer version 3.7.3, a cross-site request forgery (CSRF) vulnerability was identified. The vulnerability arises from missing origin validation in the client-side code that handles window.postMessage events. A malicious website can send forged messages to the embedding page, causing the victim's browser to execute arbitrary GraphQL queries or mutations against their GraphQL server while authenticated with the victim's cookies. This issue has been patched in Apollo Sandbox version 2.7.2 and Apollo Explorer version 3.7.3.	2025-09-26	8.2	CVE-2025-59845
ApusTheme--Findgo	Cross-Site Request Forgery (CSRF) vulnerability in ApusTheme Findgo allows Authentication Bypass. This issue affects Findgo: from n/a through 1.3.55.	2025-09-22	8.8	CVE-2025-58250
Ashwani kumar--GST for WooCommerce	Cross-Site Request Forgery (CSRF) vulnerability in Ashwani kumar GST for WooCommerce allows Stored XSS. This issue affects GST for WooCommerce: from n/a through 2.0.	2025-09-26	7.1	CVE-2025-60173
authlib--authlib	Authlib is a Python library which builds OAuth and OpenID Connect servers. Prior to version 1.6.4, Authlib's JWS verification accepts tokens that declare unknown critical header parameters (crit), violating RFC 7515 "must-understand" semantics. An attacker can craft a signed token with a critical header (for example, bork or cnf) that strict verifiers reject but Authlib accepts. In mixed-language fleets, this	2025-09-22	7.5	CVE-2025-59420

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	enables split-brain verification and can lead to policy bypass, replay, or privilege escalation. This issue has been patched in version 1.6.4.			
Autodesk--Fusion	A maliciously crafted HTML payload, when rendered by the Autodesk Fusion desktop application, can trigger a Stored Cross-site Scripting (XSS) vulnerability. A malicious actor may leverage this vulnerability to read local files or execute arbitrary code in the context of the current process.	2025-09-23	8.7	CVE-2025-10244
Autodesk--Revit	A maliciously crafted RFA file, when parsed through Autodesk Revit, can force a Type Confusion vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.	2025-09-23	7.8	CVE-2025-8354
Autodesk--Shared Components	A maliciously crafted PRT file, when parsed through certain Autodesk products, can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	2025-09-22	7.8	CVE-2025-8892
AutomationDirect--CLICK PLUS C0-0x CPU firmware	A predictable seed in pseudo-random number generator vulnerability has been discovered in firmware version 3.60 of the Click Plus PLC. The vulnerability relies on the fact that the software implements a predictable seed for its pseudo-random number generator, which compromises the security of the generated private keys.	2025-09-23	8.3	CVE-2025-55069
AutomationDirect--CLICK PLUS C0-0x CPU firmware	The use of a broken or risky cryptographic algorithm was discovered in firmware version 3.60 of the Click Plus PLC. The vulnerability relies on the fact that the software uses an insecure implementation of the RSA encryption algorithm.	2025-09-23	8.3	CVE-2025-59484
awesomesupport--Awesome Support	Deserialization of Untrusted Data vulnerability in awesomesupport Awesome Support allows Object Injection. This issue affects Awesome Support: from n/a through 6.3.4.	2025-09-22	7.2	CVE-2025-58662
B-Link--BL-AC2100	A security flaw has been discovered in B-Link BL-AC2100 up to 1.0.3. Affected by this issue is the function delshrpath of the file /goform/set_delshrpath_cfg of the component Web Management Interface. The manipulation of the argument Type 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. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-22	8.8	CVE-2025-10773
Campcodes--Advanced Online Voting Management System	A weakness has been identified in Campcodes Advanced Online Voting Management System 1.0. This affects an unknown function of the file /admin/candidates_edit.php. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	2025-09-28	7.3	CVE-2025-11111
Campcodes--Computer Sales and Inventory System	A vulnerability was detected in Campcodes Computer Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /pages/sup_edit1.php. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	2025-09-23	7.3	CVE-2025-10829
Campcodes--Computer Sales and Inventory System	A flaw has been found in Campcodes Computer Sales and Inventory System 1.0. This issue affects some unknown processing of the file /pages/inv_edit1.php. Executing manipulation of the argument idd can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	2025-09-23	7.3	CVE-2025-10830
Campcodes--Computer Sales and Inventory System	A vulnerability has been found in Campcodes Computer Sales and Inventory System 1.0. Impacted is an unknown function of the file /pages/pro_edit1.php. The manipulation of the argument prodcode leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	2025-09-23	7.3	CVE-2025-10831
Campcodes--Computer Sales and Inventory System	A security vulnerability has been detected in Campcodes Computer Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/us_edit1.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	2025-09-26	7.3	CVE-2025-11039
Campcodes--Computer Sales and Inventory System	A vulnerability was identified in Campcodes Computer Sales and Inventory System 1.0. The affected element is an unknown function of the file /pages/us_edit.php?action=edit. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	2025-09-28	7.3	CVE-2025-11109
Campcodes--Farm Management System	A weakness has been identified in Campcodes Farm Management System 1.0. Impacted is an unknown function of the file /uploadProduct.php. This manipulation of the argument Type causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	2025-09-22	7.3	CVE-2025-10808
Campcodes--Grocery Sales and Inventory System	A vulnerability was detected in Campcodes Grocery Sales and Inventory System 1.0. This affects an unknown part of the file /manage_user.php. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	2025-09-22	7.3	CVE-2025-10785

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Campcodes--Grocery Sales and Inventory System	A flaw has been found in Campcodes Grocery Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /ajax.php?action=delete_user. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	2025-09-22	7.3	CVE-2025-10786
Campcodes--Gym Management System	A security flaw has been discovered in Campcodes Gym Management System 1.0. Impacted is an unknown function of the file /ajax.php?action=login. Performing manipulation of the argument Username results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	2025-09-23	7.3	CVE-2025-10851
Campcodes--Online Learning Management System	A vulnerability was identified in Campcodes Online Learning Management System 1.0. This impacts an unknown function of the file /admin/edit_class.php. Such manipulation of the argument class_name leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	2025-09-22	7.3	CVE-2025-10781
Campcodes--Online Learning Management System	A security flaw has been discovered in Campcodes Online Learning Management System 1.0. Affected is an unknown function of the file /admin/class.php. Performing manipulation of the argument class_name results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.	2025-09-22	7.3	CVE-2025-10782
Campcodes--Online Learning Management System	A weakness has been identified in Campcodes Online Learning Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/add_subject.php. Executing manipulation of the argument subject_code can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be exploited.	2025-09-22	7.3	CVE-2025-10783
Campcodes--Online Learning Management System	A security vulnerability has been detected in Campcodes Online Learning Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/edit_subject.php. The manipulation of the argument subject_code leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	2025-09-22	7.3	CVE-2025-10784
Campcodes--Online Learning Management System	A security vulnerability has been detected in Campcodes Online Learning Management System 1.0. The affected element is an unknown function of the file /admin/department.php. Such manipulation of the argument d leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	2025-09-22	7.3	CVE-2025-10809
Campcodes--Online Learning Management System	A vulnerability was detected in Campcodes Online Learning Management System 1.0. The impacted element is an unknown function of the file /admin/edit_user.php. Performing manipulation of the argument firstname results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2025-09-22	7.3	CVE-2025-10810
Campcodes--Online Learning Management System	A weakness has been identified in Campcodes Online Learning Management System 1.0. This vulnerability affects unknown code of the file /admin/admin_user.php. Executing manipulation of the argument firstname can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	2025-09-22	7.3	CVE-2025-10817
Campcodes--Online Learning Management System	A vulnerability was found in Campcodes Online Learning Management System 1.0. This affects an unknown part of the file /admin/edit_student.php. Performing manipulation of the argument cys results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	2025-09-27	7.3	CVE-2025-11061
Campcodes--Online Learning Management System	A vulnerability was determined in Campcodes Online Learning Management System 1.0. This vulnerability affects unknown code of the file /admin/save_student.php. Executing manipulation of the argument class_id can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	2025-09-27	7.3	CVE-2025-11062
Campcodes--Online Learning Management System	A vulnerability was identified in Campcodes Online Learning Management System 1.0. This issue affects some unknown processing of the file /admin/edit_department.php. The manipulation of the argument d leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	2025-09-27	7.3	CVE-2025-11063
Campcodes--Online Learning Management System	A security flaw has been discovered in Campcodes Online Learning Management System 1.0. Impacted is an unknown function of the file /admin/teachers.php. The manipulation of the argument department results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	2025-09-27	7.3	CVE-2025-11064
Campcodes--Online Learning	A vulnerability has been found in Campcodes Online Learning Management System 1.0. This affects an unknown function of the file /admin/de_activate.php. Such	2025-09-27	7.3	CVE-2025-11075

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.			
Campcodes--Online Learning Management System	A vulnerability was found in Campcodes Online Learning Management System 1.0. This impacts an unknown function of the file /admin/edit_teacher.php. Performing manipulation of the argument department results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	2025-09-27	7.3	CVE-2025-11076
Campcodes--Online Learning Management System	A vulnerability was determined in Campcodes Online Learning Management System 1.0. Affected is an unknown function of the file /admin/add_content.php. Executing manipulation of the argument Title can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-27	7.3	CVE-2025-11077
Campcodes--Online Learning Management System	A weakness has been identified in Campcodes Online Learning Management System 1.0. Affected is an unknown function of the file /admin/edit_content.php. Executing manipulation of the argument Title can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.	2025-09-28	7.3	CVE-2025-11102
Campcodes--Online Learning Management System	A security flaw has been discovered in Campcodes Online Learning Management System 1.0. The impacted element is an unknown function of the file /admin/school_year.php. The manipulation of the argument school_year results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	2025-09-28	7.3	CVE-2025-11110
Campcodes--Point of Sale System POS	A security flaw has been discovered in Campcodes Point of Sale System POS 1.0. Affected by this issue is some unknown functionality of the file /login.php. Performing manipulation of the argument Username results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited.	2025-09-23	7.3	CVE-2025-10857
Casengo--Casengo Live Chat Support	Cross-Site Request Forgery (CSRF) vulnerability in Casengo Casengo Live Chat Support allows Stored XSS. This issue affects Casengo Live Chat Support: from n/a through 2.1.4.	2025-09-22	7.1	CVE-2025-58688
Cisco--Cisco Adaptive Security Appliance (ASA) Software	A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to improper validation of user-supplied input in HTTP(S) requests. An attacker with valid VPN user credentials could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code as root, possibly resulting in the complete compromise of the affected device.	2025-09-25	9.9	CVE-2025-20333
Cisco--Cisco IOS XE Software	A vulnerability in the Network-Based Application Recognition (NBAR) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, causing a denial of service (DoS) condition. This vulnerability is due to improper handling of malformed Control and Provisioning of Wireless Access Points (CAPWAP) packets. An attacker could exploit this vulnerability by sending malformed CAPWAP packets through an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.	2025-09-24	8.6	CVE-2025-20315
Cisco--Cisco IOS XE Software	A vulnerability in the HTTP API subsystem of Cisco IOS XE Software could allow a remote attacker to inject commands that will execute with root privileges into the underlying operating system. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by authenticating to an affected system and performing an API call with crafted input. Alternatively, an unauthenticated attacker could persuade a legitimate user with administrative privileges who is currently logged in to the system to click a crafted link. A successful exploit could allow the attacker to execute arbitrary commands as the root user.	2025-09-24	8.8	CVE-2025-20334
Cisco--Cisco IOS XE Software	A vulnerability in the handling of certain Ethernet frames in Cisco IOS XE Software for Catalyst 9000 Series Switches could allow an unauthenticated, adjacent attacker to cause an egress port to become blocked and drop all outbound traffic. This vulnerability is due to improper handling of crafted Ethernet frames. An attacker could exploit this vulnerability by sending crafted Ethernet frames through an affected switch. A successful exploit could allow the attacker to cause the egress port to which the crafted frame is forwarded to start dropping all frames, resulting in a denial of service (DoS) condition.	2025-09-24	7.4	CVE-2025-20311
Cisco--Cisco IOS XE Software	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS XE Software could allow an authenticated, remote attacker to cause a	2025-09-24	7.7	CVE-2025-20312

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	denial of service (DoS) condition on an affected device. This vulnerability is due to improper error handling when parsing a specific SNMP request. An attacker could exploit this vulnerability by sending a specific SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition. This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMPv2c or earlier, the attacker must know a valid read-write or read-only SNMP community string for the affected system. To exploit this vulnerability through SNMPv3, the attacker must have valid SNMP user credentials for the affected system.			
Cisco--IOS	A vulnerability in the web services of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, Cisco Secure Firewall Threat Defense (FTD) Software, Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an unauthenticated, remote attacker (Cisco ASA and FTD Software) or authenticated, remote attacker (Cisco IOS, IOS XE, and IOS XR Software) with low user privileges to execute arbitrary code on an affected device. This vulnerability is due to improper validation of user-supplied input in HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted web service on an affected device after obtaining additional information about the system, overcoming exploit mitigations, or both. A successful exploit could allow the attacker to execute arbitrary code as root, which may lead to the complete compromise of the affected device. For more information about this vulnerability, see the Details ["#details"] section of this advisory.	2025-09-25	9	CVE-2025-20363
Cisco--IOS	A vulnerability in the implementation of the TACACS+ protocol in Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to view sensitive data or bypass authentication. This vulnerability exists because the system does not properly check whether the required TACACS+ shared secret is configured. A machine-in-the-middle attacker could exploit this vulnerability by intercepting and reading unencrypted TACACS+ messages or impersonating the TACACS+ server and falsely accepting arbitrary authentication requests. A successful exploit could allow the attacker to view sensitive information in a TACACS+ message or bypass authentication and gain access to the affected device.	2025-09-24	8.1	CVE-2025-20160
Cisco--IOS	A vulnerability in the web UI of Cisco IOS Software could allow an authenticated, remote attacker with low privileges to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper input validation. An attacker could exploit this vulnerability by sending a crafted URL in an HTTP request. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2025-09-24	7.7	CVE-2025-20327
Cisco--IOS	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software could allow the following: An authenticated, remote attacker with low privileges could cause a denial of service (DoS) condition on an affected device that is running Cisco IOS Software or Cisco IOS XE Software. To cause the DoS, the attacker must have the SNMPv2c or earlier read-only community string or valid SNMPv3 user credentials. An authenticated, remote attacker with high privileges could execute code as the root user on an affected device that is running Cisco IOS XE Software. To execute code as the root user, the attacker must have the SNMPv1 or v2c read-only community string or valid SNMPv3 user credentials and administrative or privilege 15 credentials on the affected device. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device over IPv4 or IPv6 networks. This vulnerability is due to a stack overflow condition in the SNMP subsystem of the affected software. A successful exploit could allow a low-privileged attacker to cause the affected system to reload, resulting in a DoS condition, or allow a high-privileged attacker to execute arbitrary code as the root user and obtain full control of the affected system. Note: This vulnerability affects all versions of SNMP.	2025-09-24	7.7	CVE-2025-20352
code-projects--E-Commerce Website	A vulnerability was detected in code-projects E-Commerce Website 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/admin_account_delete.php. Performing manipulation of the argument user_id results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	2025-09-22	7.3	CVE-2025-10793
code-projects--E-Commerce Website	A vulnerability was identified in code-projects E-Commerce Website 1.0. This affects an unknown function of the file /pages/admin_account_update.php. Such manipulation of the argument user_id leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	2025-09-26	7.3	CVE-2025-11036

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects--E-Commerce Website	A security flaw has been discovered in code-projects E-Commerce Website 1.0. This impacts an unknown function of the file /pages/admin_index_search.php. Performing manipulation of the argument Search results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	2025-09-26	7.3	CVE-2025-11037
code-projects--E-Commerce Website	A security vulnerability has been detected in code-projects E-Commerce Website 1.0. This affects an unknown part of the file /pages/admin_product_details.php. Such manipulation of the argument prod_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	2025-09-28	7.3	CVE-2025-11094
code-projects--Hostel Management System	A vulnerability was found in code-projects Hostel Management System 1.0. This vulnerability affects unknown code of the file /justines/admin/login.php. The manipulation of the argument email results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	2025-09-22	7.3	CVE-2025-10796
code-projects--Hostel Management System	A vulnerability was determined in code-projects Hostel Management System 1.0. This issue affects some unknown processing of the file /justines/index.php. This manipulation of the argument log_email causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-22	7.3	CVE-2025-10797
code-projects--Hostel Management System	A vulnerability was identified in code-projects Hostel Management System 1.0. Impacted is an unknown function of the file /justines/admin/mod_roomtype/index.php?view=view. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	2025-09-22	7.3	CVE-2025-10798
code-projects--Hostel Management System	A security flaw has been discovered in code-projects Hostel Management System 1.0. The affected element is an unknown function of the file /justines/admin/mod_reservation/index.php?view=view. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.	2025-09-22	7.3	CVE-2025-10799
code-projects--Hostel Management System	A flaw has been found in code-projects Hostel Management System 1.0. This affects an unknown function of the file /justines/admin/mod_comments/index.php?view=view. Executing manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	2025-09-22	7.3	CVE-2025-10811
code-projects--Hostel Management System	A vulnerability has been found in code-projects Hostel Management System 1.0. This impacts an unknown function of the file /justines/admin/mod_amenities/index.php?view=view. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2025-09-22	7.3	CVE-2025-10812
code-projects--Hostel Management System	A vulnerability was found in code-projects Hostel Management System 1.0. Affected is an unknown function of the file /justines/admin/mod_reports/index.php. The manipulation of the argument Home results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	2025-09-22	7.3	CVE-2025-10813
code-projects--Hostel Management System	A vulnerability was detected in code-projects Hostel Management System 1.0. Affected by this issue is some unknown functionality of the file /justines/admin/mod_users/index.php?view=view. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	2025-09-26	7.3	CVE-2025-11040
code-projects--Online Bidding System	A weakness has been identified in code-projects Online Bidding System 1.0. This impacts an unknown function of the file /administrator/index.php. This manipulation of the argument aduser causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	2025-09-22	7.3	CVE-2025-10791
code-projects--Online Bidding System	A vulnerability has been found in code-projects Online Bidding System 1.0. This affects an unknown part of the file /administrator/bidupdate.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-09-22	7.3	CVE-2025-10795
code-projects--Online Bidding System	A flaw has been found in code-projects Online Bidding System 1.0. Affected is an unknown function of the file /administrator/remove.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	2025-09-22	7.3	CVE-2025-10802
code-projects--Online Bidding System	A security vulnerability has been detected in code-projects Online Bidding System 1.0. This impacts an unknown function of the file /administrator/weweee.php. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	2025-09-23	7.3	CVE-2025-10841

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects--Online Bidding System	A vulnerability was detected in code-projects Online Bidding System 1.0. Affected is an unknown function of the file /administrator/wew.php. Performing manipulation of the argument ID results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used.	2025-09-23	7.3	CVE-2025-10842
code-projects--Online Bidding System	A flaw has been found in code-projects Online Bidding System 1.0. This impacts an unknown function of the file /administrator/bidlist.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	2025-09-27	7.3	CVE-2025-11066
code-projects--Project Monitoring System	A flaw has been found in code-projects Project Monitoring System 1.0. The impacted element is an unknown function of the file /login.php. This manipulation of the argument username/password causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	2025-09-27	7.3	CVE-2025-11074
code-projects--Simple Scheduling System	A flaw has been found in code-projects Simple Scheduling System 1.0. This affects an unknown part of the file /schedulingsystem/addsubject.php. This manipulation of the argument subcode causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	2025-09-28	7.3	CVE-2025-11105
code-projects--Simple Scheduling System	A vulnerability has been found in code-projects Simple Scheduling System 1.0. This vulnerability affects unknown code of the file /schedulingsystem/addfaculty.php. Such manipulation of the argument falname leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	2025-09-28	7.3	CVE-2025-11106
code-projects--Simple Scheduling System	A vulnerability was found in code-projects Simple Scheduling System 1.0. This issue affects some unknown processing of the file /schedulingsystem/addcourse.php. Performing manipulation of the argument corcode results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	2025-09-28	7.3	CVE-2025-11107
code-projects--Simple Scheduling System	A vulnerability was determined in code-projects Simple Scheduling System 1.0. Impacted is an unknown function of the file /schedulingsystem/addroom.php. Executing manipulation of the argument room can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	2025-09-28	7.3	CVE-2025-11108
code-projects--Simple Scheduling System	A vulnerability has been found in code-projects Simple Scheduling System 1.0. Affected by this issue is some unknown functionality of the file /addtime.php. The manipulation of the argument starttime/endtime leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	2025-09-28	7.3	CVE-2025-11115
code-projects--Simple Scheduling System	A vulnerability was found in code-projects Simple Scheduling System 1.0. This affects an unknown part of the file /add.home.php. The manipulation of the argument faculty results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used. Other parameters might be affected as well.	2025-09-28	7.3	CVE-2025-11116
CodeAstro--Student Grading System	A vulnerability was identified in CodeAstro Student Grading System 1.0. This issue affects some unknown processing of the file /adminLogin.php. Such manipulation of the argument staffId leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	2025-09-28	7.3	CVE-2025-11118
ConveyThis--Language Translate Widget for WordPress ConveyThis	Deserialization of Untrusted Data vulnerability in ConveyThis Language Translate Widget for WordPress - ConveyThis allows Object Injection. This issue affects Language Translate Widget for WordPress - ConveyThis: from n/a through 264.	2025-09-22	7.2	CVE-2025-57919
cubecart--v6	CubeCart is an ecommerce software solution. Prior to version 6.5.11, there is an absence of automatic session expiration following a user's password change. This oversight poses a security risk, as if a user forgets to log out from a location where they accessed their account, an unauthorized user can maintain access even after the password has been changed. Due to this bug, if an account has already been compromised, the legitimate user has no way to revoke the attacker's access. The malicious actor retains full access to the account until their session naturally expires. This means the account remains insecure even after the password has been changed. This issue has been patched in version 6.5.11.	2025-09-22	7.1	CVE-2025-59335
D-Link--DCS-935L	A vulnerability was found in D-Link DCS-935L up to 1.13.01. The impacted element is the function sub_402280 of the file /HNAP1/. The manipulation of the argument HNAP_AUTH/SOAPAction results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-09-22	8.8	CVE-2025-10779

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
D-Link--DIR-513	A security vulnerability has been detected in D-Link DIR-513 A1FW110. Affected is an unknown function of the file /goform/formWPS. Such manipulation of the argument webpage leads to buffer overflow. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-09-22	8.8	CVE-2025-10792
Dell--BSAFE Micro Edition Suite	Dell BSAFE Micro Edition Suite, versions prior to 5.0.2.3 contain an Out-of-bounds Write vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to denial of service.	2025-09-25	7.5	CVE-2024-48014
Dell--Wireless 5932e	Dell Wireless 5932e and Qualcomm Snapdragon X62 Firmware and GNSS/GPS Driver, versions prior to 3.2.0.22 contain an Unquoted Search Path or Element vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code Execution.	2025-09-25	7.8	CVE-2025-43993
Delta Electronics--CNCSoft-G2	Delta Electronics CNCSoft-G2 lacks proper validation of the user-supplied file. If a user opens a malicious file, an attacker can leverage this vulnerability to execute code in the context of the current process.	2025-09-24	7.8	CVE-2025-58317
Delta Electronics--CNCSoft-G2	Delta Electronics CNCSoft-G2 lacks proper validation of the user-supplied file. If a user opens a malicious file, an attacker can leverage this vulnerability to execute code in the context of the current process.	2025-09-24	7.8	CVE-2025-58319
dnnsoftware--Dnn.Platform	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.1.0, the Prompt module allows execution of commands that can return raw HTML. Malicious input, even if sanitized for display elsewhere, can be executed when processed through certain commands, leading to potential script execution (XSS). This issue has been patched in version 10.1.0.	2025-09-23	9.1	CVE-2025-59545
e4jvikwp--VikRestaurants Table Reservations and Take-Away	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikRestaurants Table Reservations and Take-Away allows Reflected XSS. This issue affects VikRestaurants Table Reservations and Take-Away: from n/a through 1.4.	2025-09-22	7.1	CVE-2025-57968
EdwardBock--Grid	Cross-Site Request Forgery (CSRF) vulnerability in EdwardBock Grid allows Stored XSS. This issue affects Grid: from n/a through 2.3.1.	2025-09-22	7.1	CVE-2025-58657
ERA404--LinkedInclude	Cross-Site Request Forgery (CSRF) vulnerability in ERA404 LinkedInclude allows Stored XSS. This issue affects LinkedInclude: from n/a through 3.0.4.	2025-09-22	7.1	CVE-2025-57918
eteubert--Podlove Podcast Publisher	The Podlove Podcast Publisher plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'move_as_original_file' function in all versions up to, and including, 4.2.6. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	2025-09-23	9.8	CVE-2025-10147
extendyourweb--HORIZONTAL SLIDER	Cross-Site Request Forgery (CSRF) vulnerability in extendyourweb HORIZONTAL SLIDER allows Stored XSS. This issue affects HORIZONTAL SLIDER: from n/a through 2.4.	2025-09-22	7.1	CVE-2025-58676
FlagForgeCTF--flagForge	Flag Forge is a Capture The Flag (CTF) platform. In versions from 2.2.0 to before 2.3.1, the FlagForge web application improperly handles session invalidation. Authenticated users can continue to access protected endpoints, such as /api/profile, even after logging out. CSRF tokens are also still valid post-logout, which can allow unauthorized actions. This issue has been patched in version 2.3.1.	2025-09-25	9.8	CVE-2025-59841
FlagForgeCTF--flagForge	Flag Forge is a Capture The Flag (CTF) platform. From versions 2.0.0 to before 2.3.1, the /api/resources endpoint previously allowed POST and DELETE requests without proper authentication or authorization. This could have enabled unauthorized users to create, modify, or delete resources on the platform. The issue has been fixed in FlagForge version 2.3.1.	2025-09-27	8.6	CVE-2025-59932
FlagForgeCTF--flagForge	Flag Forge is a Capture The Flag (CTF) platform. In version 2.1.0, non-admin users can create arbitrary challenges, potentially introducing malicious, incorrect, or misleading content. This issue has been patched in version 2.2.0.	2025-09-23	7.6	CVE-2025-59826
FlagForgeCTF--flagForge	Flag Forge is a Capture The Flag (CTF) platform. In versions from 2.1.0 to before 2.3.0, the API endpoint GET /api/problems/:id returns challenge hints in plaintext within the question object, regardless of whether the user has unlocked them via point deduction. Users can view all hints for free, undermining the business logic of the platform and reducing the integrity of the challenge system. This issue has been patched in version 2.3.0.	2025-09-24	7.5	CVE-2025-59833
FlowiseAI--Flowise	Flowise is a drag & drop user interface to build a customized large language model flow. In version 3.0.5, Flowise is vulnerable to remote code execution. The CustomMCP node allows users to input configuration settings for connecting to an external MCP server. This node parses the user-provided mcpServerConfig string to build the MCP server configuration. However, during this process, it executes JavaScript code without any security validation. Specifically, inside the	2025-09-22	10	CVE-2025-59528

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	convertToValidJSONString function, user input is directly passed to the Function() constructor, which evaluates and executes the input as JavaScript code. Since this runs with full Node.js runtime privileges, it can access dangerous modules such as child_process and fs. This issue has been patched in version 3.0.6.			
FlowiseAI--Flowise	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to August 2025 Cloud-Hosted Flowise, an authenticated vulnerability in Flowise Cloud allows any user on the free tier to access sensitive environment variables from other tenants via the Custom JavaScript Function node. This includes secrets such as OpenAI API keys, AWS credentials, Supabase tokens, and Google Cloud secrets - resulting in a full cross-tenant data exposure. This issue has been patched in the August 2025 Cloud-Hosted Flowise.	2025-09-22	9.6	CVE-2025-59434
FlowiseAI--Flowise	Flowise is a drag & drop user interface to build a customized large language model flow. In version 3.0.5, a Server-Side Request Forgery (SSRF) vulnerability was discovered in the /api/v1/fetch-links endpoint of the Flowise application. This vulnerability allows an attacker to use the Flowise server as a proxy to access internal network web services and explore their link structures. This issue has been patched in version 3.0.6.	2025-09-22	7.5	CVE-2025-59527
flytedesk--Flytedesk Digital	Cross-Site Request Forgery (CSRF) vulnerability in flytedesk Flytedesk Digital allows Stored XSS. This issue affects Flytedesk Digital: from n/a through 20181101.	2025-09-26	7.1	CVE-2025-60172
formbricks--formbricks	Formbricks is an open source qualtrics alternative. Prior to version 4.0.1, Formbricks is missing JWT signature verification. This vulnerability stems from a token validation routine that only decodes JWTs (jwt.decode) without verifying their signatures. Both the email verification token login path and the password reset server action use the same validator, which does not check the token's signature, expiration, issuer, or audience. If an attacker learns the victim's actual user.id, they can craft an arbitrary JWT with an alg: "none" header and use it to authenticate and reset the victim's password. This issue has been patched in version 4.0.1.	2025-09-26	9.4	CVE-2025-59934
FrontFin--mesh-web-sdk	Mesh Connect JS SDK contains JS libraries for integrating with Mesh Connect. Prior to version 3.3.2, the lack of sanitization of URLs protocols in the createLink.openLink function enables the execution of arbitrary JavaScript code within the context of the parent page. This is technically indistinguishable from a real page at the rendering level and allows access to the parent page DOM, storage, session, and cookies. If the attacker can specify customIframeId, they can hijack the source of existing iframes. This issue has been patched in version 3.3.2.	2025-09-22	8.2	CVE-2025-59430
gamerz--WP-DownloadManager	The WP-DownloadManager plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the download-add.php file in all versions up to, and including, 1.68.11. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2025-09-26	7.2	CVE-2025-10747
geyang--ml-logger	A vulnerability was identified in geyang ml-logger up to acf255bade5be6ad88d90735c8367b28cbe3a743. Affected by this vulnerability is the function log_handler of the file ml_logger/server.py. Such manipulation of the argument File leads to path traversal. It is possible to launch the attack remotely. The exploit is publicly available and might be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	2025-09-25	7.3	CVE-2025-10951
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 14.10 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1 that could allow an attacker to inject malicious content that may lead to account takeover.	2025-09-26	8.7	CVE-2025-9642
GitLab--GitLab	An issue was discovered in GitLab CE/EE affecting all versions before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1 that allows unauthenticated users to cause a Denial of Service (DoS) condition while uploading specifically crafted large JSON files.	2025-09-26	7.5	CVE-2025-10858
GitLab--GitLab	Denial of Service issue in GraphQL endpoints in Gitlab EE/CE affecting all versions from 11.10 prior to 18.2.7, 18.3 prior to 18.3.3, and 18.4 prior to 18.4.1 allows unauthenticated users to potentially bypass query complexity limits leading to resource exhaustion and service disruption.	2025-09-27	7.5	CVE-2025-8014
gopiplus@hotmail.com--Wp tabber widget	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in gopiplus@hotmail.com Wp tabber widget allows SQL Injection. This issue affects Wp tabber widget: from n/a through 4.0.	2025-09-22	8.5	CVE-2025-53468
H3C--Magic B3	A vulnerability was identified in H3C Magic B3 up to 100R002. This affects the function AddMacList of the file /goform/aspForm. The manipulation of the argument param leads to buffer overflow. The attack can be initiated remotely.	2025-09-25	8.8	CVE-2025-10942

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.			
HaruTheme--WooCommerce Designer Pro	Unrestricted Upload of File with Dangerous Type vulnerability in HaruTheme WooCommerce Designer Pro allows Upload a Web Shell to a Web Server. This issue affects WooCommerce Designer Pro: from n/a through 1.9.24.	2025-09-26	10	CVE-2025-60219
hashthemes--Easy Elementor Addons	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in hashthemes Easy Elementor Addons allows PHP Local File Inclusion. This issue affects Easy Elementor Addons: from n/a through 2.2.8.	2025-09-22	7.5	CVE-2025-58973
horilla-opensource--horilla	Horilla is a free and open source Human Resource Management System (HRMS). Prior to version 1.4.0, there is a stored XSS vulnerability in the ticket comment editor. A low-privilege authenticated user could run arbitrary JavaScript in an admin's browser, exfiltrate the admin's cookies/CSRF token, and hijack their session. This issue has been patched in version 1.4.0.	2025-09-25	9.9	CVE-2025-59832
horilla-opensource--horilla	Horilla is a free and open source Human Resource Management System (HRMS). An authenticated Remote Code Execution (RCE) vulnerability exists in Horilla 1.3.0 due to the unsafe use of Python's eval() function on a user-controlled query parameter in the project_bulk_archive view. This allows privileged users (e.g., administrators) to execute arbitrary system commands on the server. While having Django's DEBUG=True makes exploitation visibly easier by returning command output in the HTTP response, this is not required. The vulnerability can still be exploited in DEBUG=False mode by using blind payloads such as a reverse shell, leading to full remote code execution. This issue has been patched in version 1.3.1.	2025-09-24	7.2	CVE-2025-48868
horilla-opensource--horilla	Horilla is a free and open source Human Resource Management System (HRMS). Unauthenticated users can access uploaded resume files in Horilla 1.3.0 by directly guessing or predicting file URLs. These files are stored in a publicly accessible directory, allowing attackers to retrieve sensitive candidate information without authentication. At time of publication there is no known patch.	2025-09-24	7.5	CVE-2025-48869
IBM--Aspera HTTP Gateway	IBM Aspera HTTP Gateway 2.0.0 through 2.3.1 stores sensitive information in clear text in easily obtainable files which can be read by an unauthenticated user.	2025-09-26	7.5	CVE-2025-36274
IBM--webMethods Integration	IBM webMethods Integration 10.15 and 11.1 could allow an authenticated user with required execute Services to execute commands on the system due to the improper validation of format string strings passed as an argument from an external source.	2025-09-22	7.5	CVE-2025-36202
immonex--immonex Kickstart Team	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in immonex immonex Kickstart Team allows PHP Local File Inclusion. This issue affects immonex Kickstart Team: from n/a through 1.6.9.	2025-09-22	7.5	CVE-2025-57925
Iron Mountain Archiving Services Inc.--enVision	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Iron Mountain Archiving Services Inc. EnVision allows Command Injection.This issue affects enVision: before 250563.	2025-09-23	10	CVE-2025-9588
itsourcecode--Online Discussion Forum	A weakness has been identified in itsourcecode Online Discussion Forum 1.0. The impacted element is an unknown function of the file /index.php. Executing manipulation of the argument email/password can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.	2025-09-22	7.3	CVE-2025-10800
itsourcecode--Open Source Job Portal	A vulnerability was identified in itsourcecode Open Source Job Portal 1.0. This affects an unknown function of the file /jobportal/admin/login.php. Such manipulation of the argument user_email leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	2025-09-23	7.3	CVE-2025-10834
itsourcecode--Open Source Job Portal	A security flaw has been discovered in itsourcecode Open Source Job Portal 1.0. This impacts an unknown function of the file /jobportal/admin/company/index.php?view=edit. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	2025-09-28	7.3	CVE-2025-11101
JackieDYH--Resume-management-system	A flaw has been found in JackieDYH Resume-management-system up to fb6b857d852dd796e748ce30c606fe5e61c18273. Affected by this issue is some unknown functionality of the file /admin/show.php. This manipulation of the argument userid causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	7.3	CVE-2025-10973
javothemes--Javo Core	Cross-Site Request Forgery (CSRF) vulnerability in javothemes Javo Core allows Authentication Bypass. This issue affects Javo Core: from n/a through 3.0.0.266.	2025-09-26	8.8	CVE-2025-60111

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Jinher--OA	A security flaw has been discovered in Jinher OA 2.0. This affects an unknown part of the file /c6/Jhsoft.Web.module/ToolBar/GetWordFileName.aspx/?text=GetUrl&style=add of the component XML Handler. Performing manipulation results in xml external entity reference. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	2025-09-22	7.3	CVE-2025-10816
kidaze--CourseSelectionSystem	A flaw has been found in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. This issue affects some unknown processing of the file /Profilers/PriProfile/COUNT3s6.php. Executing manipulation of the argument CPU can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed.	2025-09-26	7.3	CVE-2025-11032
kidaze--CourseSelectionSystem	A vulnerability has been found in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. Impacted is an unknown function of the file /Profilers/PriProfile/COUNT3s7.php. The manipulation of the argument cbe leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	2025-09-26	7.3	CVE-2025-11033
kidaze--CourseSelectionSystem	A security flaw has been discovered in kidaze CourseSelectionSystem 1.0/5.php. The impacted element is an unknown function of the file /Profilers/PriProfile/COUNT3s5.php. Performing manipulation of the argument csslc results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	2025-09-27	7.3	CVE-2025-11052
kidaze--CourseSelectionSystem	A vulnerability was determined in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. This impacts an unknown function of the file /Profilers/PriProfile/COUNT3s4.php. Executing manipulation of the argument cbranch can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available.	2025-09-28	7.3	CVE-2025-11089
LabRedesCefetRJ--WeGIA	WeGIA is a Web manager for charitable institutions. Prior to version 3.5.0, WeGIA is vulnerable to SQL Injection attacks in the control.php endpoint with the following parameters: nomeClasse=ProdutoControle&metodo=excluir&id_produto=[malicious command]. It is necessary to apply prepared statements methods, sanitization, and validations on theid_produto parameter. This issue has been patched in version 3.5.0.	2025-09-27	8.8	CVE-2025-59939
LambertGroup--AllInOne - Banner Rotator	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup AllInOne - Banner Rotator allows SQL Injection. This issue affects AllInOne - Banner Rotator: from n/a through 3.8.	2025-09-26	8.5	CVE-2025-60110
LambertGroup--LambertGroup - AllInOne - Banner with Playlist	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup LambertGroup - AllInOne - Banner with Playlist allows Blind SQL Injection. This issue affects LambertGroup - AllInOne - Banner with Playlist: from n/a through 3.8.	2025-09-26	8.5	CVE-2025-60107
LambertGroup--LambertGroup - AllInOne - Banner with Thumbnails	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup LambertGroup - AllInOne - Banner with Thumbnails allows Blind SQL Injection. This issue affects LambertGroup - AllInOne - Banner with Thumbnails: from n/a through 3.8.	2025-09-26	8.5	CVE-2025-60108
LambertGroup--LambertGroup - AllInOne - Content Slider	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LambertGroup LambertGroup - AllInOne - Content Slider allows Blind SQL Injection. This issue affects LambertGroup - AllInOne - Content Slider: from n/a through 3.8.	2025-09-26	8.5	CVE-2025-60109
loopus--WP Attractive Donations System	Cross-Site Request Forgery (CSRF) vulnerability in loopus WP Attractive Donations System allows Stored XSS. This issue affects WP Attractive Donations System: from n/a through n/a.	2025-09-22	7.1	CVE-2025-58956
Maciej Bis--Permalink Manager Lite	Insertion of Sensitive Information Into Sent Data vulnerability in Maciej Bis Permalink Manager Lite allows Retrieve Embedded Sensitive Data. This issue affects Permalink Manager Lite: from n/a through 2.5.1.3.	2025-09-26	7.5	CVE-2025-59010
Magnetism Studios--Endurance	A flaw has been found in Magnetism Studios Endurance up to 3.3.0 on macOS. This affects the function loadModuleNamed:WithReply of the file /Applications/Endurance.app/Contents/Library/LaunchServices/com.MagnetismStudios.endurance.helper of the component NSXPC Interface. Executing	2025-09-24	8.4	CVE-2025-10906

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	manipulation can lead to missing authentication. The attack needs to be launched locally. The exploit has been published and may be used.			
Metagauss--ProfileGrid	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Metagauss ProfileGrid allows Reflected XSS. This issue affects ProfileGrid : from n/a through 5.9.5.7.	2025-09-26	7.1	CVE-2025-4957
Microsoft--Microsoft Edge (Chromium-based)	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2025-09-24	7.6	CVE-2025-59251
Microsoft--OmniParser	Binding to an unrestricted ip address in GitHub allows an unauthorized attacker to execute code over a network.	2025-09-24	7.3	CVE-2025-55322
MikroTik--RouterOS	A vulnerability has been found in MikroTik RouterOS 7. This affects the function parse_json_element of the file /rest/ip/address/print of the component libjson.so. The manipulation leads to buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	8.8	CVE-2025-10948
MooMoo--Product Options and Price Calculation Formulas for WooCommerce Uni CPO (Premium)	The Product Options and Price Calculation Formulas for WooCommerce - Uni CPO (Premium) plugin for WordPress is vulnerable to arbitrary file uploads due to misconfigured file type validation in the 'uni_cpo_upload_file' function in all versions up to, and including, 4.9.54. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	2025-09-23	9.8	CVE-2025-10412
morganrichards--Auction Feed	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in morganrichards Auction Feed allows Stored XSS. This issue affects Auction Feed: from n/a through 1.1.3.	2025-09-22	7.1	CVE-2025-58671
MuFen-mker--PHP-Usermm	A vulnerability was detected in MuFen-mker PHP-Usermm up to 37f2d24e51b04346dfc565b93fc2fc6b37bdaea9. This affects an unknown part of the file /chkuser.php. Performing manipulation of the argument Username results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	7.3	CVE-2025-10967
nasa--CryptoLib	CryptoLib provides a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Prior to version 1.4.2, there is a command Injection vulnerability in initialize_kerberos_keytab_file_login(). The vulnerability exists because the code directly interpolates user-controlled input into a shell command and executes it via system() without any sanitization or validation. This issue has been patched in version 1.4.2.	2025-09-23	7.3	CVE-2025-59534
Netcad Software Inc.--Netigma	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Netcad Software Inc. Netigma allows Stored XSS.This issue affects Netigma: from 6.3.3 before 6.3.5 V8.	2025-09-23	8.9	CVE-2025-9798
NewsMAN--NewsmanApp	Cross-Site Request Forgery (CSRF) vulnerability in NewsMAN NewsmanApp allows Stored XSS. This issue affects NewsmanApp: from n/a through 2.7.7.	2025-09-26	7.1	CVE-2025-60164
NIX Solutions Ltd--NIX Anti-Spam Light	Cross-Site Request Forgery (CSRF) vulnerability in NIX Solutions Ltd NIX Anti-Spam Light allows Cross Site Request Forgery. This issue affects NIX Anti-Spam Light: from n/a through 0.0.4.	2025-09-22	7.1	CVE-2025-58270
NVIDIA--Megatron-LM	NVIDIA Megatron-LM for all platforms contains a vulnerability in the pretrain_gpt script, where malicious data created by an attacker may cause a code injection issue. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, information disclosure, and data tampering.	2025-09-24	7.8	CVE-2025-23348
NVIDIA--Megatron-LM	NVIDIA Megatron-LM for all platforms contains a vulnerability in the tasks/orqa/unsupervised/nq.py component, where an attacker may cause a code injection. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, information disclosure, and data tampering.	2025-09-24	7.8	CVE-2025-23349
NVIDIA--Megatron-LM	NVIDIA Megatron-LM for all platforms contains a vulnerability in the msdp preprocessing script where malicious data created by an attacker may cause an injection. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, Information disclosure, and data tampering.	2025-09-24	7.8	CVE-2025-23353
NVIDIA--Megatron-LM	NVIDIA Megatron-LM for all platforms contains a vulnerability in the ensemble_classifer script where malicious data created by an attacker may cause an injection. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, Information disclosure, and data tampering.	2025-09-24	7.8	CVE-2025-23354

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pebas--CouponXxL	Cross-Site Request Forgery (CSRF) vulnerability in pebas CouponXxL allows Privilege Escalation. This issue affects CouponXxL: from n/a through 4.5.0.	2025-09-22	8.8	CVE-2025-58013
PenciDesign--Soledad	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in PenciDesign Soledad allows PHP Local File Inclusion. This issue affects Soledad: from n/a through 8.6.8.	2025-09-22	7.5	CVE-2025-59588
PHPGurukul--Small CRM	A weakness has been identified in PHPGurukul Small CRM 4.0. This affects an unknown function of the file /forgot-password.php. Executing manipulation of the argument email can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.	2025-09-27	7.3	CVE-2025-11053
PluginOps--Testimonial Slider	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in PluginOps Testimonial Slider allows PHP Local File Inclusion. This issue affects Testimonial Slider: from n/a through 3.5.8.6.	2025-09-26	8.8	CVE-2025-60126
Pluginwale--Easy Pricing Table WP	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Pluginwale Easy Pricing Table WP allows PHP Local File Inclusion. This issue affects Easy Pricing Table WP: from n/a through 1.1.3.	2025-09-22	7.5	CVE-2025-53450
Potenzaglobalsolutions--PGS Core	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Potenzaglobalsolutions PGS Core allows SQL Injection. This issue affects PGS Core: from n/a through 5.9.0.	2025-09-26	8.5	CVE-2025-60118
PressPage Entertainment Inc--Mavis HTTPS to HTTP Redirection	Cross-Site Request Forgery (CSRF) vulnerability in PressPage Entertainment Inc Mavis HTTPS to HTTP Redirection allows Stored XSS. This issue affects Mavis HTTPS to HTTP Redirection: from n/a through 1.4.3.	2025-09-22	7.1	CVE-2025-58261
Projectworlds--Online Shopping System	A vulnerability was identified in Projectworlds Online Shopping System 1.0. This affects an unknown part of the file /store/cart_add.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	2025-09-27	7.3	CVE-2025-11070
PROLIZ Computer Software Hardware Service Trade Ltd. Co.--OBS (Student Affairs Information System)	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PROLIZ Computer Software Hardware Service Trade Ltd. Co. OBS (Student Affairs Information System) allows Stored XSS.This issue affects OBS (Student Affairs Information System): before v25.0401.	2025-09-25	8.9	CVE-2025-10467
ptibogxiv--Doliconnect	Cross-Site Request Forgery (CSRF) vulnerability in ptibogxiv Doliconnect allows Stored XSS. This issue affects Doliconnect: from n/a through 9.5.7.	2025-09-22	7.1	CVE-2025-58690
puravida1976--ShrinkTheWeb (STW) Website Previews	Cross-Site Request Forgery (CSRF) vulnerability in puravida1976 ShrinkTheWeb (STW) Website Previews allows Stored XSS. This issue affects ShrinkTheWeb (STW) Website Previews: from n/a through 2.8.5.	2025-09-22	7.1	CVE-2025-58677
purethemes--WorkScout-Core	Cross-Site Request Forgery (CSRF) vulnerability in purethemes WorkScout-Core allows Cross Site Request Forgery. This issue affects WorkScout-Core: from n/a through n/a.	2025-09-22	8.8	CVE-2025-59572
Python - - txtai arbitrary file write ver. 0 thru 9.0	The txtai framework allows the loading of compressed tar files as embedding indices. While the validate function is intended to prevent path traversal vulnerabilities by ensuring safe filenames, it does not account for symbolic links within the tar file. An attacker is able to write a file anywhere in the filesystem when txtai is used to load untrusted embedding indices	2025-09-22	8.1	CVE-2025-10854
quadlayers--Perfect Brands for WooCommerce	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in quadlayers Perfect Brands for WooCommerce allows SQL Injection. This issue affects Perfect Brands for WooCommerce: from n/a through 3.6.0.	2025-09-22	8.5	CVE-2025-58686
Qualcomm, Inc.--Snapdragon	Memory corruption when the UE receives an RTP packet from the network, during the reassembly of NALUs.	2025-09-24	9.8	CVE-2025-21483
Qualcomm, Inc.--Snapdragon	Memory corruption while selecting the PLMN from SOR failed list.	2025-09-24	9.8	CVE-2025-27034
Qualcomm, Inc.--Snapdragon	Information disclosure when UE receives the RTP packet from the network, while decoding and reassembling the fragments from RTP packet.	2025-09-24	8.2	CVE-2025-21484
Qualcomm, Inc.--Snapdragon	Information disclosure while decoding RTP packet received by UE from the network, when payload length mentioned is greater than the available buffer length.	2025-09-24	8.2	CVE-2025-21487
Qualcomm, Inc.--Snapdragon	Information disclosure while decoding this RTP packet headers received by UE from the network when the padding bit is set.	2025-09-24	8.2	CVE-2025-21488
Qualcomm, Inc.--Snapdragon	Memory corruption when passing parameters to the Trusted Virtual Machine during the handshake.	2025-09-24	7.8	CVE-2025-21476

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Qualcomm, Inc.--Snapdragon	Memory corruption while performing private key encryption in trusted application.	2025-09-24	7.8	CVE-2025-21481
Qualcomm, Inc.--Snapdragon	Cryptographic issue while performing RSA PKCS padding decoding.	2025-09-24	7.1	CVE-2025-21482
Qualcomm, Inc.--Snapdragon	memory corruption while loading a PIL authenticated VM, when authenticated VM image is loaded without maintaining cache coherency.	2025-09-24	7.8	CVE-2025-27032
Qualcomm, Inc.--Snapdragon	Memory corruption while processing config_dev IOCTL when camera kernel driver drops its reference to CPU buffers.	2025-09-24	7.8	CVE-2025-27037
Qualcomm, Inc.--Snapdragon	Memory corruption while processing message in guest VM.	2025-09-24	7.8	CVE-2025-27077
Qualcomm, Inc.--Snapdragon	Memory corruption while processing data sent by FE driver.	2025-09-24	7.8	CVE-2025-47314
Qualcomm, Inc.--Snapdragon	Memory corruption while handling repeated memory unmap requests from guest VM.	2025-09-24	7.8	CVE-2025-47315
Qualcomm, Inc.--Snapdragon	Memory corruption due to double free when multiple threads race to set the timestamp store.	2025-09-24	7.8	CVE-2025-47316
Qualcomm, Inc.--Snapdragon	Memory corruption due to global buffer overflow when a test command uses an invalid payload type.	2025-09-24	7.8	CVE-2025-47317
Qualcomm, Inc.--Snapdragon	Transient DOS while parsing the EPTM test control message to get the test pattern.	2025-09-24	7.5	CVE-2025-47318
Qualcomm, Inc.--Snapdragon	Transient DOS while handling command data during power control processing.	2025-09-24	7.5	CVE-2025-47326
Qualcomm, Inc.--Snapdragon	Memory corruption while encoding the image data.	2025-09-24	7.8	CVE-2025-47327
Qualcomm, Inc.--Snapdragon	Transient DOS while processing power control requests with invalid antenna or stream values.	2025-09-24	7.5	CVE-2025-47328
Qualcomm, Inc.--Snapdragon	Memory corruption while handling invalid inputs in application info setup.	2025-09-24	7.8	CVE-2025-47329
rack--rack	Rack is a modular Ruby web server interface. Prior to version 2.2.18, Rack::QueryParser enforces its params_limit only for parameters separated by &, while still splitting on both & and ;. As a result, attackers could use ; separators to bypass the parameter count limit and submit more parameters than intended. Applications or middleware that directly invoke Rack::QueryParser with its default configuration (no explicit delimiter) could be exposed to increased CPU and memory consumption. This can be abused as a limited denial-of-service vector. This issue has been patched in version 2.2.18.	2025-09-25	7.5	CVE-2025-59830
raoinfotech--GSheets Connector	Deserialization of Untrusted Data vulnerability in raoinfotech GSheets Connector allows Object Injection. This issue affects GSheets Connector: from n/a through 1.1.1.	2025-09-22	7.2	CVE-2025-53465
Red Hat --Ver. 20.12 and 21.8	Malicious code was inserted into the Nx (build system) package and several related plugins. The tampered package was published to the npm software registry, via a supply-chain attack. Affected versions contain code that scans the file system, collects credentials, and posts them to GitHub as a repo under user's accounts.	2025-09-24	9.6	CVE-2025-10894
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in Libtiff. This vulnerability is a "write-what-where" condition, triggered when the library processes a specially crafted TIFF image file. By providing an abnormally large image height value in the file's metadata, an attacker can trick the library into writing attacker-controlled color data to an arbitrary memory location. This memory corruption can be exploited to cause a denial of service (application crash) or to achieve arbitrary code execution with the permissions of the user.	2025-09-23	8.8	CVE-2025-9900
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in the cookie date handling logic of the libsoup HTTP library, widely used by GNOME and other applications for web communication. When processing cookies with specially crafted expiration dates, the library may perform an out-of-bounds memory read. This flaw could result in unintended disclosure of memory contents, potentially exposing sensitive information from the process using libsoup.	2025-09-26	7.5	CVE-2025-11021
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in the Lightspeed history service. Insufficient access controls allow a local, unprivileged user to access and manipulate the chat history of another user on the same system. By abusing inter-process communication calls to the history service, an attacker can view, delete, or inject arbitrary history entries, including misleading or malicious commands. This can be used to deceive another user into executing harmful actions, posing a risk of privilege misuse or unauthorized command execution through social engineering.	2025-09-22	7.7	CVE-2025-5962
Reservation--Online Hotel	A flaw has been found in Reservation Online Hotel Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file	2025-09-23	7.3	CVE-2025-10843

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Reservation System	/reservation/paypalpayout.php. Executing manipulation of the argument confirm can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.			
Saysis Computer Systems Trade Ltd. Co.--Saysis Web Portal	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Saysis Computer Systems Trade Ltd. Co. Saysis Web Portal allows Path Traversal.This issue affects Saysis Web Portal: from 3.1.9 & 3.2.0 before 3.2.1.	2025-09-25	8.6	CVE-2025-10449
scriptsbundle--Nokri	Cross-Site Request Forgery (CSRF) vulnerability in scriptsbundle Nokri allows Cross Site Request Forgery. This issue affects Nokri: from n/a through 1.6.4.	2025-09-22	7.1	CVE-2025-58259
SeaTheme--BM Content Builder	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in SeaTheme BM Content Builder allows Path Traversal. This issue affects BM Content Builder: from n/a through n/a.	2025-09-26	7.7	CVE-2025-59002
Shankaranand Maurya--WP Content Protection	Cross-Site Request Forgery (CSRF) vulnerability in Shankaranand Maurya WP Content Protection allows Stored XSS. This issue affects WP Content Protection: from n/a through 1.3.	2025-09-22	7.1	CVE-2025-58670
shinetheme--Traveler	Missing Authorization vulnerability in shinetheme Traveler allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Traveler: from n/a through n/a.	2025-09-26	7.5	CVE-2025-59011
shinetheme--Traveler	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in shinetheme Traveler allows Reflected XSS. This issue affects Traveler: from n/a through n/a.	2025-09-26	7.1	CVE-2025-59012
SolarWinds--Web Help Desk	SolarWinds Web Help Desk was found to be susceptible to an unauthenticated AjaxProxy deserialization remote code execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. This vulnerability is a patch bypass of CVE-2024-28988, which in turn is a patch bypass of CVE-2024-28986.	2025-09-23	9.8	CVE-2025-26399
SourceCodester--Online Hotel Reservation System	A vulnerability was determined in SourceCodester Online Hotel Reservation System 1.0. The affected element is an unknown function of the file deleteroominventory.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-22	7.3	CVE-2025-10788
SourceCodester--Online Hotel Reservation System	A vulnerability was identified in SourceCodester Online Hotel Reservation System 1.0. The impacted element is an unknown function of the file deleteslide.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	2025-09-22	7.3	CVE-2025-10789
SourceCodester--Online Hotel Reservation System	A vulnerability was detected in SourceCodester Online Hotel Reservation System 1.0. Affected is an unknown function of the file /admin/updateaddress.php. The manipulation of the argument address results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	2025-09-27	7.3	CVE-2025-11055
SourceCodester--Pet Grooming Management Software	A security vulnerability has been detected in SourceCodester Pet Grooming Management Software 1.0. This affects an unknown function of the file /admin/edit_tax.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	2025-09-22	7.3	CVE-2025-10801
SourceCodester--Pet Grooming Management Software	A vulnerability was found in SourceCodester Pet Grooming Management Software 1.0. The affected element is an unknown function of the file /admin/fetch_product_details.php. The manipulation of the argument barcode results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	2025-09-23	7.3	CVE-2025-10832
SourceCodester--Pet Grooming Management Software	A weakness has been identified in SourceCodester Pet Grooming Management Software 1.0. Affected is an unknown function of the file /admin/print1.php. Executing manipulation of the argument ID can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.	2025-09-23	7.3	CVE-2025-10836
SourceCodester--Pet Grooming Management Software	A vulnerability has been found in SourceCodester Pet Grooming Management Software 1.0. Affected by this issue is some unknown functionality of the file /admin/print_inv.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	2025-09-27	7.3	CVE-2025-11057
srmorete--adb-mcp	ADB MCP Server is a MCP (Model Context Protocol) server for interacting with Android devices through ADB. In versions 0.1.0 and prior, the MCP Server is written in a way that is vulnerable to command injection vulnerability attacks as part of some of its MCP Server tool definition and implementation. This issue has been patched via commit 041729c.	2025-09-25	9.8	CVE-2025-59834

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
StarCitizenWiki--mediawiki-extensions-EmbedVideo	The EmbedVideo Extension is a MediaWiki extension which adds a parser function called #ev and various parser tags for embedding video clips from various video sharing services. In versions 4.0.0 and prior, the EmbedVideo extension allows adding arbitrary attributes to an HTML element, allowing for stored XSS through wikitext. This issue has been patched via commit 4e075d3.	2025-09-25	8.6	CVE-2025-59839
Syslifters--sysreptor	SysReptor is a fully customizable pentest reporting platform. In versions from 2024.74 to before 2025.83, authenticated and unprivileged (non-admin) users can assign the is_project_admin permission to their own user. This allows users to read, modify and delete pentesting projects they are not members of and are therefore not supposed to access. This issue has been patched in version 2025.83.	2025-09-27	8.1	CVE-2025-59945
TalentSys Consulting Information Technology Industry Inc.--Inka.Net	Unrestricted Upload of File with Dangerous Type vulnerability in TalentSys Consulting Information Technology Industry Inc. Inka.Net allows Command Injection.This issue affects Inka.Net: before 6.7.1.	2025-09-23	10	CVE-2025-9846
Taraprasad Swain--HTACCESS IP Blocker	Cross-Site Request Forgery (CSRF) vulnerability in Taraprasad Swain HTACCESS IP Blocker allows Stored XSS. This issue affects HTACCESS IP Blocker: from n/a through 1.0.	2025-09-26	7.1	CVE-2025-60170
Techspawn--MultiLoca - WooCommerce Multi Locations Inventory Management	The MultiLoca - WooCommerce Multi Locations Inventory Management plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the 'wcmlim_settings_ajax_handler' function in all versions up to, and including, 4.2.8. This makes it possible for unauthenticated attackers to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	2025-09-24	9.8	CVE-2025-9054
Tencent--WeKnora	A security flaw has been discovered in Tencent WeKnora 0.1.0. This impacts the function testEmbeddingModel of the file /api/v1/initialization/embedding/test. The manipulation of the argument baseUrl results in server-side request forgery. The attack can be launched remotely. The exploit has been released to the public and may be exploited. It is advisable to upgrade the affected component. The vendor responds: "We have confirmed that the issue mentioned in the report does not exist in the latest releases".	2025-09-26	7.3	CVE-2025-11046
Tenda--AC18	A vulnerability was detected in Tenda AC18 15.03.05.19. This affects an unknown function of the file /goform/WizardHandle. The manipulation of the argument WANT/mtuvalue results in stack-based buffer overflow. The attack can be launched remotely. The exploit is now public and may be used.	2025-09-28	8.8	CVE-2025-11122
Tenda--AC18	A flaw has been found in Tenda AC18 15.03.05.19. This impacts an unknown function of the file /goform/saveAutoQos. This manipulation of the argument enable causes stack-based buffer overflow. The attack may be initiated remotely. The exploit has been published and may be used.	2025-09-28	8.8	CVE-2025-11123
Tenda--AC20	A vulnerability was identified in Tenda AC20 up to 16.03.08.12. Affected by this issue is the function strcpy of the file /goform/SetPptpServerCfg of the component HTTP POST Request Handler. Such manipulation of the argument startIp leads to buffer overflow. The attack can be launched remotely. The exploit is publicly available and might be used.	2025-09-22	8.8	CVE-2025-10815
Tenda--AC21	A vulnerability was identified in Tenda AC21 16.03.08.16. The affected element is the function sub_45BB10 of the file /goform/WifiExtraSet. The manipulation of the argument wpapsk_crypto leads to buffer overflow. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	2025-09-23	8.8	CVE-2025-10838
Tenda--AC21	A security flaw has been discovered in Tenda AC21 up to 16.03.08.16. Affected by this vulnerability is the function sscanf of the file /goform/SetStaticRouteCfg. The manipulation of the argument list results in buffer overflow. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	2025-09-28	8.8	CVE-2025-11091
Tenda--AC23	A vulnerability has been found in Tenda AC23 up to 16.03.07.52. Affected by this vulnerability is the function sscanf of the file /goform/SetPptpServerCfg of the component HTTP POST Request Handler. Such manipulation of the argument startIp leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2025-09-22	8.8	CVE-2025-10803
Tenda--AC8	A weakness has been identified in Tenda AC8 16.03.34.06. The affected element is the function formSetServerConfig of the file /goform/SetServerConfig. Executing manipulation can lead to buffer overflow. It is possible to launch the attack	2025-09-28	8.8	CVE-2025-11120

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remotely. The exploit has been made available to the public and could be exploited.			
Tenda--CH22	A vulnerability was determined in Tenda CH22 1.0.0.1. This vulnerability affects the function formWrlExtraGet of the file /goform/GstDhcpSetSer. This manipulation of the argument dips causes buffer overflow. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-28	8.8	CVE-2025-11117
Topaz--SERVCore Teller	A vulnerability was determined in Topaz SERVCore Teller 2.14.0-RC2/2.14.1. Affected by this issue is some unknown functionality of the file SERVCoreTeller_2.0.40D.msi of the component Installer. Executing manipulation can lead to permission issues. The attack needs to be launched locally. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	7.8	CVE-2025-10941
Tutorials-Website--Employee Management System	A vulnerability was detected in Tutorials-Website Employee Management System up to 611887d8f8375271ce8abc704507d46340837a60. Impacted is an unknown function of the file /admin/all-applied-leave.php of the component HTTP Request Handler. The manipulation results in improper authorization. The attack may be performed from remote. The exploit is now public and may be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed.	2025-09-26	7.3	CVE-2025-11030
undsgn--Uncode	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in undsgn Uncode allows Reflected XSS. This issue affects Uncode: from n/a through n/a.	2025-09-26	7.1	CVE-2025-48107
Unitree--Go2	Unitree Go2, G1, H1, and B2 devices through 2025-09-20 allow root OS command injection via the hostapd_restart.sh wifi_ssid or wifi_pass parameter (within restart_wifi_ap and restart_wifi_sta).	2025-09-26	8.2	CVE-2025-60017
Unitree--Go2	Multiple robotic products by Unitree sharing a common firmware, including the Go2, G1, H1, and B2 devices, contain a command injection vulnerability. By setting a malicious string when configuring the on-board WiFi via a BLE module of an affected robot, then triggering a restart of the WiFi service, an attacker can ultimately trigger commands to be run as root via the wpa_supplicant_restart.sh shell script. All Unitree models use firmware derived from the same codebase (MIT Cheetah), and the two major forks are the G1 (humanoid) and Go2 (quadruped) branches.	2025-09-26	7.3	CVE-2025-35027
UTT--1200GW	A security vulnerability has been detected in UTT 1200GW and 1250GW up to 3.0.0-170831/3.2.2-200710. This vulnerability affects unknown code of the file /goform/formApMail. The manipulation of the argument senderEmail leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	8.8	CVE-2025-10953
veronalabs--WP Statistics Simple, privacy-friendly Google Analytics alternative	The WP Statistics - The Most Popular Privacy-Friendly Analytics Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the User-Agent Header in all versions up to, and including, 14.5.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-27	7.2	CVE-2025-9816
W3S Cloud Technology--W3SCloud Contact Form 7 to Zoho CRM	Cross-Site Request Forgery (CSRF) vulnerability in W3S Cloud Technology W3SCloud Contact Form 7 to Zoho CRM allows Stored XSS. This issue affects W3SCloud Contact Form 7 to Zoho CRM: from n/a through 3.0.	2025-09-26	7.1	CVE-2025-60169
WAGO--Device Sphere	The database for the web application is exposed without authentication, allowing an unauthenticated remote attacker to gain unauthorized access and potentially compromise it.	2025-09-24	9.8	CVE-2025-41715
WAYOS--LQ_04	A vulnerability was identified in WAYOS LQ_04, LQ_05, LQ_06, LQ_07 and LQ_09 22.03.17. This affects an unknown function of the file /usb_paswd.asp. The manipulation of the argument Name leads to command injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	2025-09-26	7.3	CVE-2025-11045
webandprint--AR For WordPress	Cross-Site Request Forgery (CSRF) vulnerability in webandprint AR For WordPress allows Upload a Web Shell to a Web Server. This issue affects AR For WordPress: from n/a through 7.98.	2025-09-26	9.6	CVE-2025-60156
WP CMS Ninja--Current Age Plugin	Cross-Site Request Forgery (CSRF) vulnerability in WP CMS Ninja Current Age Plugin allows Stored XSS. This issue affects Current Age Plugin: from n/a through 1.6.	2025-09-22	7.1	CVE-2025-58687
wpdesk--Flexible PDF Invoices for WooCommerce & WordPress	Cross-Site Request Forgery (CSRF) vulnerability in wpdesk Flexible PDF Invoices for WooCommerce & WordPress allows Cross Site Request Forgery. This issue affects Flexible PDF Invoices for WooCommerce & WordPress: from n/a through 6.0.13.	2025-09-22	7.1	CVE-2025-57977

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wpdirectorykit--Sweet Energy Efficiency	Cross-Site Request Forgery (CSRF) vulnerability in wpdirectorykit Sweet Energy Efficiency allows Stored XSS. This issue affects Sweet Energy Efficiency: from n/a through 1.0.6.	2025-09-22	7.1	CVE-2025-58262
WPFunnels--Mail Mint	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPFunnels Mail Mint allows SQL Injection. This issue affects Mail Mint: from n/a through 1.18.6.	2025-09-22	7.6	CVE-2025-59570
wplakeorg--Advanced Views Display Posts, Custom Fields, and More	The Advanced Views - Display Posts, Custom Fields, and More plugin for WordPress is vulnerable to Server-Side Template Injection in all versions up to, and including, 3.7.19. This is due to insufficient input sanitization and lack of access control when processing custom Twig templates in the Model panel. This makes it possible for authenticated attackers, with author-level access or higher, to execute arbitrary PHP code and commands on the server.	2025-09-23	8.8	CVE-2025-10380
WPMK--WPMK PDF Generator	Cross-Site Request Forgery (CSRF) vulnerability in WPMK WPMK PDF Generator allows Stored XSS. This issue affects WPMK PDF Generator: from n/a through 1.0.1.	2025-09-22	7.1	CVE-2025-58268
wpshuffle--Subscribe to Download	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in wpshuffle Subscribe to Download allows PHP Local File Inclusion. This issue affects Subscribe to Download: from n/a through 2.0.9.	2025-09-26	7.5	CVE-2025-60150
wpshuffle--Subscribe To Unlock	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in wpshuffle Subscribe To Unlock allows PHP Local File Inclusion. This issue affects Subscribe To Unlock: from n/a through 1.1.5.	2025-09-26	7.5	CVE-2025-60153
wpsight--WPCasa	The WPCasa plugin for WordPress is vulnerable to Code Injection in all versions up to, and including, 1.4.1. This is due to insufficient input validation and restriction on the 'api_requests' function. This makes it possible for unauthenticated attackers to call arbitrary functions and execute code.	2025-09-23	9.8	CVE-2025-9321
yonisink--Custom Post Type Images	Cross-Site Request Forgery (CSRF) vulnerability in yonisink Custom Post Type Images allows Code Injection. This issue affects Custom Post Type Images: from n/a through 0.5.	2025-09-22	9.6	CVE-2025-58255
Yordam Information Technology Consulting Education and Electrical Systems Industry Trade Inc.--Yordam Katalog	Path Traversal: 'dir/../../filename' vulnerability in Yordam Information Technology Consulting Education and Electrical Systems Industry Trade Inc. Yordam Katalog allows Path Traversal.This issue affects Yordam Katalog: before 21.7.	2025-09-25	8.6	CVE-2025-10438
yourplugins--Conditional Cart Messages for WooCommerce – YourPlugins.com	Cross-Site Request Forgery (CSRF) vulnerability in yourplugins Conditional Cart Messages for WooCommerce – YourPlugins.com allows Stored XSS. This issue affects Conditional Cart Messages for WooCommerce – YourPlugins.com: from n/a through 1.2.10.	2025-09-26	7.1	CVE-2025-60171
Zenitel--ICX500	This vulnerability allows malicious actors to gain unauthorized access to the Zenitel ICX500 and ICX510 Gateway Billing Admin endpoint, enabling them to read the entire contents of the Billing Admin database.	2025-09-25	8.8	CVE-2025-59814
Zenitel--ICX500	This vulnerability allows malicious actors to execute arbitrary commands on the underlying system of the Zenitel ICX500 and ICX510 Gateway, granting shell access. Exploitation can compromise the device's availability, confidentiality, and integrity.	2025-09-25	8.4	CVE-2025-59815
Zenitel--ICX500	This vulnerability allows attackers to directly query the underlying database, potentially retrieving all data stored in the Billing Admin database, including user credentials. User passwords are stored in plaintext, significantly increasing the severity of this issue.	2025-09-25	7.3	CVE-2025-59816
Zenitel--TCIS-3+	This vulnerability allows attackers to execute arbitrary commands on the underlying system. Because the web portal runs with root privileges, successful exploitation grants full control over the device, potentially compromising its availability, confidentiality, and integrity.	2025-09-25	8.4	CVE-2025-59817

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xorux -- lpar2rrd	A password mismanagement situation exists in XoruX LPAR2RRD and STOR2RRD before 7.30 because cleartext information is present in HTML password input fields in the device properties. (Viewing the passwords requires configuring a web browser to display HTML password input fields.)	2021-11-08	4.3	CVE-2021-42370
ablancodev--Woocommerce Notify Updated Product	Cross-Site Request Forgery (CSRF) vulnerability in ablancodev Woocommerce Notify Updated Product allows Stored XSS. This issue affects Woocommerce Notify Updated Product: from n/a through 1.6.	2025-09-05	6.5	CVE-2025-58856
add-ons.org--PDF for WPForms	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in add-ons.org PDF for WPForms allows Stored XSS. This issue affects PDF for WPForms: from n/a through 6.2.1.	2025-09-03	6.5	CVE-2025-58620
aitool--Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One	Server-Side Request Forgery (SSRF) vulnerability in aitool Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One allows Server Side Request Forgery. This issue affects Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One: from n/a through 2.2.6.	2025-09-05	4.9	CVE-2025-58829
Akinsoft--e-Mutabakat	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Akinsoft e-Mutabakat allows Cross-Site Scripting (XSS).This issue affects e-Mutabakat: from 2.02.05 before v2.02.06.	2025-09-04	4.3	CVE-2024-13071
Akinsoft--LimonDesk	Improper Restriction of Rendered UI Layers or Frames vulnerability in Akinsoft LimonDesk allows iFrame Overlay, CAPEC - 103 - Clickjacking.This issue affects LimonDesk: from s1.02.14 before v1.02.17.	2025-09-03	4.3	CVE-2024-13066
Akinsoft--LimonDesk	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Akinsoft LimonDesk allows Cross-Site Scripting (XSS).This issue affects LimonDesk: from s1.02.14 before v1.02.17.	2025-09-03	4.7	CVE-2025-0878
Akinsoft--MyRezzta	Authorization Bypass Through User-Controlled Key vulnerability in Akinsoft MyRezzta allows Forceful Browsing.This issue affects MyRezzta: from s2.02.02 before v2.05.01.	2025-09-03	6.8	CVE-2024-13063
Akinsoft--MyRezzta	Improper Enforcement of Behavioral Workflow, Uncontrolled Resource Consumption vulnerability in Akinsoft MyRezzta allows Input Data Manipulation, CAPEC - 125 - Flooding.This issue affects MyRezzta: from s2.02.02 before v2.05.01.	2025-09-03	6.3	CVE-2024-13065
Akinsoft--MyRezzta	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Akinsoft MyRezzta allows Cross-Site Scripting (XSS).This issue affects MyRezzta: from s2.02.02 before v2.05.01.	2025-09-03	4.3	CVE-2024-13064
Akinsoft--OctoCloud	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Akinsoft OctoCloud allows Cross-Site Scripting (XSS).This issue affects OctoCloud: from s1.09.01 before v1.11.01.	2025-09-02	4.3	CVE-2024-12972
Akinsoft--OctoCloud	Origin Validation Error vulnerability in Akinsoft OctoCloud allows HTTP Response Splitting, CAPEC - 87 - Forceful Browsing.This issue affects OctoCloud: from s1.09.01 before v1.11.01.	2025-09-02	4.7	CVE-2024-12973
Akinsoft--OctoCloud	Authorization Bypass Through User-Controlled Key vulnerability in Akinsoft OctoCloud allows Resource Leak Exposure.This issue affects OctoCloud: from s1.09.02 before v1.11.01.	2025-09-02	4.7	CVE-2025-0640
Akinsoft--ProKuafor	Authorization Bypass Through User-Controlled Key vulnerability in Akinsoft ProKuafor allows Resource Leak Exposure.This issue affects ProKuafor: from s1.02.07 before v1.02.08.	2025-09-02	4.7	CVE-2025-0670

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Akinsoft--ProKuafr	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Akinsoft ProKuafÃ¶r allows Cross-Site Scripting (XSS).This issue affects ProKuafÃ¶r: from s1.02.07 before v1.02.08.	2025-09-02	4.3	CVE-2024-12974
Akinsoft--TaskPano	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Akinsoft TaskPano allows Cross-Site Scripting (XSS).This issue affects TaskPano: s1.06.04.	2025-09-04	4.7	CVE-2024-13073
Aknsoft--QR Men	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in AkÄ±nsoft QR MenÃ¼ allows Forceful Browsing, Phishing.This issue affects QR MenÃ¼: from s1.05.05 before v1.05.12.	2025-09-01	6.3	CVE-2024-12924
Aknsoft--QR Men	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AkÄ±nsoft QR MenÃ¼ allows Cross-Site Scripting (XSS).This issue affects QR MenÃ¼: from s1.05.05 before v1.05.12.	2025-09-01	4.3	CVE-2024-12914
Ali Aghdam--Aparat Video Shortcode	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ali Aghdam Aparat Video Shortcode allows Stored XSS. This issue affects Aparat Video Shortcode: from n/a through 0.2.4.	2025-09-05	6.5	CVE-2025-58876
Ali Khallad--Contact Form By Mega Forms	Missing Authorization vulnerability in Ali Khallad Contact Form By Mega Forms allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Contact Form By Mega Forms: from n/a through 1.6.1.	2025-09-03	5.4	CVE-2025-58639
alimuzzamanalim--Html Social share buttons	The Html Social share buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'zm_sh_btn' shortcode in all versions up to, and including, 2.1.16 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.	2025-09-06	5.3	CVE-2025-9849
alobaidi--PopAd	The PopAd plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.4. This is due to missing or incorrect nonce validation on the PopAd_reset_cookie_time function. This makes it possible for unauthenticated attackers to reset cookie time settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-04	5.3	CVE-2025-9616
AMD--AMD EPYC 7003 Series Processors	Improper restriction of operations in the IOMMU could allow a malicious hypervisor to access guest private memory resulting in loss of integrity.	2025-09-06	5.3	CVE-2023-31351
AMD--AMD Instinct MI300A	Improper input validation in AMD Power Management Firmware (PMFW) could allow a privileged attacker from Guest VM to send arbitrary input data potentially causing a GPU Reset condition.	2025-09-06	6	CVE-2024-36346
AMD--AMD Instinct MI300X	Insufficient parameter sanitization in TEE SOC Driver could allow an attacker to issue a malformed DRV_SOC_CMD_ID_SRIOV_SPATIAL_PART and cause read or write past the end of allocated arrays, potentially resulting in a loss of platform integrity or denial of service.	2025-09-06	4.7	CVE-2025-0034
AMD--AMD Radeon RX 5000 Series Graphics Products	An out of bounds write in the Linux graphics driver could allow an attacker to overflow the buffer potentially resulting in loss of confidentiality, integrity, or availability.	2025-09-06	6.1	CVE-2025-0010
AMD--AMD Ryzen 5000 Series Processors with Radeon Graphics	Insufficient parameter validation while allocating process space in the Trusted OS (TOS) may allow for a malicious userspace process to trigger an integer overflow, leading to a potential denial of service.	2025-09-06	4.1	CVE-2021-26377

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
AMD--AMD Ryzen 7035 Series Processor with Radeon Graphics	A NULL pointer dereference in AMD Crash Defender could allow an attacker to write a NULL output to a log file potentially resulting in a system crash and loss of availability.	2025-09-06	5.5	CVE-2025-0009
AMD--AMD Ryzen Threadripper 3000 Processors	Improper validation of an array index in the AND power Management Firmware could allow a privileged attacker to corrupt AGESA memory potentially leading to a loss of integrity.	2025-09-06	4.4	CVE-2024-21970
Amuse Labs--PuzzleMe for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Amuse Labs PuzzleMe for WordPress allows Stored XSS. This issue affects PuzzleMe for WordPress: from n/a through 1.2.0.	2025-09-03	6.5	CVE-2025-58621
antirez--linenoise	TOCTOU in linenoiseHistorySave in linenoise allows local attackers to overwrite arbitrary files and change permissions via a symlink race between fopen("w") on the history path and subsequent chmod() on the same path.	2025-09-01	6.8	CVE-2025-9810
arisoft--ARI Fancy Lightbox	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in arisoft ARI Fancy Lightbox allows Stored XSS. This issue affects ARI Fancy Lightbox: from n/a through 1.4.0.	2025-09-05	6.5	CVE-2025-58784
Arjan Olsder--SEO Auto Linker	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Arjan Olsder SEO Auto Linker allows Stored XSS. This issue affects SEO Auto Linker: from n/a through 1.5.3.	2025-09-05	5.9	CVE-2025-58791
Babar--prettyPhoto	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Babar prettyPhoto allows Stored XSS. This issue affects prettyPhoto: from n/a through 1.2.4.	2025-09-05	6.5	CVE-2025-58808
Barn2 Plugins--Posts Table with Search & Sort	Missing Authorization vulnerability in Barn2 Plugins Posts Table with Search & Sort allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Posts Table with Search & Sort: from n/a through 1.4.10.	2025-09-03	5.3	CVE-2025-58613
Bjorn Manintveld--BCM Duplicate Menu	Cross-Site Request Forgery (CSRF) vulnerability in Bjorn Manintveld BCM Duplicate Menu allows Cross Site Request Forgery. This issue affects BCM Duplicate Menu: from n/a through 1.1.2.	2025-09-05	4.3	CVE-2025-58798
Bohemia Plugins--Event Feed for Eventbrite	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bohemia Plugins Event Feed for Eventbrite allows DOM-Based XSS. This issue affects Event Feed for Eventbrite: from n/a through 1.3.2.	2025-09-03	6.5	CVE-2025-58623
brijrajs--WooCommerce Single Page Checkout	Cross-Site Request Forgery (CSRF) vulnerability in brijrajs WooCommerce Single Page Checkout allows Cross Site Request Forgery. This issue affects WooCommerce Single Page Checkout: from n/a through 1.2.7.	2025-09-05	4.3	CVE-2025-58804
calliko--Bonus for Woo	Improper Validation of Specified Quantity in Input vulnerability in calliko Bonus for Woo allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Bonus for Woo: from n/a through 7.4.1.	2025-09-05	5.3	CVE-2025-58835
Campcodes--Grocery Sales and Inventory System	A vulnerability was detected in Campcodes Grocery Sales and Inventory System 1.0. The affected element is an unknown function of the file /index.php. The manipulation of the argument page results in cross site scripting. The attack can be executed remotely. The exploit is now public and may be used.	2025-09-06	4.3	CVE-2025-10032
Campcodes--Recruitment Management System	A security flaw has been discovered in Campcodes Recruitment Management System 1.0. This impacts the function include of the file /admin/index.php. The manipulation of the argument page results in file inclusion. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	2025-09-03	4.7	CVE-2025-9920

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Campcodes--Sales and Inventory System	A security vulnerability has been detected in Campcodes Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /index.php. Such manipulation of the argument page leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	2025-09-03	4.3	CVE-2025-9922
Campcodes--Sales and Inventory System	A flaw has been found in Campcodes Sales and Inventory System 1.0. This affects an unknown part of the file /index.php. Executing manipulation of the argument page can lead to cross site scripting. The attack may be launched remotely. The exploit has been published and may be used.	2025-09-03	4.3	CVE-2025-9923
choijun--LA-Studio Element Kit for Elementor	The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of the plugin's widgets in all versions up to, and including, 1.5.5.1 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.	2025-09-06	6.4	CVE-2025-8360
Cisco--Cisco Evolved Programmable Network Manager (EPNM)	A vulnerability in the web-based management interface of Cisco Evolved Programmable Network Manager (EPNM) and Cisco Prime Infrastructure could allow an authenticated, remote attacker to obtain sensitive information from an affected system. This vulnerability is due to improper validation of requests to API endpoints. An attacker could exploit this vulnerability by sending a valid request to a specific API endpoint within the affected system. A successful exploit could allow a low-privileged user to view sensitive configuration information on the affected system that should be restricted. To exploit this vulnerability, an attacker must have access as a low-privileged user.	2025-09-03	4.3	CVE-2025-20270
Cisco--Cisco Evolved Programmable Network Manager (EPNM)	A vulnerability in the web-based management interface of Cisco Evolved Programmable Network Manager (EPNM) and Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against users of the interface of an affected system. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious code into specific data fields in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, an attacker must have valid administrative credentials.	2025-09-03	4.8	CVE-2025-20280
Cisco--Cisco Evolved Programmable Network Manager (EPNM)	A vulnerability in the web-based management interface of Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to upload arbitrary files to an affected device. This vulnerability is due to improper validation of files that are uploaded to the web-based management interface. An attacker could exploit this vulnerability by sending a crafted file upload request to a specific API endpoint. A successful exploit could allow the attacker to upload arbitrary files to an affected system. To exploit this vulnerability, an attacker must have at least valid Config Managers credentials on the affected device.	2025-09-03	4.3	CVE-2025-20287
Cisco--Cisco Session Initiation Protocol (SIP) Software	A vulnerability in the directory permissions of Cisco Desk Phone 9800 Series, Cisco IP Phone 7800 and 8800 Series, and Cisco Video Phone 8875 could allow an unauthenticated, remote attacker to write arbitrary files on an affected device. This vulnerability is due to a lack of proper authentication controls. An attacker could exploit this vulnerability by sending a crafted request to an affected device. A successful exploit could allow the attacker to perform arbitrary file writes to specific directories in the underlying operating system. Note: To exploit this vulnerability, Web Access must be enabled on the phone. Web Access is disabled by default.	2025-09-03	5.3	CVE-2025-20335
Cisco--Cisco Session Initiation	A vulnerability in the directory permissions of Cisco Desk Phone 9800 Series, Cisco IP Phone 7800 and 8800 Series, and Cisco Video Phone 8875 could allow an	2025-09-03	5.3	CVE-2025-20336

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Protocol (SIP) Software	unauthenticated, remote attacker to access sensitive information on an affected device. This vulnerability exists because the product exposes sensitive information to an actor that is not explicitly authorized to have access to that information. An attacker could exploit this vulnerability by sending a crafted packet to the IP address of a device that has Web Access enabled. A successful exploit could allow the attacker to access sensitive information from the device. Note: To exploit this vulnerability, Web Access must be enabled on the phone. Web Access is disabled by default.			
Cisco--Cisco Unified Communications Manager	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) Software and Cisco Unified CM Session Management Edition (SME) Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user.	2025-09-03	4.3	CVE-2025-20326
Cisco--Cisco Unified Communications Manager IM and Presence Service	A vulnerability in the web-based management interface of Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2025-09-03	6.1	CVE-2025-20330
Cisco--Cisco Webex Meetings	A vulnerability in the user profile component of Cisco Webex Meetings could have allowed an authenticated, remote attacker with low privileges to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. Cisco has addressed this vulnerability in the Cisco Webex Meetings service, and no customer action is needed. This vulnerability existed because of insufficient validation of user-supplied input to the user profile component of Cisco Webex Meetings. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could have allowed the attacker to conduct an XSS attack against the targeted user.	2025-09-03	5.4	CVE-2025-20328
Cisco--Cisco Webex Meetings	A vulnerability in Cisco Webex Meetings could have allowed an unauthenticated, remote attacker to redirect a targeted Webex Meetings user to an untrusted website. Cisco has addressed this vulnerability in the Cisco Webex Meetings service, and no customer action is needed. This vulnerability existed because of insufficient validation of URLs that were included in a meeting-join URL. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by including a URL to a website of their choosing in a specific value of a Cisco Webex Meetings join URL. A successful exploit could have allowed the attacker to redirect a targeted user to a website that was controlled by the attacker, possibly making the user more likely to believe the website was trusted by Webex and perform additional actions as part of phishing attacks.	2025-09-03	4.3	CVE-2025-20291
cloudinfrastructureservices--Cloud SAML SSO Single Sign On Login	The Cloud SAML SSO plugin for WordPress is vulnerable to Identity Provider Deletion due to a missing capability check on the delete_config action of the csso_handle_actions() function in all versions up to, and including, 1.0.19. This makes it possible for unauthenticated attackers to delete any configured IdP, breaking the SSO authentication flow and causing a denial-of-service.	2025-09-06	6.5	CVE-2025-7045
code-projects--Mobile Shop	A security vulnerability has been detected in code-projects Mobile Shop Management System 1.0. This affects an unknown function of the file AddNewProduct.php. The manipulation of the argument ProductImage leads to	2025-09-02	6.3	CVE-2025-9841

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	unrestricted upload. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.			
CodeAstro--Real Estate Management System	A flaw has been found in CodeAstro Real Estate Management System 1.0. This impacts an unknown function of the file /register.php. Executing manipulation of the argument uimage can lead to unrestricted upload. The attack can be launched remotely. The exploit has been published and may be used.	2025-09-04	6.3	CVE-2025-9941
CodeAstro--Real Estate Management System	A vulnerability has been found in CodeAstro Real Estate Management System 1.0. Affected is an unknown function of the file /submitproperty.php. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-09-04	6.3	CVE-2025-9942
codemstory--	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codemstory ì½"ë"œì— ìƒµ ì†Œì…œí†¡ allows Stored XSS. This issue affects ì½"ë"œì— ìƒµ ì†Œì…œí†¡: from n/a through 1.2.1.	2025-09-05	6.5	CVE-2025-58828
Course Finder | andr martin - it solutions & research UG--Course Booking Platform	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Course Finder | andrÃ© martin - it solutions & research UG Course Booking Platform allows Stored XSS. This issue affects Course Booking Platform: from n/a through 1.0.0.	2025-09-05	6.5	CVE-2025-58887
Cozmoslabs--Paid Member Subscriptions	Missing Authorization vulnerability in Cozmoslabs Paid Member Subscriptions allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Paid Member Subscriptions: from n/a through 2.15.9.	2025-09-03	5.3	CVE-2025-58600
CozyThemes--SaasLauncher	Missing Authorization vulnerability in CozyThemes SaasLauncher allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects SaasLauncher: from n/a through 1.3.0.	2025-09-03	5	CVE-2025-58606
D-Link--DI-7400G+	A security flaw has been discovered in D-Link DI-7400G+ 19.12.25A1. Affected is the function sub_478D28 of the file /mng_platform.asp. The manipulation of the argument addr with the input `echo 12345 > poc.txt` results in command injection. An attack on the physical device is feasible. The exploit has been released to the public and may be exploited.	2025-09-01	4.1	CVE-2025-9769
Dadevarzan--Dadevarzan WordPress Common	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dadevarzan Dadevarzan WordPress Common allows Stored XSS. This issue affects Dadevarzan WordPress Common: from n/a through 2.2.2.	2025-09-03	6.5	CVE-2025-58632
Das--Parking Management System	A vulnerability was detected in Das Parking Management System å•œè½¦åœºç®¡ç•†ç³»ç»Ÿ 6.2.0. This impacts an unknown function of the file /Operator/Search. The manipulation results in information disclosure. The attack may be performed from remote. The exploit is now public and may be used.	2025-09-03	5.3	CVE-2025-9842
Das--Parking Management System	A flaw has been found in Das Parking Management System å•œè½¦åœºç®¡ç•†ç³»ç»Ÿ 6.2.0. Affected is an unknown function of the file /Operator/FindAll. This manipulation causes information disclosure. It is possible to initiate the attack remotely. The exploit has been published and may be used.	2025-09-03	5.3	CVE-2025-9843
DeBAAT--WP-GraphViz	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DeBAAT WP-GraphViz allows DOM-Based XSS. This issue affects WP-GraphViz: from n/a through 1.5.1.	2025-09-05	6.5	CVE-2025-58870
deepakmisal24--Chemical Inventory Management System	A vulnerability was identified in deepakmisal24 Chemical Inventory Management System up to 1.0. Affected by this vulnerability is an unknown functionality of the file /inventory_form.php. Such manipulation of the argument chem_name leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	2025-09-01	6.3	CVE-2025-9758

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Deetronix--Booking Ultra Pro	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Deetronix Booking Ultra Pro allows Stored XSS. This issue affects Booking Ultra Pro: from n/a through 1.1.21.	2025-09-03	6.5	CVE-2025-58633
Dell--Alienware Command Center 5.x (AWCC)	Dell Alienware Command Center 5.x (AWCC), versions prior to 5.10.2.0, contains an Improper Link Resolution Before File Access ('Link Following')" vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	2025-09-02	6.7	CVE-2025-43726
DesertThemes--SoftMe	Missing Authorization vulnerability in DesertThemes SoftMe allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects SoftMe: from n/a through 1.1.24.	2025-09-05	4.3	CVE-2025-58817
designful--Smart Table Builder	The Smart Table Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-06	6.4	CVE-2025-9126
DigitalCourt--Boxed Content	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DigitalCourt Boxed Content allows Stored XSS. This issue affects Boxed Content: from n/a through 1.0.	2025-09-05	6.5	CVE-2025-58851
docjojo--atec Debug	The atec Debug plugin for WordPress is vulnerable to arbitrary file read in all versions up to, and including, 1.2.22 via the 'custom_log' parameter. This makes it possible for authenticated attackers, with Administrator-level access and above, to view the contents of files outside of the originally intended directory.	2025-09-04	4.9	CVE-2025-9516
dudaster--Elementor Element Condition	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dudaster Elementor Element Condition allows Stored XSS. This issue affects Elementor Element Condition: from n/a through 1.0.5.	2025-09-05	6.5	CVE-2025-58796
Eaton--NMC G2	An attacker with authenticated and privileged access could modify the contents of a non-sensitive file by traversing the path in the limited shell of the CLI. This security issue has been fixed in the latest version of NMC G2 which is available on the Eaton download center.	2025-09-05	4.7	CVE-2025-48395
ECOVACS--DEEBOT X1 Series	ECOVACS robot vacuums and base stations communicate via an insecure Wi-Fi network with a deterministic WPA2-PSK, which can be easily derived.	2025-09-05	6.3	CVE-2025-30198
ECOVACS--DEEBOT X1 Series	ECOVACS robot vacuums and base stations communicate via an insecure Wi-Fi network with a deterministic AES encryption key, which can be easily derived.	2025-09-05	6.3	CVE-2025-30200
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. In versions below 35.7.5, 36.0.0-alpha.1 through 36.8.0, 37.0.0-alpha.1 through 37.3.1 and 38.0.0-alpha.1 through 38.0.0-beta.6, ASAR Integrity Bypass via resource modification. This only impacts apps that have the embeddedAsarIntegrityValidation and onlyLoadAppFromAsar fuses enabled. Apps without these fuses enabled are not impacted. This issue is fixed in versions 35.7.5, 36.8.1, 37.3.1 and 38.0.0-beta.6.	2025-09-04	6.1	CVE-2025-55305
elextensions--ELEX WooCommerce Google Shopping (Google Product Feed)	The ELEX WooCommerce Google Shopping (Google Product Feed) plugin for WordPress is vulnerable to SQL Injection via the 'file_to_delete' parameter in all versions up to, and including, 1.4.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-06	4.9	CVE-2025-10046
elunez--eladmin	A security flaw has been discovered in elunez eladmin 1.1. Impacted is the function deleteFile of the component LocalStorageController. The manipulation results in	2025-09-03	5.4	CVE-2025-9937

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	improper authorization. The attack may be performed from remote. The exploit has been released to the public and may be exploited.			
envoyproxy--envoy	Envoy is an open source L7 proxy and communication bus designed for large modern service oriented architectures. In versions below 1.32.10 and 1.33.0 through 1.33.6, 1.34.0 through 1.34.4 and 1.35.0, insufficient Session Expiration in the Envoy OAuth2 filter leads to failed logout operations. When configured with __Secure- or __Host- prefixed cookie names, the filter fails to append the required Secure attribute to the Set-Cookie header during deletion. Modern browsers ignore this invalid request, causing the session cookie to persist. This allows a user to remain logged in after they believe they have logged out, creating a session hijacking risk on shared computers. The current implementation iterates through the configured cookie names to generate deletion headers but does not check for these prefixes. This failure to properly construct the deletion header means the user's session cookies are never removed by the browser, leaving the session active and allowing the next user of the same browser to gain unauthorized access to the original user's account and data. This is fixed in versions 1.32.10, 1.33.7, 1.34.5 and 1.35.1.	2025-09-03	6.3	CVE-2025-55162
Eric Mann--WP Publication Archive	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Eric Mann WP Publication Archive allows Stored XSS. This issue affects WP Publication Archive : from n/a through 3.0.1.	2025-09-05	6.5	CVE-2025-58826
FAKTOR VIER--F4 Media Taxonomies	Missing Authorization vulnerability in FAKTOR VIER F4 Media Taxonomies allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects F4 Media Taxonomies: from n/a through 1.1.4.	2025-09-03	4.3	CVE-2025-58617
falselight--Exchange Rates	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in falselight Exchange Rates allows Stored XSS. This issue affects Exchange Rates: from n/a through 1.2.5.	2025-09-03	6.5	CVE-2025-58624
Frisbii--Frisbii Pay	Missing Authorization vulnerability in Frisbii Frisbii Pay allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Frisbii Pay: from n/a through 1.8.2.1.	2025-09-03	6.5	CVE-2025-58616
fullworks--Quick Paypal Payments	Cross-Site Request Forgery (CSRF) vulnerability in fullworks Quick Paypal Payments allows Cross Site Request Forgery. This issue affects Quick Paypal Payments: from n/a through 5.7.46.	2025-09-05	4.3	CVE-2025-27003
fuyang_lipengjun--platform	A vulnerability was identified in fuyang_lipengjun platform 1.0.0. This issue affects the function AdController of the file /ad/queryAll. The manipulation leads to improper authorization. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	2025-09-03	4.3	CVE-2025-9936
GDPR Info--Cookie Notice & Consent Banner for GDPR & CCPA Compliance	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GDPR Info Cookie Notice & Consent Banner for GDPR & CCPA Compliance allows Stored XSS. This issue affects Cookie Notice & Consent Banner for GDPR & CCPA Compliance: from n/a through 1.7.11.	2025-09-03	6.5	CVE-2025-58607
George Sexton--WordPress Events Calendar Plugin connectDaily	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in George Sexton WordPress Events Calendar Plugin - connectDaily allows Stored XSS. This issue affects WordPress Events Calendar Plugin - connectDaily: from n/a through 1.5.3.	2025-09-05	6.5	CVE-2025-58862
gfazioli--WP Bannerize Pro	Server-Side Request Forgery (SSRF) vulnerability in gfazioli WP Bannerize Pro allows Server Side Request Forgery. This issue affects WP Bannerize Pro: from n/a through 1.10.0.	2025-09-03	4.4	CVE-2025-58615
givecloud--Donation Forms WP by Givecloud	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in givecloud Donation Forms WP by Givecloud allows	2025-09-05	6.5	CVE-2025-58842

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Stored XSS. This issue affects Donation Forms WP by Givecloud: from n/a through 1.0.9.			
gourl--GoUrl Bitcoin Payment Gateway & Paid Downloads & Membership	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gourl GoUrl Bitcoin Payment Gateway & Paid Downloads & Membership allows Stored XSS. This issue affects GoUrl Bitcoin Payment Gateway & Paid Downloads & Membership: from n/a through 1.6.6.	2025-09-05	5.9	CVE-2025-48102
gugu--short.io	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gugu short.io allows DOM-Based XSS. This issue affects short.io: from n/a through 2.4.0.	2025-09-05	6.5	CVE-2025-58834
gutentor--Gutentor	Missing Authorization vulnerability in gutentor Gutentor allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Gutentor: from n/a through 3.5.1.	2025-09-05	4.3	CVE-2025-58783
Habibur Rahman--Comment Form WP â€“ Customize Default Comment Form	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Habibur Rahman Comment Form WP – Customize Default Comment Form allows Stored XSS. This issue affects Comment Form WP – Customize Default Comment Form: from n/a through 2.0.0.	2025-09-05	5.9	CVE-2025-58825
Huawei--HarmonyOS	Permission verification vulnerability in the home screen module Impact: Successful exploitation of this vulnerability may affect availability.	2025-09-05	6.8	CVE-2025-58276
Huawei--HarmonyOS	Race condition vulnerability in the device standby module. Impact: Successful exploitation of this vulnerability may cause feature exceptions of the device standby module.	2025-09-05	5.1	CVE-2025-58313
iamroody--	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in iamroody é‡‘æ•°æ•® allows Stored XSS. This issue affects é‡‘æ•°æ•®: from n/a through 1.0.	2025-09-05	6.5	CVE-2025-58864
IBM--App Connect Enterprise Certified Container	IBM App Connect Enterprise Certified Container CD: 9.2.0 through 11.6.0, 12.1.0 through 12.14.0, and 12.0 LTS: 12.0.0 through 12.0.14stores potentially sensitive information in log files during installation that could be read by a local user on the container.	2025-09-01	5.9	CVE-2025-36133
IBM--Concert Software	IBM Concert Software 1.0.0 through 1.1.0 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-09-01	6.1	CVE-2025-0656
IBM--Concert Software	IBM Concert Software 1.0.0 through 1.1.0 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-09-01	5.4	CVE-2025-33082
IBM--Concert Software	IBM Concert Software 1.0.0 through 1.1.0 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-09-01	5.4	CVE-2025-33083
IBM--Concert Software	IBM Concert Software 1.0.0 through 1.1.0 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.	2025-09-01	5.9	CVE-2025-33084
IBM--Concert Software	IBM Concert Software 1.0.0 through 1.1.0 could allow a remote attacker to perform unauthorized actions using man in the middle techniques due to improper certificate validation.	2025-09-01	5.9	CVE-2025-33099

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--Concert Software	IBM Concert Software 1.0.0 through 1.1.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	2025-09-01	5.9	CVE-2025-33102
IBM--Jazz Foundation	IBM Jazz Foundation 7.0.2 through 7.0.2 iFix033, 7.0.3 through 7.0.3 iFix012, and 7.1.0 through 7.1.0 iFix002 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-09-04	6.1	CVE-2024-43184
IBM--Jazz Foundation	IBM Jazz Foundation 7.0.2 through 7.0.2 iFix033, 7.0.3 through 7.0.3 iFix012, and 7.1.0 through 7.1.0 iFix002 could allow an authenticated user to upload files to the system due to improper neutralization of sequences that can resolve to a restricted directory.	2025-09-04	6.5	CVE-2025-25048
IBM--MQ	IBM MQ LTS 9.1.0.0 through 9.1.0.29, 9.2.0.0 through 9.2.0.36, 9.3.0.0 through 9.3.0.30 and 9.4.0.0 through 9.4.0.12 and IBM MQ CD 9.3.0.0 through 9.3.5.1 and 9.4.0.0 through 9.4.3.0 Java and JMS stores a password in client configuration files when trace is enabled which can be read by a local user.	2025-09-07	5.1	CVE-2025-36100
IBM--Sterling B2B Integrator	IBM Sterling B2B Integrator 6.0.0.0 through 6.1.2.7_1 and 6.2.0.0 through 6.2.0.4 and IBM Sterling File Gateway 6.0.0.0 through 6.1.2.7_1 and 6.2.0.0 through 6.2.0.4 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-09-04	4.8	CVE-2025-2694
IBM--UrbanCode Deploy	IBM DevOps Deploy / IBM UrbanCode Deploy (UCD) 8.1 before 8.1.2.2 could allow an authenticated user to obtain sensitive information about configuration on the system.	2025-09-02	4.3	CVE-2025-36162
Ibnul H.--Custom Team Manager	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ibnul H. Custom Team Manager allows Stored XSS. This issue affects Custom Team Manager: from n/a through 2.4.2.	2025-09-05	6.5	CVE-2025-58840
IfSo Dynamic Content--If-So Dynamic Content Personalization	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in IfSo Dynamic Content If-So Dynamic Content Personalization allows Stored XSS. This issue affects If-So Dynamic Content Personalization: from n/a through 1.9.4.	2025-09-03	6.5	CVE-2025-58602
itsourcecode--POS Point of Sale System	A vulnerability was identified in itsourcecode POS Point of Sale System 1.0. This vulnerability affects unknown code of the file /inventory/main/vendors/datatables/unit_testing/templates/deferred_table.php. The manipulation of the argument scripts leads to cross site scripting. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	2025-09-06	4.3	CVE-2025-10063
itsourcecode--POS Point of Sale System	A security flaw has been discovered in itsourcecode POS Point of Sale System 1.0. This issue affects some unknown processing of the file /inventory/main/vendors/datatables/unit_testing/templates/dom_data_two_headers.php. The manipulation of the argument scripts results in cross site scripting. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	2025-09-07	4.3	CVE-2025-10064
itsourcecode--POS Point of Sale System	A weakness has been identified in itsourcecode POS Point of Sale System 1.0. Impacted is an unknown function of the file /inventory/main/vendors/datatables/unit_testing/templates/dom_data_th.php. This manipulation of the argument scripts causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	2025-09-07	4.3	CVE-2025-10065

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
itsourcecode--POS Point of Sale System	A security vulnerability has been detected in itsourcecode POS Point of Sale System 1.0. The affected element is an unknown function of the file /inventory/main/vendors/datatables/unit_testing/templates/dymanic_table.php. Such manipulation of the argument scripts leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	2025-09-07	4.3	CVE-2025-10066
itsourcecode--POS Point of Sale System	A vulnerability was detected in itsourcecode POS Point of Sale System 1.0. The impacted element is an unknown function of the file /inventory/main/vendors/datatables/unit_testing/templates/empty_table.php. Performing manipulation of the argument scripts results in cross site scripting. It is possible to initiate the attack remotely. The exploit is now public and may be used.	2025-09-07	4.3	CVE-2025-10067
itsourcecode--Sports Management System	A vulnerability was identified in itsourcecode Sports Management System 1.0. This impacts an unknown function of the file /Admin/mode.php. The manipulation of the argument code leads to sql injection. The attack is possible to be carried out remotely.	2025-09-01	6.3	CVE-2025-9768
itsourcecode--Sports Management System	A weakness has been identified in itsourcecode Sports Management System 1.0. The impacted element is an unknown function of the file /Admin/gametype.php. Executing manipulation of the argument code can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.	2025-09-02	6.3	CVE-2025-9840
Iulia Cazan--Latest Post Shortcode	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Iulia Cazan Latest Post Shortcode allows Stored XSS. This issue affects Latest Post Shortcode: from n/a through 14.0.3.	2025-09-03	6.5	CVE-2025-58609
Ivan Drago--vipdrv	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ivan Drago vipdrv allows Stored XSS. This issue affects vipdrv: from n/a through 1.0.3.	2025-09-05	5.9	CVE-2025-58884
Jamel.Z--Tooltipy	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jamel.Z Tooltipy allows Stored XSS. This issue affects Tooltipy: from n/a through 5.5.6.	2025-09-03	6.5	CVE-2025-58614
jbhovik--Ray Enterprise Translation	Missing Authorization vulnerability in jbhovik Ray Enterprise Translation allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Ray Enterprise Translation: from n/a through 1.7.1.	2025-09-05	5.4	CVE-2025-58785
jimmywb--Simple Link List Widget	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jimmywb Simple Link List Widget allows Stored XSS. This issue affects Simple Link List Widget: from n/a through 0.3.2.	2025-09-05	5.9	CVE-2025-58810
Jinher--OA	A vulnerability was detected in Jinher OA 1.0. Affected is an unknown function of the file /jc6/platform/sys/login!changePassWord.action of the component POST Request Handler. The manipulation of the argument Account results in cross site scripting. The attack can be launched remotely. The exploit is now public and may be used.	2025-09-03	4.3	CVE-2025-9931
John Luetke--Media Author	Incorrect Privilege Assignment vulnerability in John Luetke Media Author allows Privilege Escalation. This issue affects Media Author: from n/a through 1.0.4.	2025-09-05	5.5	CVE-2025-58841
Jonathan Jernigan--Pie Calendar	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jonathan Jernigan Pie Calendar allows DOM-Based XSS. This issue affects Pie Calendar: from n/a through 1.2.8.	2025-09-03	6.5	CVE-2025-58618
josepsitjar--StoryMap	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in josepsitjar StoryMap allows DOM-Based XSS. This issue affects StoryMap: from n/a through 2.1.	2025-09-05	6.5	CVE-2025-58874

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kamleshyadav--Exit Intent Popup	Server-Side Request Forgery (SSRF) vulnerability in kamleshyadav Exit Intent Popup allows Server Side Request Forgery. This issue affects Exit Intent Popup: from n/a through 1.0.1.	2025-09-03	5.4	CVE-2025-58641
KCS--Responder	Cross-Site Request Forgery (CSRF) vulnerability in KCS Responder allows Cross Site Request Forgery. This issue affects Responder: from n/a through 4.3.8.	2025-09-05	5.4	CVE-2025-58801
Khanakag-17--Library Management System	A vulnerability has been found in Khanakag-17 Library Management System up to 60ed174506094dcd166e34904a54288e5d10ff24. This affects an unknown function of the file /index.php. The manipulation of the argument msg leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided.	2025-09-01	4.3	CVE-2025-9755
Klarna--Klarna Order Management for WooCommerce	Insertion of Sensitive Information Into Debugging Code vulnerability in Klarna Klarna Order Management for WooCommerce allows Retrieve Embedded Sensitive Data. This issue affects Klarna Order Management for WooCommerce: from n/a through 1.9.8.	2025-09-03	6.6	CVE-2025-58598
Kubernetes--secrets-store-sync-controller	Kubernetes secrets-store-sync-controller in versions before 0.0.2 discloses service account tokens in logs.	2025-09-05	6.5	CVE-2025-7445
Luis Rock--Master Paper Collapse Toggle	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Luis Rock Master Paper Collapse Toggle allows Stored XSS. This issue affects Master Paper Collapse Toggle: from n/a through 1.1.	2025-09-05	6.5	CVE-2025-58871
macrozheng--mall	A vulnerability has been found in macrozheng mall up to 1.0.3. This affects the function cancelOrder of the file /order/cancelUserOrder. The manipulation of the argument orderId leads to authorization bypass. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-09-02	4.3	CVE-2025-9835
macrozheng--mall	A vulnerability was found in macrozheng mall up to 1.0.3. This vulnerability affects the function paySuccess of the file /order/paySuccess. The manipulation of the argument orderId results in authorization bypass. The attack can be launched remotely. The exploit has been made public and could be used.	2025-09-02	4.3	CVE-2025-9836
Mahmudul Hasan Arif--Ninja Charts	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Mahmudul Hasan Arif Ninja Charts allows Retrieve Embedded Sensitive Data. This issue affects Ninja Charts: from n/a through 3.3.2.	2025-09-05	5.3	CVE-2025-58797
Malcure Web Security--Malcure Malware Scanner	Missing Authorization vulnerability in Malcure Web Security Malcure Malware Scanner allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Malcure Malware Scanner: from n/a through 16.8.	2025-09-03	4.3	CVE-2025-3701
marcshowpass--Showpass WordPress Extension	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in marcshowpass Showpass WordPress Extension allows Stored XSS. This issue affects Showpass WordPress Extension: from n/a through 4.0.3.	2025-09-05	6.5	CVE-2025-58850
MatrixAddons--Document Engine	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MatrixAddons Document Engine allows Stored XSS. This issue affects Document Engine: from n/a through 1.2.	2025-09-03	6.5	CVE-2025-58640
Mautic--Mautic	SummaryA user with administrator rights can change the configuration of the mautic application and extract secrets that are not normally available. ImpactAn administrator who usually does not have access to certain parameters, such as database credentials, can disclose them.	2025-09-03	5.5	CVE-2025-9822
Mautic--Mautic	ImpactThe attacker can validate if a user exists by checking the time login returns. This timing difference can be used to enumerate valid usernames, after which an attacker could attempt brute force attacks. PatchesThis vulnerability has been	2025-09-03	5.9	CVE-2025-9824

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	patched, implementing a timing-safe form login authenticator that ensures consistent response times regardless of whether a user exists or not. Technical DetailsThe vulnerability was caused by different response times when: * A valid username was provided (password hashing occurred) * An invalid username was provided (no password hashing occurred) The fix introduces a TimingSafeFormLoginAuthenticator that performs a dummy password hash verification even for non-existent users, ensuring consistent timing. WorkaroundsNo workarounds are available. Users should upgrade to the patched version. References * https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/03-Identity_Management_Testing/04-Testing_for_Account_Enumeration_and_Guessable_User_Account			
michalzagdan--TrustMate.io WooCommerce integration	Cross-Site Request Forgery (CSRF) vulnerability in michalzagdan TrustMate.io - WooCommerce integration allows Cross Site Request Forgery. This issue affects TrustMate.io - WooCommerce integration: from n/a through 1.14.0.	2025-09-05	4.3	CVE-2025-58802
Microsoft--Microsoft Edge (Chromium-based)	Improper access control in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network.	2025-09-05	4.7	CVE-2025-53791
Microsoft--Xbox Gaming Services	Exposure of sensitive information to an unauthorized actor in Xbox allows an unauthorized attacker to disclose information over a network.	2025-09-04	6.5	CVE-2025-55242
Mikado Themes--Biagiotti Core	The Biagiotti Core plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 2.1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-05	6.4	CVE-2025-9057
mndpsingh287--WP Mail	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mndpsingh287 WP Mail allows DOM-Based XSS. This issue affects WP Mail: from n/a through 1.3.	2025-09-05	6.5	CVE-2025-58822
MobSF--Mobile-Security-Framework-MobSF	MobSF is a mobile application security testing tool used. In version 4.4.0, an authenticated user who uploaded a specially prepared one.a, can write arbitrary files to any directory writable by the user of the MobSF process. This issue has been patched in version 4.4.1.	2025-09-02	6.5	CVE-2025-58162
MongoDB Inc--MongoDB Server	An improper setting of the lsid field on any sharded query can cause a crash in MongoDB routers. This issue occurs when a generic argument (lsid) is provided in a case when it is not applicable. This affects MongoDB Server v6.0 versions prior to 6.0.x, MongoDB Server v7.0 versions prior to 7.0.18 and MongoDB Server v8.0 versions prior to 8.0.6.	2025-09-05	6.5	CVE-2025-10059
MongoDB Inc--MongoDB Server	MongoDB Server may allow upsert operations retried within a transaction to violate unique index constraints, potentially causing an invariant failure and server crash during commit. This issue may be triggered by improper WriteUnitOfWork state management. This issue affects MongoDB Server v6.0 versions prior to 6.0.25, MongoDB Server v7.0 versions prior to 7.0.22 and MongoDB Server v8.0 versions prior to 8.0.12	2025-09-05	6.5	CVE-2025-10060
MongoDB Inc--MongoDB Server	An authorized user can cause a crash in the MongoDB Server through a specially crafted $group query. This vulnerability is related to the incorrect handling of certain accumulator functions when additional parameters are specified within the $group operation. This vulnerability could lead to denial of service if triggered repeatedly. This issue affects MongoDB Server v6.0 versions prior to 6.0.25, MongoDB Server v7.0 versions prior to 7.0.22, MongoDB Server v8.0 versions prior to 8.0.12 and MongoDB Server v8.1 versions prior to 8.1.2	2025-09-05	6.5	CVE-2025-10061

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mulscully--Today's Date Inserter	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mulscully Today's Date Inserter allows Stored XSS. This issue affects Today's Date Inserter: from n/a through 1.2.1.	2025-09-05	6.5	CVE-2025-48103
n/a--Langfuse	A security flaw has been discovered in Langfuse up to 3.88.0. Affected by this vulnerability is the function promptChangeEventSourcing of the file web/src/features/prompts/server/routers/promptRouter.ts of the component Webhook Handler. Performing manipulation results in server-side request forgery. The attack may be initiated remotely. A high degree of complexity is needed for the attack. The exploitation appears to be difficult. The exploit has been released to the public and may be exploited.	2025-09-01	5	CVE-2025-9799
n/a--RemoteClinic	A flaw has been found in RemoteClinic up to 2.0. This vulnerability affects unknown code of the file /staff/edit.php. Executing manipulation of the argument Last Name can lead to cross site scripting. The attack can be launched remotely. The exploit has been published and may be used.	2025-09-01	4.3	CVE-2025-9773
n/a--RemoteClinic	A vulnerability has been found in RemoteClinic up to 2.0. This issue affects some unknown processing of the file /patients/edit-patient.php. The manipulation of the argument Email leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-09-01	4.3	CVE-2025-9774
n/a--RemoteClinic	A vulnerability was detected in RemoteClinic 2.0. This vulnerability affects unknown code of the file /staff/profile.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely.	2025-09-01	4.7	CVE-2025-9802
Netcad--NetGIS Server	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Netcad NetGIS Server allows Reflected XSS.This issue affects NetGIS Server: from 5.2.4 through 22.08.2025.	2025-09-05	5.4	CVE-2025-8695
NVIDIA--ConnectX GA	NVIDIA ConnectX contains a vulnerability in the management interface, where an attacker with local access could cause incorrect authorization to modify the configuration. A successful exploit of this vulnerability might lead to denial of service, escalation of privileges, information disclosure, and data tampering.	2025-09-04	6.3	CVE-2025-23262
NVIDIA--HGX, DGX Hopper	NVIDIA HGX and DGX contain a vulnerability where a misconfiguration of the VBIOS could enable an attacker to set an unsafe debug access level. A successful exploit of this vulnerability might lead to denial of service.	2025-09-04	4.2	CVE-2025-23301
NVIDIA--HGX, DGX Hopper	NVIDIA HGX and DGX contain a vulnerability where a misconfiguration of the LS10 could enable an attacker to set an unsafe debug access level. A successful exploit of this vulnerability might lead to denial of service.	2025-09-04	4.2	CVE-2025-23302
NVIDIA--Mellanox DPDK 22.11	NVIDIA Mellanox DPDK contains a vulnerability in Poll Mode Driver (PMD), where an attacker on a VM in the system might be able to cause information disclosure and denial of service on the network interface.	2025-09-04	6.5	CVE-2025-23259
NVIDIA--NVOS	NVIDIA Cumulus Linux and NVOS products contain a vulnerability, where hashed user passwords are not properly suppressed in log files, potentially disclosing information to unauthorized users.	2025-09-04	5.5	CVE-2025-23261
optio--Optio Dentistry	The Optio Dentistry plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'optio-lightbox' shortcode in all versions up to, and including, 2.2 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.	2025-09-06	6.4	CVE-2025-9853
OTWthemes--Widgetize Pages Light	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OTWthemes Widgetize Pages Light allows Stored XSS. This issue affects Widgetize Pages Light: from n/a through 3.0.	2025-09-05	5.9	CVE-2025-58805

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
outline--outline	Outline is a service that allows for collaborative documentation. In versions 0.72.0 through 0.83.0, Outline introduced a feature which facilitates local file system storage capabilities as an optional file storage strategy. This feature allowed a CSP bypass as well as a ContentType bypass that might facilitate further attacks. In the case of self-hosting and using Outline FILE_STORAGE=local on the same domain as the Outline application, a malicious payload can be uploaded as a file attachment and bypass those CSP restrictions, allowing script execution within the context of another user. This is fixed in version 0.84.0.	2025-09-03	6.8	CVE-2025-58351
PalsCode--Support Genix	Missing Authorization vulnerability in PalsCode Support Genix allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Support Genix: from n/a through 1.4.23.	2025-09-03	5.3	CVE-2025-58635
Payoneer Checkout--Payoneer Checkout	Missing Authorization vulnerability in Payoneer Checkout Payoneer Checkout allows Content Spoofing. This issue affects Payoneer Checkout: from n/a through 3.4.0.	2025-09-05	5.3	CVE-2025-58795
peachpay--PeachPay Payments	Missing Authorization vulnerability in peachpay PeachPay Payments allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects PeachPay Payments: from n/a through 1.117.4.	2025-09-03	5.3	CVE-2025-58634
PHPGurukul--User Management System	A vulnerability was found in PHPGurukul User Management System 1.0. This impacts an unknown function of the file /admin/change-emailid.php. The manipulation of the argument uid results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	2025-09-01	6.3	CVE-2025-9756
Portabilis--i-Educar	A weakness has been identified in Portabilis i-Educar up to 2.10. The affected element is an unknown function of the file /module/TabelaArredondamento/edit. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	2025-09-05	6.3	CVE-2025-10011
Portabilis--i-Educar	A security vulnerability has been detected in Portabilis i-Educar up to 2.10. The impacted element is an unknown function of the file educar_historico_escolar_lst.php. Such manipulation of the argument ref_cod_aluno leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	2025-09-05	6.3	CVE-2025-10012
Portabilis--i-Educar	A vulnerability was detected in Portabilis i-Educar up to 2.10. This affects an unknown function of the file /exportacao-para-o-seb. Performing manipulation results in improper access controls. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2025-09-05	6.3	CVE-2025-10013
Portabilis--i-Educar	A flaw has been found in Portabilis i-Educar up to 2.10. This affects an unknown part of the file /enturmacao-em-lote/. This manipulation causes improper access controls. The attack is possible to be carried out remotely. The exploit has been published and may be used.	2025-09-07	6.3	CVE-2025-10070
Portabilis--i-Educar	A vulnerability has been found in Portabilis i-Educar up to 2.10. This vulnerability affects unknown code of the file /cancelar-enturmacao-em-lote/. Such manipulation leads to improper access controls. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	2025-09-07	6.3	CVE-2025-10071
Portabilis--i-Educar	A vulnerability was found in Portabilis i-Educar up to 2.10. This issue affects some unknown processing of the file /matricula/[ID_STUDENT]/enturmar/. Performing manipulation results in improper access controls. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	2025-09-07	6.3	CVE-2025-10072
Portabilis--i-Educar	A weakness has been identified in Portabilis i-Educar up to 2.10. This affects an unknown part of the file /module/Api/aluno of the component Matricula API. Executing manipulation can lead to improper authorization. It is possible to launch	2025-09-01	6.3	CVE-2025-9760

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the attack remotely. The exploit has been made available to the public and could be exploited.			
Portabilis--i-Educar	A vulnerability was determined in Portabilis i-Educar up to 2.10. Impacted is an unknown function of the file /module/Api/turma. Executing manipulation can lead to improper authorization. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-07	4.3	CVE-2025-10073
premiumbizthemes--Simple Price Calculator	Insertion of Sensitive Information Into Sent Data vulnerability in premiumbizthemes Simple Price Calculator allows Retrieve Embedded Sensitive Data. This issue affects Simple Price Calculator: from n/a through 1.3.	2025-09-05	6.5	CVE-2025-58872
PriceListo--Best Restaurant Menu by PriceListo	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PriceListo Best Restaurant Menu by PriceListo allows Stored XSS. This issue affects Best Restaurant Menu by PriceListo: from n/a through 1.4.3.	2025-09-05	6.5	CVE-2025-58812
properfraction--MailOptin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in properfraction MailOptin allows Stored XSS. This issue affects MailOptin: from n/a through 1.2.75.0.	2025-09-03	5.9	CVE-2025-58596
Property Hive--PropertyHive	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Property Hive PropertyHive allows Stored XSS. This issue affects PropertyHive: from n/a through 2.1.5.	2025-09-03	6.5	CVE-2025-58612
pt-guy--Content Views Post Grid & Filter, Recent Posts, Category Posts (Shortcode, Blocks, and Elementor Widgets)	The Content Views plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Grid and List widgets in all versions up to, and including, 4.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-06	6.4	CVE-2025-8722
pusheco--Pushe Web Push Notification	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pusheco Pushe Web Push Notification allows Stored XSS. This issue affects Pushe Web Push Notification: from n/a through 0.5.0.	2025-09-05	5.9	CVE-2025-58873
RadiusTheme--Classified Listing	Missing Authorization vulnerability in RadiusTheme Classified Listing allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Classified Listing: from n/a through 5.0.6.	2025-09-03	4.3	CVE-2025-58601
rainafarai--Notification for Telegram	Cross-Site Request Forgery (CSRF) vulnerability in rainafarai Notification for Telegram allows Cross Site Request Forgery. This issue affects Notification for Telegram: from n/a through 3.4.6.	2025-09-05	4.3	CVE-2025-58794
Ram Ratan Maurya--Stagtools	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ram Ratan Maurya Stagtools allows Stored XSS. This issue affects Stagtools: from n/a through 2.3.8.	2025-09-05	6.5	CVE-2025-58814
rbaer--Simple Matomo Tracking Code	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rbaer Simple Matomo Tracking Code allows Stored XSS. This issue affects Simple Matomo Tracking Code: from n/a through 1.1.0.	2025-09-03	5.9	CVE-2025-58630
Red Hat--Red Hat Build of Keycloak	A flaw was found in Keycloak. Keycloak's account console and other pages accept arbitrary text in the error_description query parameter. This text is directly rendered in error pages without validation or sanitization. While HTML encoding prevents XSS, an attacker can craft URLs with misleading messages (e.g., fake support phone numbers or URLs), which are displayed within the trusted Keycloak UI. This creates a phishing vector, potentially tricking users into contacting malicious actors.	2025-09-05	4.3	CVE-2025-10044

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in libsoup's caching mechanism, SoupCache, where the HTTP Vary header is ignored when evaluating cached responses. This header ensures that responses vary appropriately based on request headers such as language or authentication. Without this check, cached content can be incorrectly reused across different requests, potentially exposing sensitive user information. While the issue is unlikely to affect everyday desktop use, it could result in confidentiality breaches in proxy or multi-user environments.	2025-09-03	5.9	CVE-2025-9901
reimund--Compact Admin	Cross-Site Request Forgery (CSRF) vulnerability in reimund Compact Admin allows Cross Site Request Forgery. This issue affects Compact Admin: from n/a through 1.3.0.	2025-09-05	4.3	CVE-2025-58865
Remi Corson--Easy Download Media Counter	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Remi Corson Easy Download Media Counter allows Stored XSS. This issue affects Easy Download Media Counter: from n/a through 1.2.	2025-09-05	6.5	CVE-2025-58867
reubenthiessen--Translate This gTranslate Shortcode	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in reubenthiessen Translate This gTranslate Shortcode allows Stored XSS. This issue affects Translate This gTranslate Shortcode: from n/a through 1.0.	2025-09-05	6.5	CVE-2025-58880
RooCodeInc--Roo-Code	Roo Code is an AI-powered autonomous coding agent that lives in users' editors. Versions 3.25.23 and below contain a vulnerability where .rooignore protections could be bypassed using symlinks. This allows an attacker with write access to the workspace to trick the extension into reading files that were intended to be excluded. As a result, sensitive files such as .env or configuration files could be exposed. An attacker able to modify files within the workspace could gain unauthorized access to sensitive information by bypassing .rooignore rules. This could include secrets, configuration details, or other excluded project data. This is fixed in version 3.26.0.	2025-09-05	5.5	CVE-2025-58373
RumbleTalk--RumbleTalk Live Group Chat	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RumbleTalk RumbleTalk Live Group Chat allows Stored XSS. This issue affects RumbleTalk Live Group Chat: from n/a through 6.3.5.	2025-09-03	6.5	CVE-2025-58626
saadiqbal--Post SMTP WP SMTP Plugin with Email Logs and Mobile App for Failure Notifications Gmail SMTP, Office 365, Brevo, Mailgun, Amazon SES and more	The Post SMTP - WP SMTP Plugin with Email Logs and Mobile App for Failure Notifications - Gmail SMTP, Office 365, Brevo, Mailgun, Amazon SES and more plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_post_smtp_pro_option_callback' function in all versions up to, and including, 3.4.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to enable pro extensions.	2025-09-03	4.3	CVE-2025-9219
Samsung Mobile--Galaxy Store	Improper Access Control vulnerability in Galaxy Store prior to version 4.5.53.6 allows local attacker to access protected data using exported service.	2025-09-03	6.4	CVE-2023-21483
Samsung Mobile--S Assistant	Improper verification of intent by SamsungExceptionalBroadcastReceiver in S Assistant prior to version 9.3.2 allows local attackers to modify itinerary information.	2025-09-03	5.1	CVE-2025-21038
Samsung Mobile--S Assistant	Improper verification of intent by SystemExceptionalBroadcastReceiver in S Assistant prior to version 9.3.2 allows local attackers to modify itinerary information.	2025-09-03	5.1	CVE-2025-21039
Samsung Mobile--S Assistant	Improper verification of intent by ExternalBroadcastReceiver in S Assistant prior to version 9.3.2 allows local attackers to modify itinerary information.	2025-09-03	5.1	CVE-2025-21040
Samsung Mobile--Samsung Account	Improper URL input validation vulnerability in Samsung Account application prior to version 14.1.0.0 allows remote attackers to get sensitive information.	2025-09-03	5.4	CVE-2023-21481

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Samsung Mobile--Samsung Calendar	Improper access control in Samsung Calendar prior to version 12.5.06.5 in Android 14 and 12.6.01.12 in Android 15 allows physical attackers to access data across multiple user profiles.	2025-09-03	4.6	CVE-2025-21035
Samsung Mobile--Samsung Camera	Missing authorization vulnerability in Camera prior to versions 11.1.02.18 in Android 11, 12.1.03.8 in Android 12 and 13.1.01.4 in Android 13 allows physical attackers to install package through Galaxy store before completion of Setup wizard.	2025-09-03	6.1	CVE-2023-21482
Samsung Mobile--Samsung Mobile Devices	Improper input validation with Exynos Fastboot USB Interface prior to SMR Apr-2023 Release 1 allows a physical attacker to execute arbitrary code in bootloader.	2025-09-03	6.8	CVE-2023-21472
Samsung Mobile--Samsung Mobile Devices	Improper input validation with Exynos Fastboot USB Interface prior to SMR Apr-2023 Release 1 allows a physical attacker to execute arbitrary code in bootloader.	2025-09-03	6.8	CVE-2023-21473
Samsung Mobile--Samsung Mobile Devices	Intent redirection vulnerability in SecSettings prior to SMR Apr-2022 Release 1 allows attackers to access arbitrary file with system privilege.	2025-09-03	6.3	CVE-2023-21474
Samsung Mobile--Samsung Mobile Devices	Improper input validation vulnerability in TIGERF trustlet prior to SMR Apr-2023 Release 1 allows local attackers to access protected data.	2025-09-03	6	CVE-2023-21478
Samsung Mobile--Samsung Mobile Devices	Improper access control in ImsService prior to SMR Sep-2025 Release 1 allows local attackers to use the privileged APIs.	2025-09-03	6.8	CVE-2025-21031
Samsung Mobile--Samsung Mobile Devices	PendingIntent hijacking vulnerability in CertificatePolicy in framework prior to SMR Apr-2023 Release 1 allows local attackers to access contentProvider without proper permission.	2025-09-03	5.3	CVE-2023-21466
Samsung Mobile--Samsung Mobile Devices	Improper access control vulnerability in Telephony prior to SMR Apr-2023 Release 1 allows attackers to access files with escalated permission.	2025-09-03	5.9	CVE-2023-21468
Samsung Mobile--Samsung Mobile Devices	Improper authorization in Smart suggestions prior to SMR Apr-2023 Release 1 in Android 13 and 4.1.01.0 in Android 12 allows remote attackers to register a schedule.	2025-09-03	5.3	CVE-2023-21479
Samsung Mobile--Samsung Mobile Devices	Improper access control in MARsExemptionManager prior to SMR Sep-2025 Release 1 allows local attackers to be excluded from background execution management.	2025-09-03	5.1	CVE-2025-21025
Samsung Mobile--Samsung Mobile Devices	Improper verification of intent by broadcast receiver in ImsService prior to SMR Sep-2025 Release 1 allows local attackers to temporarily disable the SIM.	2025-09-03	5.1	CVE-2025-21027
Samsung Mobile--Samsung Mobile Devices	Improper privilege management in ThemeManager prior to SMR Sep-2025 Release 1 allows local privileged attackers to reuse trial items.	2025-09-03	5.5	CVE-2025-21028
Samsung Mobile--Samsung Mobile Devices	Improper access control in One UI Home prior to SMR Sep-2025 Release 1 allows physical attackers to bypass Kiosk mode under limited conditions.	2025-09-03	5.9	CVE-2025-21032
Samsung Mobile--Samsung Mobile Devices	Improper access control vulnerability in retrieveExternalProxy in MiscPolicy prior to SMR Nov-2022 Release 1 allows local attacker to access to Proxy information.	2025-09-04	4.3	CVE-2022-39888

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Samsung Mobile--Samsung Mobile Devices	Error in 3GPP specification implementation in Exynos baseband prior to SMR Apr-2023 Release 1 allows incorrect handling of unencrypted message.	2025-09-03	4.6	CVE-2023-21467
Samsung Mobile--Samsung Mobile Devices	Improper access control vulnerability in SLocation prior to SMR Apr-2022 Release 1 allows local attackers to get device location information using com.samsung.android.wifi.GEOFENCE action.	2025-09-03	4	CVE-2023-21469
Samsung Mobile--Samsung Mobile Devices	Improper access control vulnerability in SLocation prior to SMR Apr-2022 Release 1 allows local attackers to get device location information using com.samsung.android.wifi.NETWORK_LOCATION action.	2025-09-03	4	CVE-2023-21470
Samsung Mobile--Samsung Mobile Devices	Improper access control vulnerability in SemClipboard prior to SMR Apr-2023 Release 1 allows attackers to read arbitrary files with system permission.	2025-09-03	4	CVE-2023-21471
Samsung Mobile--Samsung Mobile Devices	Improper handling of insufficient permission in ImsService prior to SMR Sep-2025 Release 1 allows local attackers to interrupt the call.	2025-09-03	4	CVE-2025-21026
Samsung Mobile--Samsung Mobile Devices	Improper handling of insufficient permission in System UI prior to SMR Sep-2025 Release 1 allows local attackers to send arbitrary replies to messages from the cover display.	2025-09-03	4	CVE-2025-21029
Samsung Mobile--Samsung Mobile Devices	Improper handling of insufficient permission in AppPrelaunchManagerService prior to SMR Sep-2025 Release 1 in Chinese Android 15 allows local attackers to execute arbitrary application in the background.	2025-09-03	4.3	CVE-2025-21030
Samsung Mobile--Samsung Mobile Devices	Improper access control in ContactProvider prior to SMR Sep-2025 Release 1 allows local attackers to access sensitive information.	2025-09-03	4	CVE-2025-21033
Samsung Mobile--Samsung Mobile Devices	Out-of-bounds write in libsavsvc.so prior to SMR Sep-2025 Release 1 allows local attackers to potentially execute arbitrary code.	2025-09-03	4	CVE-2025-21034
Samsung Mobile--Samsung Notes	Improper access control in Samsung Notes prior to version 4.4.30.63 allows local privileged attackers to access exported note files. User interaction is required for triggering this vulnerability.	2025-09-03	5	CVE-2025-21036
Samsung Mobile--SamsungNotes	Improper access control in Samsung Notes prior to version 4.4.30.63 allows physical attackers to access data across multiple user profiles. User interaction is required for triggering this vulnerability.	2025-09-03	4.1	CVE-2025-21037
Samsung Mobile--Secure Folder	Insecure Storage of Sensitive Information in Secure Folder prior to Android 16 allows local attackers to access sensitive information.	2025-09-03	6.2	CVE-2025-21041
ScriptAndTools--Real Estate Management System	A weakness has been identified in ScriptAndTools Real Estate Management System 1.0. Impacted is an unknown function of the file register.php. This manipulation of the argument uimage causes unrestricted upload. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	2025-09-03	6.3	CVE-2025-9847
SdeWijs--Zoomify embed for WP	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SdeWijs Zoomify embed for WP allows Stored XSS. This issue affects Zoomify embed for WP: from n/a through 1.5.2.	2025-09-05	6.5	CVE-2025-58863
Shiful H--SS Font Awesome Icon	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shiful H SS Font Awesome Icon allows Stored XSS. This issue affects SS Font Awesome Icon: from n/a through 4.1.3.	2025-09-05	6.5	CVE-2025-58837

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Simasicher--SimaCookie	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Simasicher SimaCookie allows Stored XSS. This issue affects SimaCookie: from n/a through 1.3.2.	2025-09-05	6.5	CVE-2025-58868
Simasicher--SimaCookie	Cross-Site Request Forgery (CSRF) vulnerability in Simasicher SimaCookie allows Stored XSS. This issue affects SimaCookie: from n/a through 1.3.2.	2025-09-05	6.5	CVE-2025-58869
SimStudioAI--sim	A weakness has been identified in SimStudioAI sim up to ed9b9ad83f1a7c61f4392787fb51837d34eeb0af. Affected by this issue is the function Import of the file apps/sim/app/api/files/upload/route.ts of the component HTML File Parser. Executing manipulation of the argument File can lead to unrestricted upload. The attack may be launched remotely. The exploit has been made available to the public and could be exploited. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. This patch is called 45372aece5e05e04b417442417416a52e90ba174. A patch should be applied to remediate this issue.	2025-09-01	6.3	CVE-2025-9800
SimStudioAI--sim	A vulnerability was found in SimStudioAI sim up to 51b1e97fa22c48d144aef75f8ca31a74ad2cfed2. This issue affects some unknown processing of the file apps/sim/app/api/proxy/image/route.ts. The manipulation results in server-side request forgery. The attack may be performed from remote. The exploit has been made public and could 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 patch is identified as 3424a338b763115f0269b209e777608e4cd31785. Applying a patch is advised to resolve this issue.	2025-09-02	6.3	CVE-2025-9805
SimStudioAI--sim	A security vulnerability has been detected in SimStudioAI sim up to ed9b9ad83f1a7c61f4392787fb51837d34eeb0af. This affects an unknown part. The manipulation of the argument filePath leads to path traversal. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The identifier of the patch is 45372aece5e05e04b417442417416a52e90ba174. To fix this issue, it is recommended to deploy a patch.	2025-09-01	5.4	CVE-2025-9801
sizam--REHub - Price Comparison, Multi Vendor Marketplace Wordpress Theme	The REHub - Price Comparison, Multi Vendor Marketplace Wordpress Theme theme for WordPress is vulnerable to Information Exposure in all versions up to, and including, 19.9.7 via the 'ajax_action_re_getfullcontent' function due to insufficient restrictions on which posts can be included. This makes it possible for unauthenticated attackers to extract data from password protected posts that they should not have access to.	2025-09-06	5.3	CVE-2025-7368
sjaved--Easy Social Feed Social Photos Gallery Post Feed Like Box	The Easy Social Feed - Social Photos Gallery - Post Feed - Like Box plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `data-caption` and `data-linktext` parameters in all versions up to, and including, 6.6.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-06	6.4	CVE-2025-6067
smub--aThemes Addons for Elementor	The aThemes Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown widget in all versions up to, and including, 1.1.2 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.	2025-09-06	6.4	CVE-2025-8149

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
snagysandor--Parallax Scrolling Enllax.js	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in snagysandor Parallax Scrolling Enllax.js allows Stored XSS. This issue affects Parallax Scrolling Enllax.js: from n/a through 0.0.6.	2025-09-05	6.5	CVE-2025-58830
snagysandor--Parallax Scrolling Enllax.js	Cross-Site Request Forgery (CSRF) vulnerability in snagysandor Parallax Scrolling Enllax.js allows Cross Site Request Forgery. This issue affects Parallax Scrolling Enllax.js: from n/a through 0.0.6.	2025-09-05	4.3	CVE-2025-58831
sonalsinha21--SKT Addons for Elementor	The SKT Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 3.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-06	6.4	CVE-2025-8564
Spiffy Plugins--WP Flow Plus	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Spiffy Plugins WP Flow Plus allows Stored XSS. This issue affects WP Flow Plus: from n/a through 5.2.5.	2025-09-03	5.9	CVE-2025-58625
Steve Truman--WP Email Template	Cross-Site Request Forgery (CSRF) vulnerability in Steve Truman WP Email Template allows Cross Site Request Forgery. This issue affects WP Email Template: from n/a through 2.8.3.	2025-09-05	4.3	CVE-2025-58800
stiofansisland--UsersWP Front-end login form, User Registration, User Profile & Members Directory plugin for WP	The UsersWP - Front-end login form, User Registration, User Profile & Members Directory plugin for WordPress plugin for WordPress is vulnerable to time-based SQL Injection via the 'upload_file_remove' function and 'htmlvar' parameter in all versions up to, and including, 1.2.44 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-06	6.5	CVE-2025-10003
streamweasels--StreamWeasels Kick Integration	The StreamWeasels Kick Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'vodsChannel' parameter in all versions up to, and including, 1.1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-06	6.4	CVE-2025-9442
Stylemix--MasterStudy LMS	Missing Authorization vulnerability in Stylemix MasterStudy LMS allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects MasterStudy LMS: from n/a through 3.6.15.	2025-09-05	6.5	CVE-2025-54744
Sudar Muthu--WP Github Gist	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sudar Muthu WP Github Gist allows Stored XSS. This issue affects WP Github Gist: from n/a through 0.5.	2025-09-05	6.5	CVE-2025-58875
Sunnet--eHRD CTMS	The eHRD developed by Sunnet has a Reflected Cross-site Scripting vulnerability, allowing unauthenticated remote attackers to execute arbitrary JavaScript codes in user's browser through phishing attacks.	2025-09-01	6.1	CVE-2025-9567
Sunnet--eHRD CTMS	The eHRD developed by Sunnet has a Reflected Cross-site Scripting vulnerability, allowing unauthenticated remote attackers to execute arbitrary JavaScript codes in user's browser through phishing attacks.	2025-09-01	6.1	CVE-2025-9568
Sunnet--eHRD CTMS	The eHRD developed by Sunnet has a Reflected Cross-site Scripting vulnerability, allowing unauthenticated remote attackers to execute arbitrary JavaScript codes in user's browser through phishing attacks.	2025-09-01	6.1	CVE-2025-9569
Sunnet--eHRD CTMS	The eHRD CTMS developed by Sunnet has an Arbitrary File Reading vulnerability, allowing remote attackers with administrator privileges to exploit Relative Path Traversal to download arbitrary system files.	2025-09-01	4.9	CVE-2025-9570

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Surfer--Surfer	Missing Authorization vulnerability in Surfer Surfer allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Surfer: from n/a through 1.6.4.574.	2025-09-03	5.3	CVE-2025-58603
SwiftNinjaPro--Developer Tools Blocker	Cross-Site Request Forgery (CSRF) vulnerability in SwiftNinjaPro Developer Tools Blocker allows Cross Site Request Forgery. This issue affects Developer Tools Blocker: from n/a through 3.2.1.	2025-09-05	5.4	CVE-2025-58818
Tan Nguyen--Instant Locations	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tan Nguyen Instant Locations allows Stored XSS. This issue affects Instant Locations: from n/a through 1.0.	2025-09-05	5.9	CVE-2025-58886
techjewel--Fluent Forms Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder	The Fluent Forms - Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder plugin for WordPress is vulnerable to PHP Object Injection in versions 5.1.16 to 6.1.1 via deserialization of untrusted input in the parseUserProperties function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject a PHP Object. The additional presence of a POP chain allows attackers to read arbitrary files. If allow_url_include is enabled on the server, remote code execution is possible. While the vendor patched this issue in version 6.1.0, the patch caused a fatal error in the vulnerable code, due to a missing class import, so we consider 6.1.2 to be the most complete and best patched version	2025-09-02	6.5	CVE-2025-9260
The African Boss--Get Cash	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in The African Boss Get Cash allows Stored XSS. This issue affects Get Cash: from n/a through 3.2.2.	2025-09-05	6.5	CVE-2025-58823
ThemeArile--Consultstreet	Missing Authorization vulnerability in ThemeArile Consultstreet allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Consultstreet: from n/a through 3.0.0.	2025-09-05	4.3	CVE-2025-58813
themefusecom--Brizy	Missing Authorization vulnerability in themefusecom Brizy allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Brizy: from n/a through 2.7.12.	2025-09-03	4.3	CVE-2025-58594
themehunk--Vayu Blocks Website Builder for the Block Editor	The Vayu Blocks - Website Builder for the Block Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple attributes in the Lottie block in all versions up to, and including, 1.3.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-03	6.4	CVE-2025-9378
Themeisle--Orbit Fox by ThemeIsle	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeisle Orbit Fox by ThemeIsle allows Stored XSS. This issue affects Orbit Fox by ThemeIsle: from n/a through 3.0.0.	2025-09-03	6.5	CVE-2025-58593
themejunkie--Recent Posts Widget Extended	The Recent Posts Widget Extended plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'rpwe' shortcode 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.	2025-09-06	6.4	CVE-2025-6757
themelocation--Custom WooCommerce Checkout Fields Editor	Cross-Site Request Forgery (CSRF) vulnerability in themelocation Custom WooCommerce Checkout Fields Editor allows Cross Site Request Forgery. This issue affects Custom WooCommerce Checkout Fields Editor: from n/a through 1.3.4.	2025-09-05	4.3	CVE-2025-58799
ThemeMove--Makeaholic	Missing Authorization vulnerability in ThemeMove Makeaholic allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Makeaholic: from n/a through 1.8.5.	2025-09-03	5.3	CVE-2025-58210

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Themepoints--Carousel Ultimate	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Carousel Ultimate allows Stored XSS. This issue affects Carousel Ultimate: from n/a through 1.8.	2025-09-05	5.9	CVE-2025-58820
themifyme--Themify Popup	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themifyme Themify Popup allows Stored XSS. This issue affects Themify Popup: from n/a through 1.4.4.	2025-09-05	6.5	CVE-2025-58787
Thomas Harris--Search Cloud One	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Thomas Harris Search Cloud One allows Stored XSS. This issue affects Search Cloud One: from n/a through 2.2.5.	2025-09-05	5.9	CVE-2025-58883
Tickera--Tickera	Cross-Site Request Forgery (CSRF) vulnerability in Tickera Tickera allows Cross Site Request Forgery. This issue affects Tickera: from n/a through 3.5.5.6.	2025-09-03	4.3	CVE-2025-58611
tigroumeow--AI Engine	The AI Engine plugin for WordPress is vulnerable to unauthorized access and loss of data due to a missing capability check on the rest_list and delete_files functions in all versions up to, and including, 2.9.5. This makes it possible for unauthenticated attackers to list and delete files uploaded by other users.	2025-09-03	6.5	CVE-2025-8268
Tikolan--FW Anker	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tikolan FW Anker allows Stored XSS. This issue affects FW Anker: from n/a through 1.2.6.	2025-09-05	6.5	CVE-2025-58836
Tomdever--wpForo Forum	Authorization Bypass Through User-Controlled Key vulnerability in Tomdever wpForo Forum allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects wpForo Forum: from n/a through 2.4.6.	2025-09-03	4.3	CVE-2025-58597
TOTOLINK--X5000R	A vulnerability was found in TOTOLINK X5000R 9.1.0cu.2415_B20250515. This affects the function sub_410C34 of the file /cgi-bin/cstecgi.cgi. Performing manipulation of the argument pid results in command injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	2025-09-03	6.3	CVE-2025-9934
tychesoftwares--Order Delivery Date for WooCommerce	Missing Authorization vulnerability in tychesoftwares Order Delivery Date for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Order Delivery Date for WooCommerce: from n/a through 4.1.0.	2025-09-03	4.3	CVE-2025-58599
typelevel--fs2	fs2 is a compositional, streaming I/O library for Scala. Versions 3.12.2 and lower and 3.13.0-M1 through 3.13.0-M6 is vulnerable to denial of service attacks though TLS sessions using fs2-io on the JVM using the fs2.io.net.tls package. When establishing a TLS session, if one side of the connection shuts down `write` while the peer side is awaiting more data to progress the TLS handshake, the peer side will spin loop on the socket read, fully utilizing a CPU. The CPU is consumed until the overall connection is closed, potentially shutting down a fs2-io powered server. This issue is fixed in versions 3.12.1 and 3.13.0-M7.	2025-09-05	5.3	CVE-2025-58369
usamafarooq--Woocommerce Gifts Product	Cross-Site Request Forgery (CSRF) vulnerability in usamafarooq Woocommerce Gifts Product allows Cross Site Request Forgery. This issue affects Woocommerce Gifts Product: from n/a through 1.0.0.	2025-09-05	6.5	CVE-2025-58878
ux-themes--Flatsome	The Flatsome Theme for WordPress is vulnerable to Stored Cross-Site Scripting via the theme's shortcodes in all versions up to, and including, 3.20.0 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.	2025-09-05	6.4	CVE-2025-8684
VillaTheme--HAPPY	Missing Authorization vulnerability in VillaTheme HAPPY allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects HAPPY: from n/a through 1.0.6.	2025-09-05	6.5	CVE-2025-53571

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Vincent Boiardt--Easy Flash Embed	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vincent Boiardt Easy Flash Embed allows Stored XSS. This issue affects Easy Flash Embed: from n/a through 1.0.	2025-09-05	6.5	CVE-2025-48105
VW THEMES--Ibtana Ecommerce Product Addons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VW THEMES Ibtana - Ecommerce Product Addons allows DOM-Based XSS. This issue affects Ibtana - Ecommerce Product Addons: from n/a through 0.4.7.4.	2025-09-05	6.5	CVE-2025-58786
w1zzard--Simple Text Slider	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in w1zzard Simple Text Slider allows Stored XSS. This issue affects Simple Text Slider: from n/a through 1.0.5.	2025-09-05	6.5	CVE-2025-58882
webriti--Shk Corporate	Missing Authorization vulnerability in webriti Shk Corporate allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Shk Corporate: from n/a through 2.4.1.1.	2025-09-05	4.3	CVE-2025-58824
webvitaly--Search by Google	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly Search by Google allows Stored XSS. This issue affects Search by Google: from n/a through 1.9.	2025-09-05	5.9	CVE-2025-58832
whiteshadow--Admin Menu Editor	The Admin Menu Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'placeholder' parameter in all versions up to, and including, 1.14 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.	2025-09-06	6.4	CVE-2025-9493
WP Chill--Gallery PhotoBlocks	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Gallery PhotoBlocks allows Stored XSS. This issue affects Gallery PhotoBlocks: from n/a through 1.3.1.	2025-09-03	6.5	CVE-2025-58610
WP CodeUs--Ultimate Client Dash	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP CodeUs Ultimate Client Dash allows Stored XSS. This issue affects Ultimate Client Dash: from n/a through 4.6.	2025-09-05	5.9	CVE-2025-58811
WP Delicious--WP Delicious	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Delicious WP Delicious allows Stored XSS. This issue affects WP Delicious: from n/a through 1.8.7.	2025-09-03	6.5	CVE-2025-58605
WPBean--WPB Elementor Addons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBean WPB Elementor Addons allows Stored XSS. This issue affects WPB Elementor Addons: from n/a through 1.6.	2025-09-05	6.5	CVE-2025-58793
WPBean--WPB Image Widget	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBean WPB Image Widget allows Stored XSS. This issue affects WPB Image Widget: from n/a through 1.1.	2025-09-05	6.5	CVE-2025-58858
wpdever--WP Notification Bell	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdever WP Notification Bell allows Stored XSS. This issue affects WP Notification Bell: from n/a through 1.4.5.	2025-09-05	5.9	CVE-2025-58821
wpeverest--User Registration & Membership Custom Registration Form Builder, Custom Login Form, User Profile, Content Restriction & Membership Plugin	The User Registration & Membership plugin for WordPress is vulnerable to SQL Injection via the 's' parameter in version 4.3.0. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-06	4.9	CVE-2025-9085

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WPKube--Authors List	Cross-Site Request Forgery (CSRF) vulnerability in WPKube Authors List allows Cross Site Request Forgery. This issue affects Authors List: from n/a through 2.0.6.1.	2025-09-05	4.3	CVE-2025-58792
WPKube--Kiwi	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPKube Kiwi allows Stored XSS. This issue affects Kiwi: from n/a through 2.1.8.	2025-09-05	6.5	CVE-2025-58790
xujeff--tianti	A vulnerability has been found in xujeff tianti å¤©æ¢¯ up to 2.3. The impacted element is the function ajaxUploadFile of the file src/main/java/com/jeff/tianti/controller/UploadController.java. The manipulation of the argument upfile leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2025-09-01	6.3	CVE-2025-9795
yydevelopment--Mobile Contact Line	Missing Authorization vulnerability in yydevelopment Mobile Contact Line allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Mobile Contact Line: from n/a through 2.4.0.	2025-09-03	4.3	CVE-2025-58622
Zakir--Smooth Accordion	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zakir Smooth Accordion allows Stored XSS. This issue affects Smooth Accordion: from n/a through 2.1.	2025-09-05	6.5	CVE-2025-58838
ZEEN101--IssueM	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZEEN101 IssueM allows DOM-Based XSS. This issue affects IssueM: from n/a through 2.9.0.	2025-09-03	5.9	CVE-2025-58631
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30254, 20.005.30774, 25.001.20672 and earlier are affected by a Violation of Secure Design Principles vulnerability that could result in a security feature bypass. Exploitation of this issue does not require user interaction, and scope is unchanged.	2025-09-09	4	CVE-2025-54255
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access.	2025-09-09	6.5	CVE-2025-54246
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access.	2025-09-09	6.5	CVE-2025-54247
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to manipulate server-side requests and bypass security controls allowing unauthorized read access.	2025-09-09	6.5	CVE-2025-54249
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. This could result in bypassing security features within the application. Exploitation of this issue requires user interaction in that a victim must browse to the page containing the vulnerable field.	2025-09-09	5.4	CVE-2025-54252
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A high-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access.	2025-09-09	4.9	CVE-2025-54250
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an XML Injection vulnerability that could result in a Security feature bypass. A low-	2025-09-09	4.3	CVE-2025-54251

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privileged attacker could leverage this vulnerability to manipulate XML queries and gain limited unauthorized write access.			
Adobe--After Effects	After Effects versions 25.3, 24.6.7 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure, potentially disclosing sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-09-09	5.5	CVE-2025-54239
Adobe--After Effects	After Effects versions 25.3, 24.6.7 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure, potentially disclosing sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-09-09	5.5	CVE-2025-54240
Adobe--After Effects	After Effects versions 25.3, 24.6.7 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure, potentially disclosing sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-09-09	5.5	CVE-2025-54241
Alexandre Froger--WP Weixin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alexandre Froger WP Weixin allows Stored XSS. This issue affects WP Weixin: from n/a through 1.3.16.	2025-09-09	5.9	CVE-2025-30875
andy_moyle--Church Admin	Missing Authorization vulnerability in andy_moyle Church Admin. This issue affects Church Admin: from n/a through 5.0.9.	2025-09-09	4.3	CVE-2025-39553
AntoineH--Football Pool	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AntoineH Football Pool allows Stored XSS. This issue affects Football Pool: from n/a through 2.12.6.	2025-09-09	6.5	CVE-2025-58987
arjunthakur--Duplicate Page and Post	The Duplicate Page and Post plugin for WordPress is vulnerable to time-based SQL Injection via the 'meta_key' parameter in all versions up to, and including, 2.9.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-10	6.5	CVE-2025-6189
awesomesupport--Awesome Support	Missing Authorization vulnerability in awesomesupport Awesome Support. This issue affects Awesome Support: from n/a through 6.3.4.	2025-09-09	5.3	CVE-2025-53340
AxxonSoft--AxxonNet ARP Agent	Insertion of Sensitive Information into Log File (CWE-532) in the ARP Agent component in AxxonSoft Axxon One / AxxonNet 2.0.4 and earlier on Windows platforms allows a local attacker to obtain plaintext credentials via reading TRACE log files containing serialized JSON with passwords.	2025-09-10	5.5	CVE-2025-10221
AxxonSoft--AxxonOne	Insufficient Session Expiration (CWE-613) in the Web Admin Panel in AxxonSoft Axxon One prior to 2.0.3 on Windows allows a local or remote authenticated attacker to retain access with removed privileges via continued use of an unexpired session token until natural expiration.	2025-09-10	5.4	CVE-2025-10223
AxxonSoft--AxxonOne	Improper Authentication (CWE-287) in the LDAP authentication engine in AxxonSoft Axxon One 2.0.2 and earlier on Windows allows a remote authenticated user to be denied access or misassigned roles via incorrect evaluation of nested LDAP group memberships during login.	2025-09-10	5.4	CVE-2025-10224
AxxonSoft--AxxonOne	Missing Encryption of Sensitive Data (CWE-311) in the Object Archive component in AxxonSoft Axxon One before 2.0.8 on Windows and Linux allows a local attacker with access to exported storage or stolen physical drives to extract sensitive archive data in plaintext via lack of encryption at rest.	2025-09-10	4.6	CVE-2025-10227

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
azurecurve--azurecurve BBCode	The azurecurve BBCode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'url' shortcode in all versions up to, and including, 2.0.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-11	6.4	CVE-2025-8398
Baicells--EG7035E-M11	CWE-79 Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')	2025-09-09	6.1	CVE-2025-55054
Baicells--NEUTRINO430, NOVA436Q, NOVA430e/430i, NOVA846, NOVA246, NOVA243, NOVA233, NOVA227	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	2025-09-09	4.3	CVE-2025-55052
Baicells--NOVA430e/430i, NOVA436Q, NEUTRINO430, NOVA846	CWE-328: Use of Weak Hash	2025-09-09	6.5	CVE-2025-55053
BerqWP--BerqWP	Missing Authorization vulnerability in BerqWP BerqWP allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects BerqWP: from n/a through 2.2.53.	2025-09-09	5.3	CVE-2025-58979
bessermitfahren--Mitfahrgelegenheit	The Mitfahrgelegenheit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'date' parameter in all versions up to, and including, 1.1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-11	6.4	CVE-2025-8392
binary-husky--gpt_academic	A vulnerability has been found in binary-husky gpt_academic up to 3.91. Impacted is the function merge_tex_files_ of the file crazy_functions/latex_fns/latex_toolbox.py of the component LaTeX File Handler. Such manipulation of the argument \input{} leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-11	4.3	CVE-2025-10236
bmarshall511--Jobify	The Jobify plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'keyword' parameter in all versions up to, and including, 1.4.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-11	6.4	CVE-2025-8318
catfolders--CatFolders Tame Your WordPress Media Library by Category	The CatFolders - Tame Your WordPress Media Library by Category plugin for WordPress is vulnerable to time-based SQL Injection via the CSV Import contents in all versions up to, and including, 2.5.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-11	6.5	CVE-2025-9776
cbutlerjr--WP-Members	The The WP-Members Membership Plugin plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 3.5.4.2. This is due to the software allowing users to execute an action that does not properly	2025-09-09	5	CVE-2025-9489

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Membership Plugin	validate a value before running do_shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes.			
cdevroe--unmark	A vulnerability was detected in cdevroe unmark up to 1.9.3. This affects an unknown part of the file /application/controllers/Marks.php. The manipulation of the argument url results in server-side request forgery. The attack may be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	6.3	CVE-2025-10329
cdevroe--unmark	A flaw has been found in cdevroe unmark up to 1.9.3. This vulnerability affects unknown code of the file application/views/layouts/topbar/searchform.php. This manipulation of the argument q causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	4.3	CVE-2025-10330
Checkmarx--1.0.3	'sanitize-html' prior to version 1.0.3 is vulnerable to Cross-site Scripting (XSS). The function 'naughtyHref' doesn't properly validate the hyperreference (`href`) attribute in anchor tags (`<a>`), allowing bypasses that contain different casings, whitespace characters, or hexadecimal encodings.	2025-09-08	6.1	CVE-2014-125128
Checkmarx--1.0.3	`sanitize-html` prior to version 2.0.0-beta is vulnerable to Cross-site Scripting (XSS). The `sanitizeHtml()` function in `index.js` does not sanitize content when using the custom `transformTags` option, which is intended to convert attribute values into text. As a result, malicious input can be transformed into executable code.	2025-09-08	6.1	CVE-2019-25225
Cisco--Cisco IOS XR Software	A vulnerability in the installation process of Cisco IOS XR Software could allow an authenticated, local attacker to bypass Cisco IOS XR Software image signature verification and load unsigned software on an affected device. To exploit this vulnerability, the attacker must have root-system privileges on the affected device. This vulnerability is due to incomplete validation of files during the installation of an .iso file. An attacker could exploit this vulnerability by modifying contents of the .iso image and then installing and activating it on the device. A successful exploit could allow the attacker to load an unsigned file as part of the image activation process.	2025-09-10	6	CVE-2025-20248
Cisco--Cisco IOS XR Software	A vulnerability in the management interface access control list (ACL) processing feature in Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass configured ACLs for the SSH, NetConf, and gRPC features. This vulnerability exists because management interface ACLs have not been supported on Cisco IOS XR Software Packet I/O infrastructure platforms for Linux-handled features such as SSH, NetConf, or gRPC. An attacker could exploit this vulnerability by attempting to send traffic to an affected device. A successful exploit could allow the attacker to bypass an ingress ACL that is applied on the management interface of the affected device.	2025-09-10	5.3	CVE-2025-20159
codesiddhant--Jasmin Ransomware	A vulnerability was determined in codesiddhant Jasmin Ransomware up to 1.0.1. This vulnerability affects unknown code of the file /handshake.php. This manipulation of the argument machine_name/computer_user/os/date/time/ip/location/systemid/password causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-14	6.3	CVE-2025-10387
cssigniterteam--Elements Plus!	The Elements Plus! plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Image Comparison, HotSpot Plus, and Google Maps widgets in all versions up to, and including, 2.16.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-11	6.4	CVE-2025-8689

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cyberchimps--Responsive Addons for Elementor Free Elementor Addons Plugin and Elementor Templates	The Responsive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 1.7.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-11	6.4	CVE-2025-8215
D-Link--DIR-823x	A vulnerability was detected in D-Link DIR-823x up to 250416. The affected element is an unknown function of the file /goform/diag_ping. Performing manipulation of the argument target_addr results in command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	2025-09-14	6.3	CVE-2025-10401
D-Link--DIR-852	A vulnerability was identified in D-Link DIR-852 up to 1.00CN B09. Affected by this vulnerability is the function phpcgi_main of the file /getcfg.php of the component Device Configuration Handler. Such manipulation leads to information disclosure. The attack may be performed from remote. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-09-08	5.3	CVE-2025-10093
datahihi1--tiny-env	TinyEnv is an environment variable loader for PHP applications. In versions 1.0.1, 1.0.2, 1.0.9, and 1.0.10, TinyEnv did not require the `.env` file to exist when loading environment variables. This could lead to unexpected behavior where the application silently ignores missing configuration, potentially causing insecure defaults or deployment misconfigurations. The issue has been fixed in version 1.0.11. All users should upgrade to 1.0.11 or later. As a workaround, users can manually verify the existence of the `.env` file before initializing TinyEnv.	2025-09-09	5.1	CVE-2025-58758
datahihi1--tiny-env	TinyEnv is an environment variable loader for PHP applications. In versions 1.0.9 and 1.0.10, TinyEnv did not properly strip inline comments inside .env values. This could lead to unexpected behavior or misconfiguration, where variables contain unintended characters (including # or comment text). Applications depending on strict environment values may expose logic errors, insecure defaults, or failed authentication. The issue is fixed in v1.0.11. Users should upgrade to the latest patched version. As a temporary workaround, avoid using inline comments in .env files, or sanitize loaded values manually.	2025-09-09	5.1	CVE-2025-58759
dejocar--Side Slide Responsive Menu	The Side Slide Responsive Menu plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-12	6.1	CVE-2025-9880
Dell--PowerProtect Data Manager	Dell PowerProtect Data Manager, version(s) 19.19 and 19.20, Hyper-V contain(s) a Plaintext Storage of a Password vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to gain unauthorized access with privileges of the compromised account.	2025-09-10	5	CVE-2025-43938
Dell--PowerProtect Data Manager	Dell PowerProtect Data Manager, version(s) 19.19 and 19.20, Hyper-V contain(s) a Path Traversal: '.../...//' vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Filesystem access for attacker.	2025-09-10	4.4	CVE-2025-43886
Dell--PowerScale OneFS	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an improper privilege management vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.	2025-09-08	6.7	CVE-2025-43722
Display Painis--TGA	A security flaw has been discovered in Display PainÃ©is TGA up to 7.1.41. Affected by this issue is some unknown functionality of the file /gallery/rename of the component Galeria Page. The manipulation of the argument current_folder results	2025-09-11	4.3	CVE-2025-10245

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in path traversal. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.			
DJI--Mavic Spark	A weakness has been identified in DJI Mavic Spark, Mavic Air and Mavic Mini 01.00.0500. Affected is an unknown function of the component Telemetry Channel. Executing manipulation can lead to use of hard-coded cryptographic key . The attacker needs to be present on the local network. A high complexity level is associated with this attack. The exploitability is told to be difficult. The exploit has been made available to the public and could be exploited. This vulnerability only affects products that are no longer supported by the maintainer.	2025-09-11	5	CVE-2025-10250
dontcare--Admin in English with Switch	The Admin in English with Switch plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1. This is due to missing or incorrect nonce validation on the enable_eng function. This makes it possible for unauthenticated attackers to modify administrator language settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-11	4.3	CVE-2025-9623
dpgaspar--Flask-AppBuilder	Flask-AppBuilder is an application development framework. Prior to version 4.8.1, when Flask-AppBuilder is configured to use OAuth, LDAP, or other non-database authentication methods, the password reset endpoint remains registered and accessible, despite not being displayed in the user interface. This allows an enabled user to reset their password and be able to create JWT tokens even after the user is disabled on the authentication provider. Users should upgrade to Flask-AppBuilder version 4.8.1 or later to receive a fix. If immediate upgrade is not possible, manually disable password reset routes in the application configuration; implement additional access controls at the web server or proxy level to block access to the reset my password URL; and/or monitor for suspicious password reset attempts from disabled accounts.	2025-09-11	6.5	CVE-2025-58065
edsteep--Seo Monster	The Seo Monster plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.3.3. This is due to missing or incorrect nonce validation on the check_integration() function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-11	6.1	CVE-2025-9620
eideasy--eID Easy	The eID Easy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 4.9.3 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.	2025-09-11	6.4	CVE-2025-9128
elangovan--Embed Google Datastudio	The Embed Google Datastudio plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'egds' shortcode in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-12	6.4	CVE-2025-9877
elunez--eladmin	A vulnerability was identified in elunez eladmin up to 2.7. This affects the function queryErrorLogDetail of the file /api/logs/error/1 of the component SysLogController. The manipulation leads to improper authorization. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	2025-09-08	4.3	CVE-2025-10084
Equalize Digital--Accessibility Checker by Equalize Digital	Missing Authorization vulnerability in Equalize Digital Accessibility Checker by Equalize Digital allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Accessibility Checker by Equalize Digital: from n/a through 1.31.0.	2025-09-09	5.4	CVE-2025-58981

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Equalize Digital--Accessibility Checker by Equalize Digital	Missing Authorization vulnerability in Equalize Digital Accessibility Checker by Equalize Digital allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Accessibility Checker by Equalize Digital: from n/a through 1.31.0.	2025-09-09	4.3	CVE-2025-58976
erjinzhi--10OA	A vulnerability was found in erjinzhi 10OA 1.0. This impacts an unknown function of the file /trial/mvc/finder. The manipulation of the argument Name results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-11	4.3	CVE-2025-10271
erjinzhi--10OA	A vulnerability was determined in erjinzhi 10OA 1.0. Affected is an unknown function of the file /trial/mvc/catalogue. This manipulation of the argument Name causes cross site scripting. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-11	4.3	CVE-2025-10272
erjinzhi--10OA	A security flaw has been discovered in erjinzhi 10OA 1.0. Affected by this issue is some unknown functionality of the file /trial/mvc/item. Performing manipulation of the argument Name results in cross site scripting. The attack may be initiated remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	4.3	CVE-2025-10274
evenium--Evenium	The Evenium plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'evenium_single_event' shortcode in all versions up to, and including, 1.3.11 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-11	6.4	CVE-2025-9850
evidentlycube--Publish approval	The Publish approval plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1. This is due to missing or incorrect nonce validation on the publish_save_option function. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-11	5.3	CVE-2025-9617
Express XSS Sanitizer project--Express XSS Sanitizer	The express-xss-sanitizer (aka Express XSS Sanitizer) package through 2.0.0 for Node.js has an unbounded recursion depth in sanitize in lib/sanitize.js for a JSON request body.	2025-09-14	5.3	CVE-2025-59364
fcba_zzm--ics-park Smart Park Management System	A security flaw has been discovered in fcba_zzm ics-park Smart Park Management System 2.0. This vulnerability affects unknown code of the file FileUploadUtils.java. The manipulation of the argument File results in unrestricted upload. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	2025-09-14	6.3	CVE-2025-10398
fcba_zzm--ics-park Smart Park Management System	A vulnerability has been found in fcba_zzm ics-park Smart Park Management System 2.0. Affected is an unknown function of the file ruoyi-quartz/src/main/java/com/ruoyi/quartz/controller/JobController.java of the component Scheduled Task Module. Such manipulation leads to code injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	2025-09-14	4.7	CVE-2025-10394
fernandiez--Auto Save Remote Images (Drafts)	The Auto Save Remote Images (Drafts) plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.0.9 via the fetch_images() function. This makes it possible for authenticated attackers, with Contributor-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.	2025-09-10	6.4	CVE-2025-7843

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Fortinet--FortiDDoS-F	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerabilities [CWE-78] in Fortinet FortiDDoS-F version 7.0.0 through 7.02 and before 6.6.3 may allow a privileged attacker to execute unauthorized code or commands via crafted CLI requests.	2025-09-09	6.5	CVE-2024-45325
Fortinet--FortiWeb	A Relative Path Traversal vulnerability [CWE-23] in FortiWeb 7.6.0 through 7.6.4, 7.4.0 through 7.4.8, 7.2.0 through 7.2.11, 7.0.2 through 7.0.11 may allow an authenticated attacker to perform an arbitrary file read on the underlying system via crafted requests.	2025-09-09	4.7	CVE-2025-53609
frenify--Categorify	Missing Authorization vulnerability in frenify Categorify allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Categorify: from n/a through 1.0.7.5.	2025-09-09	4.3	CVE-2025-59005
fuyang_lipengjun--platform	A weakness has been identified in fuyang_lipengjun platform 1.0.0. This issue affects the function queryAll of the file /adposition/queryAll of the component AdPositionController. This manipulation causes improper authorization. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited. Affects another part than CVE-2025-9936.	2025-09-08	6.3	CVE-2025-10086
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 10.7 before 18.1.6, 18.2 before 18.2.6, and 18.3 before 18.3.2 that could have allowed authenticated users to disrupt access to token listings and related administrative operations by creating tokens with excessively large names.	2025-09-12	6.5	CVE-2025-10094
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 15.0 before 18.1.6, 18.2 before 18.2.6, and 18.3 before 18.3.2 that could have allowed an authenticated user to stall background job processing by sending specially crafted commit messages, merge request descriptions, or notes.	2025-09-12	6.5	CVE-2025-1250
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 7.8 before 18.1.6, 18.2 before 18.2.6, and 18.3 before 18.3.2 that could have allowed an authenticated user with Developer-level access to cause a persistent denial of service affecting all users on a GitLab instance by uploading large files.	2025-09-12	6.5	CVE-2025-7337
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 15.1 before 18.1.6, 18.2 before 18.2.6, and 18.3 before 18.3.2 that could have allowed authenticated users to view administrator-only maintenance notes by accessing runner details through specific interfaces.	2025-09-12	4.3	CVE-2025-6769
GoodBarber--GoodBarber	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in GoodBarber GoodBarber. This issue affects GoodBarber: from n/a through 1.0.26.	2025-09-09	4.7	CVE-2025-39523
gyaku--AutoCatSet	The AutoCatSet plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1.4. This is due to missing or incorrect nonce validation on the autocatset_ajax function. This makes it possible for unauthenticated attackers to trigger automatic recategorization of posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-11	4.3	CVE-2025-9631
HasTech--ShopLentor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasTech ShopLentor allows Stored XSS. This issue affects ShopLentor: from n/a through 3.2.0.	2025-09-09	6.5	CVE-2025-58990
heateor--Heateor Login Social Login Plugin	The Heateor Login - Social Login Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'Heateor_Facebook_Login' shortcode in all versions up to, and including, 1.1.9 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.	2025-09-10	6.4	CVE-2025-9857

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Helmut Wandl--Advanced Settings	Cross-Site Request Forgery (CSRF) vulnerability in Helmut Wandl Advanced Settings allows Cross Site Request Forgery. This issue affects Advanced Settings: from n/a through 3.1.1.	2025-09-09	4.3	CVE-2025-58975
himmelblau-idm--himmelblau	Himmelblau is an interoperability suite for Microsoft Azure Entra ID and Intune. Himmelblau 0.9.x derives numeric GIDs for Entra ID groups from the group display name when himmelblau.conf `id_attr_map = name` (the default configuration). Because Microsoft Entra ID allows multiple groups with the same `displayName` (including end-user-created personal/O365 groups, depending on tenant policy), distinct directory groups can collapse to the same numeric GID on Linux. This issue only applies to Himmelblau versions 0.9.0 through 0.9.22. Any resource or service on a Himmelblau-joined host that enforces authorization by numeric GID (files/dirs, etc.) can be unintentionally accessible to a user who creates or joins a different Entra/O365 group that happens to share the same `displayName` as a privileged security group. Users should upgrade to 0.9.23, or 1.0.0 or later, to receive a patch. Group to GID mapping now uses Entra ID object IDs (GUIDs) and does not collide on same-name groups. As a workaround, use tenant policy hardening to restrict arbitrary group creation until all hosts are patched.	2025-09-09	4.4	CVE-2025-59044
HJSoft--HCM Human Resources Management System	A vulnerability was found in HJSoft HCM Human Resources Management System up to 20250822. Affected by this vulnerability is an unknown functionality of the file /templates/attestation/../../selfservice/lawresource/downlawbase. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-10	6.3	CVE-2025-10197
honojs--hono	Hono is a Web application framework that provides support for any JavaScript runtime. In versions prior to 4.9.7, a flaw in the `bodyLimit` middleware could allow bypassing the configured request body size limit when conflicting HTTP headers were present. The middleware previously prioritized the `Content-Length` header even when a `Transfer-Encoding: chunked` header was also included. According to the HTTP specification, `Content-Length` must be ignored in such cases. This discrepancy could allow oversized request bodies to bypass the configured limit. Most standards-compliant runtimes and reverse proxies may reject such malformed requests with `400 Bad Request`, so the practical impact depends on the runtime and deployment environment. If body size limits are used as a safeguard against large or malicious requests, this flaw could allow attackers to send oversized request bodies. The primary risk is denial of service (DoS) due to excessive memory or CPU consumption when handling very large requests. The implementation has been updated to align with the HTTP specification, ensuring that `Transfer-Encoding` takes precedence over `Content-Length`. The issue is fixed in Hono v4.9.7, and all users should upgrade immediately.	2025-09-12	5.3	CVE-2025-59139
IBM--Concert Software	IBM Concert Software 1.0.0 through 1.1.0 could allow a remote attacker to obtain sensitive information from allocated memory due to improper clearing of heap memory.	2025-09-08	5.9	CVE-2025-1761
IBM--Hardware Management Console	IBM Hardware Management Console - Power 10.3.1050.0 and 11.1.1110.0 is vulnerable to stored cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-09-09	6.4	CVE-2025-36125
IBM--Jazz for Service Management	IBM Jazz for Service Management 1.1.3.0 through 1.1.3.24 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic.	2025-09-09	4.3	CVE-2025-36011
IBM--PowerVM Hypervisor	IBM PowerVM Hypervisor FW950.00 through FW950.E0, FW1050.00 through FW1050.50, and FW1060.00 through FW1060.40 could allow a local privileged user	2025-09-14	6.7	CVE-2025-36035

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to cause a denial of service by issuing a specially crafted IBM i hypervisor call that would disclose memory contents or consume excessive memory resources.			
IBM--Security Verify Information Queue	IBM Security Verify Information Queue 10.0.5, 10.0.6, 10.0.7, and 10.0.8 could allow a remote user to cause a denial of service due to improper handling of special characters that could lead to uncontrolled resource consumption.	2025-09-10	6.5	CVE-2024-45669
IBM--Security Verify Information Queue	IBM Security Verify Information Queue 10.0.5, 10.0.6, 10.0.7, and 10.0.8 could allow a privileged user to escalate their privileges and attack surface on the host due to the containers running with unnecessary privileges.	2025-09-10	6.4	CVE-2024-47120
IBM--Security Verify Information Queue	IBM Security Verify Information Queue 10.0.5, 10.0.6, 10.0.7, and 10.0.8 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	2025-09-10	5.9	CVE-2024-45671
ideaboxcreations--PowerPack Elementor Addons (Free Widgets, Extensions and Templates)	The PowerPack Elementor Addons (Free Widgets, Extensions and Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cursor_url' parameter in all versions up to, and including, 2.9.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-10	6.4	CVE-2025-8388
indico--indico	Indico is an event management system that uses Flask-Multipass, a multi-backend authentication system for Flask. Prior to version 3.3.8, a legacy API to retrieve user details could be misused to retrieve profile details of other users without having admin permissions due to a broken access check. Users should to update to Indico 3.3.8 as soon as possible. As a workaround, it is possible to restrict access to the affected API (e.g. in the webserver config).	2025-09-10	4.3	CVE-2025-59034
indico--indico	Indico is an event management system that uses Flask-Multipass, a multi-backend authentication system for Flask. Prior to version 3.3.8, there is a Cross-Site-Scripting vulnerability when rendering LaTeX math code in contribution or abstract descriptions. Users should to update to Indico 3.3.8 as soon as possible. As a workaround, only let trustworthy users create content on Indico. Note that a conference doing a Call for Abstracts actively invites external speakers (who the organizers may not know and thus cannot fully trust) to submit content, hence the need to update to a a fixed version ASAP in particular when using such workflows.	2025-09-10	4.6	CVE-2025-59035
instantsoft--icms2	InstantCMS is a free and open source content management system. A blind Server-Side Request Forgery (SSRF) vulnerability in InstantCMS up to and including 2.17.3 allows authenticated remote attackers to make nay HTTP/HTTPS request via the package parameter. It is possible to make any HTTP/HTTPS request to any website in installer functionality. Due to such vulnerability it is possible to for example scan local network, call local services and its functions, conduct a DoS attack, and/or disclose a server's real IP if it's behind a reverse proxy. It is also possible to exhaust server resources by sending plethora of such requests. As of time of publication, no patched releases are available.	2025-09-11	4.7	CVE-2025-59055
ishan001--Analytics Reduce Bounce Rate	The Analytics Reduce Bounce Rate plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.3. This is due to missing or incorrect nonce validation on the unbounce_options function. This makes it possible for unauthenticated attackers to modify Google Analytics tracking settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-11	4.3	CVE-2025-9635
itsourcecode--E-Logbook with Health Monitoring System for COVID-19	A vulnerability was detected in itsourcecode E-Logbook with Health Monitoring System for COVID-19 1.0. This issue affects some unknown processing of the file /stc-log-keeper/check_profile.php of the component POST Request Handler. The manipulation of the argument profile_id results in cross site scripting. The attack may be launched remotely. The exploit is now public and may be used.	2025-09-14	4.3	CVE-2025-10411

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Ivanti--Connect Secure	SSRF in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with admin privileges to enumerate internal services.	2025-09-09	6.8	CVE-2025-55139
Ivanti--Connect Secure	Reflected text injection in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote unauthenticated attacker to inject arbitrary text into a crafted HTTP response. User interaction is required.	2025-09-09	6.1	CVE-2025-55143
Ivanti--Connect Secure	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure restricted settings.	2025-09-09	5.4	CVE-2025-55144
Ivanti--Connect Secure	CSRF in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote unauthenticated attacker to execute limited actions on behalf of the victim user. User interaction is required.	2025-09-09	5.4	CVE-2025-8711
Ivanti--Connect Secure	An unchecked return value in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with admin privileges to trigger a denial of service.	2025-09-09	4.9	CVE-2025-55146
Ivanti--Connect Secure before	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 22.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure restricted settings.	2025-09-09	5.4	CVE-2025-8712
izem--Run Log	The Run Log plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.7.10. This is due to missing or incorrect nonce validation on the oirl_plugin_options function. This makes it possible for unauthenticated attackers to modify plugin settings including distance units, pace display preferences, style themes, and display positions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-11	4.3	CVE-2025-9627
jegerwan--Plugin updates blocker	The Plugin updates blocker plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.2. This is due to missing or incorrect nonce validation on the pub_save action handler. This makes it possible for unauthenticated attackers to disable or enable plugin updates via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-11	4.3	CVE-2025-9634
jensg--Ultimate Blogroll	The Ultimate Blogroll plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.5.2. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-12	6.1	CVE-2025-9881
jh5ru--The integration of the AMO.CRM	The The integration of the AMO.CRM plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing or incorrect nonce validation on the settings_page function. This makes it possible for unauthenticated attackers to modify critical API connection settings including the AMO.CRM API URL, login credentials, and API hash key via a forged	2025-09-11	4.3	CVE-2025-9628

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	request granted they can trick a site administrator into performing an action such as clicking on a link.			
Joe Dolson--My Tickets	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Joe Dolson My Tickets allows Stored XSS. This issue affects My Tickets: from n/a through 2.0.22.	2025-09-09	6.5	CVE-2025-58988
junkurihara--httpsig-rs	httpsig-rs is a Rust implementation of IETF RFC 9421 http message signatures. Prior to version 0.0.19, the HMAC signature comparison is not timing-safe. This makes anyone who uses HS256 signature verification vulnerable to a timing attack that allows the attacker to forge a signature. Version 0.0.19 fixes the issue.	2025-09-12	5.9	CVE-2025-59058
kalcaddle--kodbox	A security vulnerability has been detected in kalcaddle kodbox 1.61. This affects the function fileGet/fileSave of the file app/controller/explorer/editor.class.php. The manipulation of the argument path leads to path traversal. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-10	6.3	CVE-2025-10233
kamilkhan--Coupon API	The Coupon API plugin for WordPress is vulnerable to SQL Injection via the 'log_duration' parameter in all versions up to, and including, 6.2.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-11	4.9	CVE-2025-8692
Korzh--EasyQuery	A weakness has been identified in Korzh EasyQuery up to 7.4.0. This issue affects some unknown processing of the file /api/easyquery/models/nwind/fetch of the component Query Builder UI. This manipulation causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	2025-09-14	6.3	CVE-2025-10399
Laborator--Kalium	Missing Authorization vulnerability in Laborator Kalium. This issue affects Kalium: from n/a through 3.18.3.	2025-09-09	5.3	CVE-2025-53348
laki_patel--Testimonial	The Testimonial plugin for WordPress is vulnerable to SQL Injection via the 'iNICtestimonial' shortcode in all versions up to, and including, 2.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-10	6.5	CVE-2025-7826
Lenovo--LJ2206W Printer	A missing authentication vulnerability was reported in some Lenovo printers that could allow a user to view limited device information or modify network settings via the CUPS service.	2025-09-11	5.4	CVE-2025-9214
libxml2--libxml2	Uncontrolled recursion in XPath evaluation in libxml2 up to and including version 2.9.14 allows a local attacker to cause a stack overflow via crafted expressions. XPath processing functions `xmlXPathRunEval`, `xmlXPathCtxtCompile`, and `xmlXPathEvalExpr` were resetting recursion depth to zero before making potentially recursive calls. When such functions were called recursively this could allow for uncontrolled recursion and lead to a stack overflow. These functions now preserve recursion depth across recursive calls, allowing recursion depth to be controlled.	2025-09-10	6.2	CVE-2025-9714
linlinjava--litemall	A weakness has been identified in linlinjava litemall up to 1.8.0. This affects the function WxAftersaleController of the file /wx/aftersale/cancel. Executing manipulation of the argument ID can lead to improper authorization. The attack can be executed remotely. The exploit has been made available to the public and	2025-09-12	6.3	CVE-2025-10291

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.			
LiteSpeed Technologies--LiteSpeed Cache	Server-Side Request Forgery (SSRF) vulnerability in LiteSpeed Technologies LiteSpeed Cache. This issue affects LiteSpeed Cache: from n/a through 7.0.1.	2025-09-09	6.4	CVE-2025-47437
livingos--ThemeLoom Widgets	The ThemeLoom Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'los_showposts' shortcode in all versions up to, and including, 1.8.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-11	6.4	CVE-2025-9861
lostvip-com--ruoyi-go	A flaw has been found in lostvip-com ruoyi-go 2.1. This affects the function SelectListPage of the file modules/system/dao/SysRoleDao.go of the component Background Management Page. This manipulation of the argument sortName causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-10	6.3	CVE-2025-10218
Magicblack--MacCMS	A vulnerability was found in Magicblack MacCMS 2025.1000.4050. Affected by this vulnerability is the function col_url of the component Scheduled Task Handler. Performing manipulation of the argument cjurl results in server-side request forgery. It is possible to initiate the attack remotely.	2025-09-14	4.7	CVE-2025-10395
Magicblack--MacCMS	A vulnerability was identified in Magicblack MacCMS 2025.1000.4050. This affects an unknown part of the component API Handler. The manipulation of the argument cjurl leads to server-side request forgery. The attack can be initiated remotely. The exploit is publicly available and might be used.	2025-09-14	4.7	CVE-2025-10397
Majestic Support--Majestic Support	Missing Authorization vulnerability in Majestic Support Majestic Support. This issue affects Majestic Support: from n/a through 1.1.0.	2025-09-09	5.3	CVE-2025-49860
manchumahara--CBX Map for Google Map & OpenStreetMap	The CBX Map for Google Map & OpenStreetMap plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the popup heading and location address parameters in all versions up to, and including, 1.1.12 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.	2025-09-11	6.4	CVE-2025-9123
markohoven--MyBrain Utilities	The MyBrain Utilities plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugins's 'mbumap' shortcode in all versions up to, and including, 1.0.8 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.	2025-09-10	6.4	CVE-2025-10126
martins56--PagBank / PagSeguro Connect para WooCommerce	The PagBank / PagSeguro Connect para WooCommerce plugin for WordPress is vulnerable to SQL Injection via the 'status' parameter in all versions up to, and including, 4.44.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-10	4.9	CVE-2025-10142
mdimran41--Blog Designer For Elementor Post Slider, Post Carousel, Post Grid	The Blog Designer For Elementor - Post Slider, Post Carousel, Post Grid plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.1.7. This is due to missing or incorrect nonce validation on the bdfe_install_activate_rswpbs_only function. This makes it possible for unauthenticated attackers to install the 'rs-wp-	2025-09-11	4.3	CVE-2025-8481

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	books-showcase' plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.			
Microsoft-- Microsoft Office 2019	Buffer over-read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2025-09-09	5.5	CVE-2025-54901
Microsoft-- Microsoft SQL Server 2017 (GDR)	Concurrent execution using shared resource with improper synchronization ('race condition') in SQL Server allows an authorized attacker to disclose information over a network.	2025-09-09	6.5	CVE-2025-47997
Microsoft-- Windows 10 Version 1809	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	2025-09-09	6.7	CVE-2025-53808
Microsoft-- Windows 10 Version 1809	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	2025-09-09	6.7	CVE-2025-53810
Microsoft-- Windows 10 Version 1809	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	2025-09-09	6.7	CVE-2025-54094
Microsoft-- Windows 10 Version 1809	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	2025-09-09	6.7	CVE-2025-54104
Microsoft-- Windows 10 Version 1809	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	2025-09-09	6.7	CVE-2025-54109
Microsoft-- Windows 10 Version 1809	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	2025-09-09	6.7	CVE-2025-54915
Microsoft-- Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Graphics Kernel allows an authorized attacker to execute code locally.	2025-09-09	6.7	CVE-2025-55226
Microsoft-- Windows 10 Version 1809	Use of uninitialized resource in Windows Imaging Component allows an unauthorized attacker to disclose information locally.	2025-09-09	5.5	CVE-2025-53799
Microsoft-- Windows 10 Version 1809	Generation of error message containing sensitive information in Windows Kernel allows an authorized attacker to disclose information locally.	2025-09-09	5.5	CVE-2025-53803
Microsoft-- Windows 10 Version 1809	Exposure of sensitive information to an unauthorized actor in Windows Kernel allows an authorized attacker to disclose information locally.	2025-09-09	5.5	CVE-2025-53804
Microsoft-- Windows 10 Version 1809	Use after free in Windows SMBv3 Client allows an authorized attacker to execute code over a network.	2025-09-09	4.8	CVE-2025-54101
Microsoft-- Windows 10 Version 1809	Improper resolution of path equivalence in Windows MapUrlToZone allows an unauthorized attacker to bypass a security feature over a network.	2025-09-09	4.3	CVE-2025-54107
Microsoft-- Windows 10 Version 1809	Protection mechanism failure in Windows MapUrlToZone allows an unauthorized attacker to bypass a security feature over a network.	2025-09-09	4.3	CVE-2025-54917

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows Server 2019	Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-09-09	6.5	CVE-2025-53796
Microsoft--Windows Server 2019	Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-09-09	6.5	CVE-2025-53797
Microsoft--Windows Server 2019	Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-09-09	6.5	CVE-2025-53798
Microsoft--Windows Server 2019	Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-09-09	6.5	CVE-2025-53806
Microsoft--Windows Server 2019	Out-of-bounds read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-09-09	6.5	CVE-2025-54095
Microsoft--Windows Server 2019	Out-of-bounds read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-09-09	6.5	CVE-2025-54096
Microsoft--Windows Server 2019	Out-of-bounds read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-09-09	6.5	CVE-2025-54097
Microsoft--Windows Server 2019	Out-of-bounds read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-09-09	6.5	CVE-2025-55225
Microsoft--Windows Server 2025 (Server Core installation)	Improper input validation in Windows Local Security Authority Subsystem Service (LSASS) allows an authorized attacker to deny service over a network.	2025-09-09	6.5	CVE-2025-53809
MiczFlor--RPi-Jukebox-RFID	A security flaw has been discovered in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected is an unknown function of the file /htdocs/api/playlist/single.php. Performing manipulation of the argument playlist results in os command injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	6.3	CVE-2025-10326
MiczFlor--RPi-Jukebox-RFID	A weakness has been identified in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected by this vulnerability is an unknown functionality of the file /htdocs/api/playlist/shuffle.php. Executing manipulation of the argument playlist can lead to os command injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	6.3	CVE-2025-10327
MiczFlor--RPi-Jukebox-RFID	A security vulnerability has been detected in MiczFlor RPi-Jukebox-RFID up to 2.8.0. Affected by this issue is some unknown functionality of the file /htdocs/api/playlist/playsinglefile.php. The manipulation of the argument File leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	6.3	CVE-2025-10328
Mikado Themes--Mikado Core	The Mikado Core plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 1.5.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject	2025-09-09	6.4	CVE-2025-9058

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
Mikado Themes--Wilmer Core	The Wilmer Core plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 2.4.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-09	6.4	CVE-2025-9061
miriamgoldman--Workable Api	The Workable Api plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's workable_jobs shortcode in all versions up to, and including, 1.0.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-11	6.4	CVE-2025-8721
miurla--morphic	A flaw has been found in miurla morphic up to 0.4.5. This impacts the function fetchHtml of the file /api/advanced-search of the component HTTP Status Code 3xx Handler. This manipulation causes server-side request forgery. The attack is possible to be carried out remotely. The exploit has been published and may be used.	2025-09-14	6.3	CVE-2025-10393
moreirapontocom--Certifica WP	The Certifica WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'evento' parameter in all versions up to, and including, 3.1 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.	2025-09-11	6.4	CVE-2025-8316
mythemeshop--My WP Translate	The My WP Translate plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the mtswpt_remove_plugin() and ajax_update_export_code() functions in all versions up to, and including, 1.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read and delete arbitrary WordPress options which can cause a denial of service.	2025-09-11	5.4	CVE-2025-8423
n/a--299ko	A weakness has been identified in 299ko up to 2.0.0. Affected by this issue is the function getSentDir/delete of the file plugin/filemanager/controllers/FileManagerAPIController.php. Executing manipulation can lead to path traversal. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-10	5.4	CVE-2025-10232
n/a--ChanCMS	A vulnerability was identified in ChanCMS up to 3.3.1. Impacted is an unknown function of the file /search/. The manipulation with the input '%20or%201=1%20%23/words.html leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	2025-09-08	6.3	CVE-2025-10110
n/a--CRMEB	A security vulnerability has been detected in CRMEB up to 5.6.1. The impacted element is the function testOutUrl of the file app/services/out/OutAccountServices.php. The manipulation of the argument push_token_url leads to server-side request forgery. Remote exploitation of the attack is possible. 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.	2025-09-14	6.3	CVE-2025-10391
n/a--CRMEB	A security flaw has been discovered in CRMEB up to 5.6.1. Impacted is the function Save of the file app/services/system/admin/SystemAdminServices.php of the component Administrator Password Handler. Performing manipulation of the argument ID results in improper authorization. The attack may be initiated	2025-09-14	5.4	CVE-2025-10389

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.			
n/a--CRMEB	A weakness has been identified in CRMEB up to 5.6.1. The affected element is the function editAddress of the file app/services/user/UserAddressServices.php. Executing manipulation of the argument ID can lead to improper authorization. The attack may be launched remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-14	5.4	CVE-2025-10390
n/a--FoxCMS	A vulnerability was detected in FoxCMS up to 1.24. Affected by this issue is the function batchCope of the file /app/admin/controller/Images.php. The manipulation of the argument ids results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-11	6.3	CVE-2025-10251
n/a--Freshwork	A vulnerability has been found in Freshwork up to 1.2.3. This impacts an unknown function of the file /api/v2/logout. Such manipulation of the argument post_logout_redirect_uri leads to open redirect. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.2.3 will fix this issue. You should upgrade the affected component. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-10	4.3	CVE-2025-10229
n/a--JeecgBoot	A vulnerability was identified in JeecgBoot up to 3.8.2. Affected by this vulnerability is an unknown functionality of the file /api/system/sendWebSocketMsg of the component WebSocket Message Handler. The manipulation of the argument userIds leads to improper authorization. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	6.3	CVE-2025-10318
n/a--JeecgBoot	A security flaw has been discovered in JeecgBoot up to 3.8.2. Affected by this issue is some unknown functionality of the file /sys/tenant/exportLog of the component Tenant Log Export. The manipulation results in improper authorization. The attack can be launched remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	4.3	CVE-2025-10319
n/a--JEPaaS	A security vulnerability has been detected in JEPaaS 7.2.8. This vulnerability affects the function doFilterInternal of the component Filter Handler. Such manipulation leads to improper access controls. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-11	6.3	CVE-2025-10247
n/a--jsondiffpatch	Versions of the package jsondiffpatch before 0.7.2 are vulnerable to Cross-site Scripting (XSS) via HtmlFormatter::nodeBegin. An attacker can inject malicious scripts into HTML payloads that may lead to code execution if untrusted payloads were used as source for the diff, and the result renderer using the built-in html formatter on a private website.	2025-09-11	4.7	CVE-2025-9910
n/a--Maccms10	A vulnerability was found in Maccms10 2025.1000.4050. Affected is the function rep of the file application/admin/controller/Database.php. Performing manipulation of the argument where results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	2025-09-09	4.7	CVE-2025-10122
n/a--Seismic App	A vulnerability has been found in Seismic App 2.4.2 on Android. Affected is an unknown function of the file AndroidManifest.xml of the component com.seismic.doccenter. Such manipulation leads to improper export of android application components. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-10	5.3	CVE-2025-10195

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--uverif	A flaw has been found in uverif up to 3.2. This affects the function addbatch of the file /admin/kami_list. This manipulation of the argument note causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	2025-09-09	6.3	CVE-2025-10121
nanbu--Welcart e-Commerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in nanbu Welcart e-Commerce allows Stored XSS. This issue affects Welcart e-Commerce: from n/a through 2.11.20.	2025-09-09	5.9	CVE-2025-58984
natata7--Mixtape	The Mixtape plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mixtape' shortcode in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-11	6.4	CVE-2025-9860
NewType Infortech--NUP Portal	NUP Portal developed by NewType Infortech has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to directly upload files. If the attacker manages to bypass the file extension restrictions, they could upload a webshell and execute it on the server side.	2025-09-12	5.3	CVE-2025-10267
nitropack--NitroPack Caching & Speed Optimization for Core Web Vitals, Defer CSS & JS, Lazy load Images and CDN	The NitroPack plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the nitropack_set_compression_ajax() function in all versions up to, and including, 1.18.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the nitropack-enableCompression option and effectively change plugin compression settings.	2025-09-10	4.3	CVE-2025-8778
OpenPrinting--cups	OpenPrinting CUPS is an open source printing system for Linux and other Unix-like operating systems. In versions 2.4.12 and earlier, an unsafe deserialization and validation of printer attributes causes null dereference in the libcups library. This is a remote DoS vulnerability available in local subnet in default configurations. It can cause the cups & cups-browsed to crash, on all the machines in local network who are listening for printers (so by default for all regular linux machines). On systems where the vulnerability CVE-2024-47176 (cups-filters 1.x/cups-browsed 2.x vulnerability) was not fixed, and the firewall on the machine does not reject incoming communication to IPP port, and the machine is set to be available to public internet, attack vector "Network" is possible. The current versions of CUPS and cups-browsed projects have the attack vector "Adjacent" in their default configurations. Version 2.4.13 contains a patch for CVE-2025-58364.	2025-09-11	6.5	CVE-2025-58364
opsmill--infrahub	Infrahub offers a central hub to manage data, templates, and playbooks. Prior to versiond 1.3.9 and 1.4.5, a bug in the authentication logic will cause API tokens that were deleted and/or expired to be considered valid. This means that any API token that is associated with an active user account can authenticate successfully. This issue is fixed in versions 1.3.9 and 1.4.5. As a workaround, users can delete or deactivate the account associated with a deleted API token to prevent that token from authenticating.	2025-09-09	5.5	CVE-2025-59036
Papermerge--DMS	A security flaw has been discovered in Papermerge DMS up to 3.5.3. This issue affects some unknown processing of the component Authorization Token Handler. Performing manipulation results in improper authorization. The attack can be initiated remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-10	5.4	CVE-2025-10209
peachpay--Payments Plugin and Checkout	The Payments Plugin and Checkout Plugin for WooCommerce: Stripe, PayPal, Square, Authorize.net plugin for WordPress is vulnerable to time-based SQL Injection via the 'order_by' parameter in all versions up to, and including, 1.117.5	2025-09-10	6.5	CVE-2025-9463

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Plugin for WooCommerce: Stripe, PayPal, Square, Authorize.net	due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.			
Pegasystems--Pega Infinity	Pega Platform versions 7.1.0 to Infinity 24.2.2 are affected by a Stored XSS issue in a user interface component. Requires a high privileged user with a developer role.	2025-09-10	5.5	CVE-2025-8681
PHPGurukul--User Management System	A security flaw has been discovered in PHPGurukul User Management System 1.0. Affected is an unknown function of the file /admin/edit-user-profile.php. The manipulation of the argument uid results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be exploited.	2025-09-08	6.3	CVE-2025-10098
pixeline--Pixeline's Email Protector	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pixeline Pixeline's Email Protector allows Stored XSS. This issue affects Pixeline's Email Protector: from n/a through 1.3.8.	2025-09-09	5.9	CVE-2025-58982
recorp--Export WP Page to Static HTML/CSS	Missing Authorization vulnerability in recorp Export WP Page to Static HTML/CSS allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Export WP Page to Static HTML/CSS: from n/a through 4.1.0.	2025-09-09	5.3	CVE-2025-58980
rejuancse--Digital Events Calendar	The Digital Events Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'column' parameter in all versions up to, and including, 1.0.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-11	6.4	CVE-2025-5801
Rhys Wynne--WP eBay Product Feeds	Server-Side Request Forgery (SSRF) vulnerability in Rhys Wynne WP eBay Product Feeds allows Server Side Request Forgery. This issue affects WP eBay Product Feeds: from n/a through 3.4.8.	2025-09-09	4.9	CVE-2025-58977
Roland Murg--WP Simple Booking Calendar	Missing Authorization vulnerability in Roland Murg WP Simple Booking Calendar. This issue affects WP Simple Booking Calendar: from n/a through 2.0.13.	2025-09-09	6.5	CVE-2025-39541
roncoo--roncoo-pay	A vulnerability was found in roncoo roncoo-pay up to 9428382af21cd5568319eae7429b7e1d0332ff40. The impacted element is an unknown function of the file /user/info/list. Performing manipulation results in improper authentication. It is possible to initiate the attack remotely. The exploit has been made public and could be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	5.3	CVE-2025-10288
rubengc--AutomatorWP Automator plugin for no-code automations, webhooks & custom integrations in WordPress	The AutomatorWP - Automator plugin for no-code automations, webhooks & custom integrations in WordPress plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on multiple plugin's functions in all versions up to, and including, 5.3.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify integration settings or view existing automations.	2025-09-09	5.4	CVE-2025-9542
saleor--saleor	Saleor is an e-commerce platform. Starting in version 3.21.0 and prior to version 3.21.16, requesting certain fields in the response of `accountRegister` may result in errors that could unintentionally reveal whether a user with the provided email	2025-09-09	5.3	CVE-2025-58442

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	already exists in Saleor. Version 3.21.16 fixes the issue. As a workaround, rate-limit the mutation to reduce the impact.			
SAP_SE--Fiori app (Manage Payment Blocks)	Fiori app Manage Payment Blocks does not perform the necessary authorization checks, allowing an attacker with basic user privileges to abuse functionalities that should be restricted to specific user groups.This issue could impact both the confidentiality and integrity of the application without affecting the availability.	2025-09-09	5.4	CVE-2025-42915
SAP_SE--SAP Business Planning and Consolidation	SAP Business Planning and Consolidation allows an authenticated standard user to call a function module by crafting specific parameters that causes a loop, consuming excessive resources and resulting in system unavailability. This leads to high impact on the availability of the application, there is no impact on confidentiality or integrity.	2025-09-09	6.5	CVE-2025-42930
SAP_SE--SAP Fiori App (F4044 Manage Work Center Groups)	Due to insufficient CSRF protection in SAP Fiori App Manage Work Center Groups, an authenticated user could be tricked by an attacker to send unintended request to the web server. This has low impact on integrity and no impact on confidentiality and availability of the application.	2025-09-09	4.3	CVE-2025-42923
SAP_SE--SAP HCM (Approve Timesheets Fiori 2.0 application)	SAP HCM Approve Timesheets Fiori 2.0 application does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This issue has a significant impact on the application's integrity, while confidentiality and availability remain unaffected.	2025-09-09	6.5	CVE-2025-42917
SAP_SE--SAP HCM (My Timesheet Fiori 2.0 application)	SAP HCM My Timesheet Fiori 2.0 application does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This issue has a significant impact on the application's integrity, while confidentiality and availability remain unaffected.	2025-09-09	6.5	CVE-2025-42912
SAP_SE--SAP NetWeaver (Service Data Download)	SAP NetWeaver (Service Data Download) allows an authenticated user to call a remote-enabled function module, which could grant access to information about the SAP system and operating system. This leads to a low impact on confidentiality, with no effect on the integrity and availability of the application	2025-09-09	5	CVE-2025-42911
SAP_SE--SAP NetWeaver ABAP Platform	Due to a Cross-Site Scripting (XSS) vulnerability in the SAP NetWeaver ABAP Platform, an unauthenticated attacker could generate a malicious link and make it publicly accessible. If an authenticated user clicks on this link, the injected input is processed during the websiteï¿½s page generation, resulting in the creation of malicious content. When executed, this content allows the attacker to access or modify information within the victim's browser scope, impacting the confidentiality and integrityï¿½while availability remains unaffected.	2025-09-09	6.1	CVE-2025-42938
SAP_SE--SAP NetWeaver Application Server for ABAP (Background Processing)	SAP NetWeaver Application Server for ABAP allows authenticated users with access to background processing to gain unauthorized read access to profile parameters. This results in a low impact on confidentiality, with no impact on integrity or availability	2025-09-09	4.3	CVE-2025-42918
SAP_SE--SAP NetWeaver Application Server Java	SAP NetWeaver Application Server Java does not perform an authentication check when an attacker attempts to access internal files within the web application.Upon successfully exploitation, an unauthenticated attacker could access these files to gather additional sensitive information about the system.This vulnerability has a low impact on confidentiality and does not affect the integrity or availability of the server.	2025-09-09	5.3	CVE-2025-42926
SAP_SE--SAP NetWeaver AS Java (IIOP Service)	Due to the lack of randomness in assigning Object Identifiers in the SAP NetWeaver AS JAVA IIOP service, an authenticated attacker with low privileges could predict the identifiers by conducting a brute force search. By leveraging knowledge of several identifiers generated close to the same time, the attacker could determine a desired identifier which could enable them to access limited system information.	2025-09-09	4.3	CVE-2025-42925

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This poses a low risk to confidentiality without impacting the integrity or availability of the service.			
SAP_SE--SAP Supplier Relationship Management	Due to a Cross-Site Scripting (XSS) vulnerability in the SAP Supplier Relationship Management, an unauthenticated attacker could generate a malicious link and make it publicly accessible. If an authenticated victim clicks on the link, the injected input is processed during the page generation, resulting in the execution of malicious content. This execution allows the attacker to access and modify information within the victim's browser scope, impacting confidentiality and integrity, while availability remains unaffected.	2025-09-09	6.1	CVE-2025-42920
shaikhaezaz80--Countdown Timer for Elementor	The Countdown Timer for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'countdown_label' Parameter in all versions up to, and including, 1.3.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-11	6.4	CVE-2025-8445
shawfactor--LH Signing	The LH Signing plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.83. This is due to missing or incorrect nonce validation on the plugin_options function. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-11	4.3	CVE-2025-9633
Siemens--APOGEE PXC Series (BACnet)	A vulnerability has been identified in APOGEE PXC Series (BACnet) (All versions), APOGEE PXC Series (P2 Ethernet) (All versions), TALON TC Series (BACnet) (All versions). Affected devices connected to the network allow unrestricted access to sensitive files, such as databases. This could allow an attacker to download encrypted .db file containing passwords.	2025-09-09	5.3	CVE-2025-40757
Siemens--SINAMICS G220 V6.4	A vulnerability has been identified in SINAMICS G220 V6.4 (All versions < V6.4 HF2), SINAMICS S200 V6.4 (All versions), SINAMICS S210 V6.4 (All versions < V6.4 HF2). The affected devices allow a factory reset to be executed without the required privileges due to improper privilege management as well as manipulation of configuration data because of leaked privileges of previous sessions. This could allow an unauthorized attacker to escalate their privileges.	2025-09-09	6.3	CVE-2025-40594
silverplugins217--Dynamic Text Field For Contact Form 7	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in silverplugins217 Dynamic Text Field For Contact Form 7 allows Stored XSS. This issue affects Dynamic Text Field For Contact Form 7: from n/a through 1.0.	2025-09-09	6.5	CVE-2025-58989
SimStudioAI--sim	A vulnerability was determined in SimStudioAI sim up to 1.0.0. This affects an unknown function of the file apps/sim/app/api/files/parse/route.ts. Executing manipulation of the argument filePath can lead to server-side request forgery. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. This patch is called 3424a338b763115f0269b209e777608e4cd31785. Applying a patch is advised to resolve this issue.	2025-09-08	6.3	CVE-2025-10096
SimStudioAI--sim	A vulnerability was identified in SimStudioAI sim up to 1.0.0. This impacts an unknown function of the file apps/sim/app/api/function/execute/route.ts. The manipulation of the argument code leads to code injection. The attack is possible to be carried out remotely.	2025-09-08	6.3	CVE-2025-10097
slowmove--Spotify Embed Creator	The Spotify Embed Creator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'spotify' shortcode in all versions up to, and including, 1.0.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-12	6.4	CVE-2025-9879

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
smartcatai--Smartcat Translator for WPML	The Smartcat Translator for WPML plugin for WordPress is vulnerable to time-based SQL Injection via the 'orderby' parameter in all versions up to, and including, 3.1.69 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-11	6.5	CVE-2025-9451
softmus--WP Scriptcase	The WP Scriptcase plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in all versions up to, and including, 2.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-11	6.4	CVE-2025-8691
SourceCodester--Food Ordering Management System	A security vulnerability has been detected in SourceCodester Food Ordering Management System 1.0. Impacted is an unknown function of the file /routers/ticket-message.php. Such manipulation of the argument ticket_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	2025-09-14	6.3	CVE-2025-10400
SourceCodester--Link Status Checker	A security vulnerability has been detected in SourceCodester Link Status Checker 1.0. This vulnerability affects unknown code of the file index.php. The manipulation of the argument proxy leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	2025-09-14	6.3	CVE-2025-10410
SourceCodester--Pet Grooming Management Software	A vulnerability was determined in SourceCodester Pet Grooming Management Software 1.0. Affected by this issue is some unknown functionality of the file /admin/profile.php. Executing manipulation can lead to unrestricted upload. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	2025-09-08	6.3	CVE-2025-10083
SourceCodester--Pet Grooming Management Software	A security flaw has been discovered in SourceCodester Pet Grooming Management Software 1.0. This vulnerability affects unknown code of the file manage_website.php. The manipulation results in unrestricted upload. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	2025-09-08	6.3	CVE-2025-10085
SourceCodester--Pet Grooming Management Software	A security vulnerability has been detected in SourceCodester Pet Grooming Management Software 1.0. Impacted is an unknown function of the file /admin/profit_report.php. Such manipulation of the argument product_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	2025-09-08	4.7	CVE-2025-10087
SourceCodester--Pet Management System	A flaw has been found in SourceCodester Pet Management System 1.0. This impacts an unknown function of the file /admin/profile.php. This manipulation of the argument website_image causes unrestricted upload. Remote exploitation of the attack is possible. The exploit has been published and may be used.	2025-09-08	4.7	CVE-2025-10081
SourceCodester--Student Grading System	A vulnerability was identified in SourceCodester Student Grading System 1.0. Affected by this vulnerability is an unknown functionality of the file /view_user.php. 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.	2025-09-14	6.3	CVE-2025-10407
SourceCodester--Student Grading System	A security flaw has been discovered in SourceCodester Student Grading System 1.0. Affected by this issue is some unknown functionality of the file /edit_user.php. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	2025-09-14	6.3	CVE-2025-10408

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SourceCodester--Student Grading System	A weakness has been identified in SourceCodester Student Grading System 1.0. This affects an unknown part of the file /rms.php?page=users. Executing manipulation of the argument fname can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.	2025-09-14	6.3	CVE-2025-10409
Sovica--Target Video Easy Publish	Missing Authorization vulnerability in Sovica Target Video Easy Publish. This issue affects Target Video Easy Publish: from n/a through 3.8.8.	2025-09-09	5.4	CVE-2025-32688
spoddev2021--Spreadconnect	Missing Authorization vulnerability in spoddev2021 Spreadconnect. This issue affects Spreadconnect: from n/a through 2.1.5.	2025-09-09	5.4	CVE-2025-53291
Stefano Lissa--Include Me	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stefano Lissa Include Me allows Stored XSS. This issue affects Include Me: from n/a through 1.3.2.	2025-09-09	5.9	CVE-2025-58983
TRENDnet--TEW-831DR	A vulnerability has been found in TRENDnet TEW-831DR 1.0 (601.130.1.1410). Impacted is an unknown function of the file /boafrm/formSysCmd. The manipulation of the argument sysHost leads to command injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-09	4.7	CVE-2025-10107
uscnanbu--Welcart e-Commerce	The Welcart e-Commerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via settings in all versions up to, and including, 2.11.20 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2025-09-10	5.5	CVE-2025-9367
vinzzb--PhpList Subber	The PhpList Subber plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1. This is due to missing or incorrect nonce validation on the bulk_action_handler function. This makes it possible for unauthenticated attackers to trigger bulk synchronization of subscription forms via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-11	4.3	CVE-2025-9632
Wavlink--WL-WN578W2	A vulnerability was identified in Wavlink WL-WN578W2 221110. This impacts the function sub_401340/sub_401BA4 of the file /cgi-bin/login.cgi. Such manipulation of the argument ipaddr leads to command injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	6.3	CVE-2025-10325
Wavlink--WL-WN578W2	A flaw has been found in Wavlink WL-WN578W2 221110. Impacted is an unknown function of the file /live_online.shtml. Executing manipulation can lead to information disclosure. The attack can be executed remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	5.3	CVE-2025-10321
Wavlink--WL-WN578W2	A vulnerability has been found in Wavlink WL-WN578W2 221110. The affected element is an unknown function of the file /sysinit.html. The manipulation of the argument newpass/confpass leads to weak password recovery. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	5.3	CVE-2025-10322
webcodingplace--Ultimate Classified Listings	The Ultimate Classified Listings plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_custom_fields function in all versions up to, and including, 1.6. This makes it possible for	2025-09-11	4.3	CVE-2025-0763

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated attackers, with Subscriber-level access and above, to change plugin custom fields.			
wen-solutions--WP Easy FAQs	The WP Easy FAQs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's WP_EASY_FAQ shortcode in all versions up to, and including, 1.0.5 due to insufficient input sanitization and output escaping on user supplied attributes. 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.	2025-09-11	6.4	CVE-2025-8686
Wind River Studio Developer--Wind River Studio Developer	Under heavy system utilization a random race condition can occur during authentication or token refresh operation. This flaw allows one user to be granted a token intended for another user, resulting in impersonation until the session is ended. This flaw cannot be intentionally exploited due to the required concurring action by two users. However, if the event occurs a user would be inadvertently exposed to another user's system rights and data access.	2025-09-11	6	CVE-2025-26499
wordpresschef--Salon Booking System, Appointment Scheduling for Salons, Spas & Small Businesses	The Salon Booking System, Appointment Scheduling for Salons, Spas & Small Businesses plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ajax function in all versions up to, and including, 10.20. This makes it possible for unauthenticated attackers to execute AJAX actions, including limited file uploads.	2025-09-11	5.3	CVE-2025-8492
WP Swings--PDF Generator for WordPress	Missing Authorization vulnerability in WP Swings PDF Generator for WordPress allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects PDF Generator for WordPress: from n/a through 1.5.4.	2025-09-09	5.3	CVE-2025-58978
wpblast--WP Blast | SEO & Performance Booster	The WP Blast | SEO & Performance Booster plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.8.6. This is due to missing or incorrect nonce validation on multiple administrative actions in the Settings class. This makes it possible for unauthenticated attackers to trigger cache purging, sitemap clearing, plugin data purging, and score resetting operations via forged requests granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-10	4.3	CVE-2025-9622
WPFactory--Additional Custom Product Tabs for WooCommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Additional Custom Product Tabs for WooCommerce allows Stored XSS. This issue affects Additional Custom Product Tabs for WooCommerce: from n/a through 1.7.3.	2025-09-09	6.5	CVE-2025-58985
yangzongzhuan--RuoYi	A flaw has been found in yangzongzhuan RuoYi up to 4.8.1. Affected by this vulnerability is an unknown functionality of the file /system/role/authUser/cancelAll of the component Role Handler. Executing manipulation of the argument roleId/userIds can lead to improper authorization. The attack may be performed from remote. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-13	5.4	CVE-2025-10384
yanyutao0402--ChanCMS	A flaw has been found in yanyutao0402 ChanCMS up to 3.3.1. Affected by this issue is some unknown functionality of the file /cms/article/search. This manipulation of the argument keyword causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	2025-09-08	6.3	CVE-2025-10105
yanyutao0402--ChanCMS	A vulnerability has been found in yanyutao0402 ChanCMS up to 3.3.1. This affects an unknown part of the file /cms/collect/search. Such manipulation of the argument keyword leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2025-09-08	6.3	CVE-2025-10106

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
yanyutao0402--ChanCMS	A weakness has been identified in yanyutao0402 ChanCMS up to 3.3.0. Impacted is the function Search of the file app/modules/api/service/Api.js. Executing manipulation of the argument key can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-10	6.3	CVE-2025-10210
yanyutao0402--ChanCMS	A security vulnerability has been detected in yanyutao0402 ChanCMS 3.3.0. The affected element is the function CollectController of the file /cms/collect/getArticle. The manipulation of the argument taskUrl leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-10	6.3	CVE-2025-10211
Yida--ECMS Consulting Enterprise Management System	A vulnerability was found in Yida ECMS Consulting Enterprise Management System 1.0. This affects an unknown part of the file /login.do of the component POST Request Handler. The manipulation of the argument requestUrl results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-14	4.3	CVE-2025-10386
yonifre--Maspik Ultimate Spam Protection	The Maspik - Ultimate Spam Protection plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.5.6. This is due to missing or incorrect nonce validation on the clear_log function. This makes it possible for unauthenticated attackers to clear all spam logs via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-10	4.3	CVE-2025-9888
yonifre--Maspik Ultimate Spam Protection	The Maspik plugin for WordPress is vulnerable to Missing Authorization in version 2.5.6 and prior. This is due to missing capability checks on the Maspik_spamlog_download_csv function. This makes it possible for authenticated attackers, with subscriber-level access and above, to export and download the spam log database containing blocked submission attempts, which may include misclassified but legitimate submissions with sensitive data.	2025-09-10	4.3	CVE-2025-9979
YunaiV--ruoyi-vue-pro	A security vulnerability has been detected in YunaiV ruoyi-vue-pro up to 2025.09. This vulnerability affects unknown code of the file /crm/contract/transfer. The manipulation of the argument id/newOwnerUserId leads to improper authorization. Remote exploitation of the attack is possible. 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.	2025-09-12	6.3	CVE-2025-10276
YunaiV--ruoyi-vue-pro	A flaw has been found in YunaiV ruoyi-vue-pro up to 2025.09. Impacted is an unknown function of the file /crm/contact/transfer. This manipulation of the argument ids/newOwnerUserId causes improper authorization. The attack is possible to be carried out remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	6.3	CVE-2025-10278
YunaiV--yudao-cloud	A weakness has been identified in YunaiV yudao-cloud up to 2025.09. This affects an unknown part of the file /crm/business/transfer. Executing manipulation of the argument ids/newOwnerUserId can lead to improper authorization. The attack may be launched remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	6.3	CVE-2025-10275
YunaiV--yudao-cloud	A vulnerability was detected in YunaiV yudao-cloud up to 2025.09. This issue affects some unknown processing of the file /crm/receivable/submit. The manipulation of the argument ID results in improper authorization. The attack can be executed remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-12	6.3	CVE-2025-10277

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ZhenShi--Mibro Fit App	A flaw has been found in ZhenShi Mibro Fit App 1.6.3.17499 on Android. This impacts an unknown function of the file AndroidManifest.xml of the component com.xiaoxun.xunoversea.mibrofit. This manipulation causes improper export of android application components. The attack requires local access. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-09	5.3	CVE-2025-5500
zohoflow--Zoho Flow Integrate 100+ plugins with 1000+ business apps, no-code workflow automation	The Zoho Flow plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.14.1. This is due to missing or incorrect nonce validation on the zoho_flow_deactivate_plugin function. This makes it possible for unauthenticated attackers to modify typography settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-11	4.3	CVE-2025-8479
Zoom Communications, Inc--Zoom Workplace Clients	Buffer overflow in certain Zoom Workplace Clients may allow an authenticated user to conduct a denial of service via network access.	2025-09-09	6.5	CVE-2025-49458
Zoom Communications, Inc--Zoom Workplace Clients	Uncontrolled resource consumption in certain Zoom Workplace Clients may allow an unauthenticated user to conduct a denial of service via network access.	2025-09-09	4.3	CVE-2025-49460
Zoom Communications, Inc--Zoom Workplace Clients	Cross-site scripting in certain Zoom Workplace Clients may allow an unauthenticated user to conduct a denial of service via network access.	2025-09-09	4.3	CVE-2025-49461
Zoom Communications, Inc--Zoom Workplace Clients for Windows	Improper action enforcement in certain Zoom Workplace Clients for Windows may allow an unauthenticated user to conduct a disclosure of information via network access.	2025-09-09	5.3	CVE-2025-58135
Zoom Communications, Inc--Zoom Workplace Clients for Windows	Incorrect authorization in certain Zoom Workplace Clients for Windows may allow an authenticated user to conduct an impact to integrity via network access.	2025-09-09	4.3	CVE-2025-58134
Zoom Communications, Inc--Zoom Workplace VDI Plugin macOS Universal installer for VMware Horizon	Race condition in the Zoom Workplace VDI Plugin macOS Universal installer for VMware Horizon before version 6.4.10 (or before 6.2.15 and 6.3.12 in their respective tracks) may allow an authenticated user to conduct a disclosure of information via network access.	2025-09-09	6.6	CVE-2025-58131
zuotian--Enhanced BibliPlug	The Enhanced BibliPlug plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'bibliplug_authors' shortcode in all versions up to, and including, 1.3.8 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.	2025-09-11	6.4	CVE-2025-9855
1Panel-dev--MaxKB	A vulnerability was determined in 1Panel-dev MaxKB up to 2.0.2/2.1.0. This issue affects some unknown processing of the file /admin/api/workspace/default/tool/debug. Executing manipulation of the argument code can lead to deserialization. The attack can be executed remotely.	2025-09-15	6.3	CVE-2025-10433

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The exploit has been publicly disclosed and may be utilized. Upgrading to version 2.1.1 is capable of addressing this issue. It is suggested to upgrade the affected component.			
academico-sis--academico	A vulnerability was determined in academico-sis academico up to d9a9e2636fbf7e5845ee086bcb03ca62faceb6ab. Affected by this issue is some unknown functionality of the file /edit-photo of the component Profile Picture Handler. This manipulation causes unrestricted upload. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. This product adopts a rolling release strategy to maintain continuous delivery The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-21	6.3	CVE-2025-10763
Adobe--Substance3D - Stager	Substance3D - Stager versions 3.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-09-16	5.5	CVE-2025-54237
APEUni--PTE Exam Practice App	A security flaw has been discovered in APEUni PTE Exam Practice App up to 10.8.0 on Android. The impacted element is an unknown function of the file AndroidManifest.xml of the component com.ape_edication. The manipulation results in improper export of android application components. The attack requires a local approach. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-19	5.3	CVE-2025-10715
ArgusTech--BILGER	Authorization Bypass Through User-Controlled Key vulnerability with user privileges in ArgusTech BILGER allows Exploitation of Trusted Identifiers.This issue affects BILGER: before 2.4.6.	2025-09-16	6.5	CVE-2025-5518
ArgusTech--BILGER	Insertion of Sensitive Information Into Sent Data vulnerability in ArgusTech BILGER allows Choosing Message Identifier.This issue affects BILGER: before 2.4.6.	2025-09-16	6.5	CVE-2025-5519
athemes--Sydney	The Sydney theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'activate_modules' function in all versions up to, and including, 2.56. This makes it possible for authenticated attackers, with Subscriber-level access and above, to activate or deactivate various theme modules.	2025-09-17	5.3	CVE-2025-8999
ays-pro--Quiz Maker	The Quiz Maker plugin for WordPress is vulnerable to SQL Injection via spoofed IP headers in all versions up to, and including, 6.7.0.56 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This is only exploitable in configurations where the server is set up to retrieve the IP from a user-supplied field like `X-Forwarded-For` and limit users by IP is enabled.	2025-09-17	5.9	CVE-2025-10042
Beefull Energy Technologies--Beefull App	Authorization Bypass Through User-Controlled Key vulnerability in Beefull Energy Technologies Beefull App allows Exploitation of Trusted Identifiers.This issue affects Beefull App: before 24.07.2025.	2025-09-16	6.5	CVE-2025-7355
Bimser Solution Software Trade Inc.--eBA Document and Workflow Management System	Authorization Bypass Through User-Controlled Key, CWE - 862 - Missing Authorization, - Improper Authorization vulnerability in Bimser Solution Software Trade Inc. EBA Document and Workflow Management System allows - Exploitation of Trusted Identifiers, - Exploitation of Authorization, - Variable Manipulation.This issue affects eBA Document and Workflow Management System: from 6.7.164 before 6.7.166.	2025-09-19	6.4	CVE-2025-8532

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bittokazi--Custom Login And Signup Widget	The Custom Login And Signup Widget plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incorrect nonce validation in the /frndzk_adminclsw.php file. This makes it possible for unauthenticated attackers to change the email and username settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-20	4.3	CVE-2025-9887
blazethemes--Blaze Demo Importer	The Blaze Demo Importer plugin for WordPress is vulnerable to unauthorized limited plugin install due to a missing capability check on the 'blaze_demo_importer_install_plugin' function in all versions up to, and including, 1.0.12. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install and activate a limited number of specific plugins. The News Kit Elementor Addons plugin and a BlazeThemes theme must be installed and activated in order to exploit the vulnerability.	2025-09-16	4.3	CVE-2025-8446
BMC--Control-M/Agent	Control-M/Agents use a kdb or PKCS#12 keystore by default, and the default keystore password is well known and documented. An attacker with read access to the keystore could access sensitive data using this password.	2025-09-16	5.5	CVE-2025-55110
BMC--Control-M/Agent	Certain files with overly permissive permissions were identified in the out-of-support Control-M/Agent versions 9.0.18 to 9.0.20 and potentially earlier unsupported versions as well as in newer versions which were upgraded from an affected version. These files contain keys and passwords relating to SSL files, keystore and policies. An attacker with local access to the system running the Agent can access these files.	2025-09-16	5.5	CVE-2025-55111
BMC--Control-M/Agent	The improper order of AUTHORIZED_CTM_IP validation in the Control-M/Agent, where the Control-M/Server IP address is validated only after the SSL/TLS handshake is completed, exposes the Control-M/Agent to vulnerabilities in the SSL/TLS implementation under certain non-default conditions (e.g. CVE-2025-55117 or CVE-2025-55118) or potentially to resource exhaustion.	2025-09-16	5.3	CVE-2025-55114
BMC--Control-M/Agent	A stack-based buffer overflow can be remotely triggered when formatting an error message in the Control-M/Agent when SSL/TLS communication is configured. The issue occurs in the following cases: * Control-M/Agent 9.0.20: SSL/TLS configuration is set to the non-default setting "use_openssl=n"; * Control-M/Agent 9.0.21 and 9.0.22: Agent router configuration uses the non-default settings "JAVA_AR=N" and "use_openssl=n".	2025-09-16	5.3	CVE-2025-55117
bpedrassani--Browser Sniff	The Browser Sniff plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.3. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-20	6.1	CVE-2025-9883
bplugins--Media Player Addons for Elementor Audio and Video Widgets for Elementor	The Media Player Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'subtitle_ssize', 'track_title', and 'track_artist_name' parameters in version 1.0.5. This is due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-17	6.4	CVE-2025-9203
brainstormforce--SureForms Drag and Drop Contact Form Builder Multi-step Forms, Conversational Forms and more	The SureForms - Drag and Drop Contact Form Builder - Multi-step Forms, Conversational Forms and more plugin for WordPress is vulnerable to unauthorized creation of forms due to a missing capability check on the register_post_types() function in all versions up to, and including, 1.12.0. This makes it possible for authenticated attackers, with Contributor-level access and above, to create forms when the user interface specifically prohibits it.	2025-09-20	4.3	CVE-2025-10489

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Campcodes--Grocery Sales and Inventory System	A vulnerability was identified in Campcodes Grocery Sales and Inventory System 1.0. Affected by this issue is some unknown functionality of the file /index.php?page=users. The manipulation of the argument page leads to cross site scripting. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	2025-09-16	4.3	CVE-2025-10566
CISA--Thorium	CISA Thorium does not adequately validate the paths of downloaded files via 'download_ephemeral' and 'download_children'. A remote, authenticated attacker could access arbitrary files subject to file system permissions. Fixed in 1.1.2.	2025-09-17	5	CVE-2025-35430
CISA--Thorium	CISA Thorium does not escape user controlled strings used in LDAP queries. An authenticated remote attacker can modify LDAP authorization data such as group memberships. Fixed in 1.1.1.	2025-09-17	5.4	CVE-2025-35431
CISA--Thorium	CISA Thorium does not rate limit requests to send account verification email messages. A remote unauthenticated attacker can send unlimited messages to a user who is pending verification. Fixed in 1.1.1 by adding a rate limit set by default to 10 minutes.	2025-09-17	5.3	CVE-2025-35432
CISA--Thorium	CISA Thorium does not properly invalidate previously used tokens when resetting passwords. An attacker that possesses a previously used token could still log in after a password reset. Fixed in 1.1.1.	2025-09-17	5	CVE-2025-35433
CISA--Thorium	CISA Thorium uses '.unwrap()' to handle errors related to account verification email messages. An unauthenticated remote attacker could cause a crash by providing a specially crafted email address or response. Fixed in commit 6a65a27.	2025-09-17	5.3	CVE-2025-35436
CISA--Thorium	CISA Thorium does not validate TLS certificates when connecting to Elasticsearch. An unauthenticated attacker with access to a Thorium cluster could impersonate the Elasticsearch service. Fixed in 1.1.2.	2025-09-17	4.2	CVE-2025-35434
CISA--Thorium	CISA Thorium accepts a stream split size of zero then divides by this value. A remote, authenticated attacker could cause the service to crash. Fixed in commit 89101a6.	2025-09-17	4.3	CVE-2025-35435
clickwhale--ClickWhale Link Manager, Link Shortener and Click Tracker for Affiliate Links & Link Pages	The ClickWhale - Link Manager, Link Shortener and Click Tracker for Affiliate Links & Link Pages plugin for WordPress is vulnerable to SQL Injection via the export_csv() function in all versions up to, and including, 2.5.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This may be exploitable by lower level users if access to the plugin is granted.	2025-09-20	4.9	CVE-2025-10002
codename065--Download Manager	The Download Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'user_ids' parameter in all versions up to, and including, 3.3.23 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.	2025-09-19	6.1	CVE-2025-10146
CosmodiumCS--OnlyRAT	A vulnerability was detected in CosmodiumCS OnlyRAT up to 3.2. The affected element is the function connect/remote_upload/remote_download of the file main.py of the component Configuration File Handler. The manipulation of the argument configuration["PASSWORD"] results in os command injection. The attack requires a local approach. Attacks of this nature are highly complex. The exploitability is described as difficult. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-21	4.5	CVE-2025-10767

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Creality--Cloud App	A flaw has been found in Creality Cloud App up to 6.1.0 on Android. Affected by this vulnerability is an unknown functionality of the file AndroidManifest.xml of the component com.cxsw.sdprinter. Executing manipulation can lead to improper export of android application components. It is possible to launch the attack on the local host. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-19	5.3	CVE-2025-10716
creativethemeshq--Blocksy Companion	The Blocksy Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's blocksy_newsletter_subscribe shortcode in all versions up to, and including, 2.1.10 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.	2025-09-17	6.4	CVE-2025-9565
cyberlord92--User Sync	The User Sync - Remote User Sync plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.2. This is due to missing or incorrect nonce validation on the mo_user_sync_form_handler() function. This makes it possible for unauthenticated attackers to deactivate the plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-17	4.3	CVE-2025-9891
D-Link--DI-8100	A vulnerability has been found in D-Link DI-8100, DI-8100G, DI-8200, DI-8200G, DI-8003 and DI-8003G 16.07.26A1/17.12.20A1/19.12.10A1. Affected by this vulnerability is the function sub_4621DC of the file usb_paswd.asp of the component jhttpd. The manipulation of the argument hname leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-09-15	6.3	CVE-2025-10440
D-Link--DI-8100G	A vulnerability was found in D-Link DI-8100G, DI-8200G and DI-8003G 17.12.20A1/19.12.10A1. Affected by this issue is the function sub_433F7C of the file version_upgrade.asp of the component jhttpd. The manipulation of the argument path results in os command injection. The attack may be launched remotely. The exploit has been made public and could be used.	2025-09-15	6.3	CVE-2025-10441
D-Link--DIR-645	A vulnerability was identified in D-Link DIR-645 105B01. This issue affects the function soapcgi_main of the file /soap.cgi. Such manipulation of the argument service leads to command injection. The attack can be launched remotely. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-09-18	6.3	CVE-2025-10689
D-Link--DIR-823X	A weakness has been identified in D-Link DIR-823X 240126/240802/250416. The impacted element is the function sub_412E7C of the file /usr/sbin/goahead of the component Environment Variable Handler. This manipulation of the argument terminal_addr/server_ip/server_port causes command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	2025-09-18	6.3	CVE-2025-10634
D-Link--DIR-852	A vulnerability was found in D-Link DIR-852 1.00CN B09. This vulnerability affects unknown code of the file /htdocs/cgibin/hedwig.cgi of the component Web Management Interface. Performing manipulation results in command injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-09-18	6.3	CVE-2025-10628
D-Link--DIR-852	A vulnerability was determined in D-Link DIR-852 1.00CN B09. This issue affects the function ssdpcgi_main of the file htodcs/cgibin of the component Simple Service Discovery Protocol Service. Executing manipulation of the argument ST can lead to command injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This vulnerability only affects products that are no longer supported by the maintainer.	2025-09-18	6.3	CVE-2025-10629

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dartiss--Draft List	The Draft List plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'drafts' shortcode in all versions up to, and including, 2.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-20	6.4	CVE-2025-10181
DigitalOcean--@digitalocean/do-markdownit	In the @digitalocean/do-markdownit package through 1.16.1 (in npm), the callout and fence_environment plugins perform .includes substring matching if allowedClasses or allowedEnvironments is a string (instead of an array).	2025-09-19	5.4	CVE-2025-59717
Dolusoft--Omaspot	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Dolusoft Omaspot allows Reflected XSS.This issue affects Omaspot: before 12.09.2025.	2025-09-16	5.4	CVE-2025-6575
Enalean--tuleap	Tuleap is an Open Source Suite to improve management of software developments and collaboration. Backlog item representations do not verify the permissions of the child trackers. Users might see tracker names they should not have access to. This vulnerability is fixed in Tuleap Community Edition 16.11.99.1757427600 and Tuleap Enterprise Edition 16.11-6 and 16.10-8.	2025-09-18	4.3	CVE-2025-59040
endisha--Secure Passkeys	The Secure Passkeys plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the delete_passkey() and passkeys_list() function in all versions up to, and including, 1.2.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view and delete passkeys.	2025-09-20	5.3	CVE-2025-10305
Ericsson--Ericsson Catalog Manager	Ericsson Catalog Manager and Ericsson Order Care APIs do not have authentication enabled by default. Authentication checks can be configured to remediate the information disclosure issue.	2025-09-18	5.3	CVE-2024-25011
eskapism--Developer Loggers for Simple History	The Developer Loggers for Simple History plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 0.5 via the enabled_loggers parameter. This makes it possible for authenticated attackers, with Administrator-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	2025-09-17	6.6	CVE-2025-10050
extendthemes--Kubio AI Page Builder	The Kubio AI Page Builder plugin for WordPress is vulnerable to unauthorized plugin installation due to a missing capability check on the kubio-image-hub-install-plugin AJAX action in all versions up to, and including, 2.6.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install the Image Hub plugin.	2025-09-19	5.4	CVE-2025-8487
Four-Faith--Water Conservancy Informatization Platform	A security vulnerability has been detected in Four-Faith Water Conservancy Informatization Platform 1.0. Affected by this vulnerability is an unknown functionality of the file /history/historyDownload.do;usrlogout.do. The manipulation of the argument fileName leads to path traversal. Remote exploitation of the attack is possible. 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.	2025-09-19	5.3	CVE-2025-10708
Four-Faith--Water Conservancy Informatization Platform	A vulnerability was detected in Four-Faith Water Conservancy Informatization Platform 1.0. Affected by this issue is some unknown functionality of the file /history/historyDownload.do;otheruserLogin.do;getfile. The manipulation of the argument fileName results in path traversal. The attack can be executed remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-19	5.3	CVE-2025-10709
frappe--lms	Frappe Learning is a learning system that helps users structure their content. In versions 2.34.1 and below, there is a security vulnerability in Frappe Learning where the system did not adequately sanitize the content uploaded in the profile	2025-09-17	4.6	CVE-2025-59415

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bio. Malicious SVG files could be used to execute arbitrary scripts in the context of other users.			
fuyang_lipengjun--platform	A vulnerability was identified in fuyang_lipengjun platform 1.0. This affects the function AttributeCategoryController of the file /attributecategory/queryAll. Such manipulation leads to improper authorization. The attack may be launched remotely. The exploit is publicly available and might be used.	2025-09-18	4.3	CVE-2025-10674
fuyang_lipengjun--platform	A security flaw has been discovered in fuyang_lipengjun platform 1.0. This impacts the function AttributeController of the file /attribute/queryAll. Performing manipulation results in improper authorization. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.	2025-09-18	4.3	CVE-2025-10675
fuyang_lipengjun--platform	A weakness has been identified in fuyang_lipengjun platform 1.0. Affected is the function BrandController of the file /brand/queryAll. Executing manipulation can lead to improper authorization. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.	2025-09-18	4.3	CVE-2025-10676
gentlesource--Appointmind	The Appointmind plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'appointmind_calendar' shortcode in all versions up to, and including, 4.1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-17	6.4	CVE-2025-9851
GNU--Guix	In guix-daemon in GNU Guix before 1618ca7, a content-addressed-mirrors file can be written to create a setuid program that allows a regular user to gain the privileges of the build user that runs it (even after the build has ended).	2025-09-15	5.7	CVE-2025-59378
Grafana--grafana-zabbix-plugin	Grafana is an open-source platform for monitoring and observability. Grafana-Zabbix is a plugin for Grafana allowing to visualize monitoring data from Zabbix and create dashboards for analyzing metrics and realtime monitoring. Versions 5.2.1 and below contained a ReDoS vulnerability via user-supplied regex query which could causes CPU usage to max out. This vulnerability is fixed in version 6.0.0.	2025-09-19	4.3	CVE-2025-10630
h2oai--h2o-3	A flaw has been found in h2oai h2o-3 up to 3.46.08. The impacted element is an unknown function of the file /99/ImportSQLTable of the component IBMDB2 JDBC Driver. This manipulation of the argument connection_url causes deserialization. The attack may be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-21	6.3	CVE-2025-10768
h2oai--h2o-3	A vulnerability has been found in h2oai h2o-3 up to 3.46.08. This affects an unknown function of the file /99/ImportSQLTable of the component H2 JDBC Driver. Such manipulation of the argument connection_url leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-21	6.3	CVE-2025-10769
harry0703--MoneyPrinterTurbo	A vulnerability has been found in harry0703 MoneyPrinterTurbo up to 1.2.6. The impacted element is the function download_video/stream_video of the file app/controllers/v1/video.py of the component URL Handler. The manipulation of the argument file_path leads to path traversal. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-09-15	5.3	CVE-2025-10472
Hewlett Packard Enterprise (HPE)--HPE Aruba Networking ClearPass Policy Manager	A vulnerability in the web-based management interface of network access control services could allow an unauthenticated remote attacker to conduct a Reflected Cross-Site Scripting (XSS) attack. Successful exploitation could allow an attacker to execute arbitrary JavaScript code in a victim's browser in the context of the affected interface.	2025-09-17	6.1	CVE-2025-37122

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Hewlett Packard Enterprise (HPE)--HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability in the web API of HPE Aruba Networking EdgeConnect SD-WAN Gateways could allow an authenticated remote attacker to terminate arbitrary running processes. Successful exploitation could allow an attacker to disrupt system operations, potentially resulting in an unstable system state.	2025-09-16	6.8	CVE-2025-37128
Hewlett Packard Enterprise (HPE)--HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerable feature in the command line interface of EdgeConnect SD-WAN could allow an authenticated attacker to exploit built-in script execution capabilities. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system if the feature is enabled without proper security measures.	2025-09-16	6.7	CVE-2025-37129
Hewlett Packard Enterprise (HPE)--HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability in the command-line interface of EdgeConnect SD-WAN could allow an authenticated attacker to read arbitrary files within the system. Successful exploitation could allow an attacker to read sensitive data from the underlying file system.	2025-09-16	6.5	CVE-2025-37130
Hewlett Packard Enterprise (HPE)--HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability in EdgeConnect SD-WAN ECOS could allow an authenticated remote threat actor with admin privileges to access sensitive unauthorized system files. Under certain conditions, this could lead to exposure and exfiltration of sensitive information.	2025-09-16	4.9	CVE-2025-37131
Holistic IT, Consultancy Coop.--Workcube ERP	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Holistic IT, Consultancy Coop. Workcube ERP allows Reflected XSS.This issue affects Workcube ERP: from V12 - V14 before Cognitive.	2025-09-16	5.3	CVE-2024-12796
huggingface--LeRobot	A vulnerability was identified in huggingface LeRobot up to 0.3.3. Affected by this vulnerability is an unknown functionality of the file lerobot/common/robot_devices/robots/lekiwi_remote.py of the component ZeroMQ Socket Handler. The manipulation leads to missing authentication. The attack can only be initiated within the local network. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-21	6.3	CVE-2025-10772
I-O DATA DEVICE, INC.--WN-7D36QR	Hidden functionality issue exists in WN-7D36QR and WN-7D36QR/UE. If this vulnerability is exploited, SSH may be enabled by a remote authenticated attacker.	2025-09-17	4.9	CVE-2025-55075
IBM--Copy Services Manager	IBM Copy Services Manager 6.3.13 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-09-19	5.4	CVE-2025-36248
IBM--OpenPages	IBM OpenPages 9.0 and 9.1 allows web page cache to be stored locally which can be read by another user on the system.	2025-09-15	4	CVE-2025-36082
IBM--watsonx.data	IBM Lakehouse (watsonx.data 2.2) is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-09-18	5.5	CVE-2025-36139
IBM--watsonx.data	IBM Lakehouse (watsonx.data 2.2) could allow an authenticated privileged user to execute arbitrary commands on the system due to improper validation of user supplied input.	2025-09-18	4.7	CVE-2025-36143
IBM--watsonx.data	IBM Lakehouse (watsonx.data 2.2) could allow an authenticated user to obtain sensitive server component version information which could aid in further attacks against the system.	2025-09-18	4.3	CVE-2025-36146

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
igniterealtime--Openfire	Openfire is an XMPP server licensed under the Open Source Apache License. Openfire's SASL EXTERNAL mechanism for client TLS authentication contains a vulnerability in how it extracts user identities from X.509 certificates. Instead of parsing the structured ASN.1 data, the code calls X509Certificate.getSubjectDN().getName() and applies a regex to look for CN=. This method produces a provider-dependent string that does not escape special characters. In SunJSSE (sun.security.x509.X500Name), for example, commas and equals signs inside attribute values are not escaped. As a result, a malicious certificate can embed CN= inside another attribute value (e.g. OU="CN=admin,"). The regex will incorrectly interpret this as a legitimate Common Name and extract admin. If SASL EXTERNAL is enabled and configured to map CNs to user accounts, this allows the attacker to impersonate another user. The fix is included in Openfire 5.0.2 and 5.1.0.	2025-09-15	5.9	CVE-2025-59154
Internet2--Grouper	In Internet2 Grouper 5.17.1 before 5.20.5, group admins who are not Grouper sysadmins can configure loader jobs.	2025-09-19	6.5	CVE-2025-59714
intsig--CamScanner App	A vulnerability has been found in intsig CamScanner App 6.91.1.5.250711 on Android. Affected by this issue is some unknown functionality of the file AndroidManifest.xml of the component com.intsig.camscanner. The manipulation leads to improper export of android application components. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-19	5.3	CVE-2025-10717
itsourcecode--E-Commerce Website	A vulnerability was identified in itsourcecode E-Commerce Website 1.0. This impacts an unknown function of the file /admin/products.php. The manipulation leads to unrestricted upload. The attack can be initiated remotely. The exploit is publicly available and might be used.	2025-09-17	6.3	CVE-2025-10615
itsourcecode--E-Commerce Website	A security flaw has been discovered in itsourcecode E-Commerce Website 1.0. Affected is an unknown function of the file /admin/users.php. The manipulation results in unrestricted upload. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	2025-09-17	6.3	CVE-2025-10616
itsourcecode--E-Logbook with Health Monitoring System for COVID-19	A vulnerability was determined in itsourcecode E-Logbook with Health Monitoring System for COVID-19 1.0 on COVID. This affects an unknown function of the file /print_reports_prev.php. Executing manipulation of the argument profile_id can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-17	4.3	CVE-2025-10614
itsourcecode--Online Clinic Management System	A security vulnerability has been detected in itsourcecode Online Clinic Management System 1.0. Affected by this issue is some unknown functionality of the file transact.php. Such manipulation of the argument firstname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. Other parameters might be affected as well.	2025-09-17	6.3	CVE-2025-10618
itsourcecode--Online Clinic Management System	A flaw has been found in itsourcecode Online Clinic Management System 1.0. This vulnerability affects unknown code of the file /editp2.php. Executing manipulation of the argument id/firstname/lastname/type/age/address can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	2025-09-17	6.3	CVE-2025-10620
itsourcecode--Online Public Access Catalog OPAC	A security vulnerability has been detected in itsourcecode Online Public Access Catalog OPAC 1.0. This impacts an unknown function of the file mysearch.php of the component POST Parameter Handler. Such manipulation of the argument search_field/search_text leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	2025-09-17	6.3	CVE-2025-10592
itsourcecode--Student	A vulnerability has been found in itsourcecode Student Information System 1.0. The affected element is an unknown function of the file /leveledit1.php. Such manipulation of the argument level_id leads to sql injection. The attack may be	2025-09-17	6.3	CVE-2025-10613

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Information System	performed from remote. The exploit has been disclosed to the public and may be used.			
jeecgboot--JimuReport	A vulnerability was found in jeecgboot JimuReport up to 2.1.2. This impacts an unknown function of the file /drag/onlDragDataSource/testConnection of the component MySQL JDBC Handler. Performing manipulation results in deserialization. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	2025-09-21	6.3	CVE-2025-10770
jeecgboot--JimuReport	A vulnerability was determined in jeecgboot JimuReport up to 2.1.2. Affected is an unknown function of the file /drag/onlDragDataSource/testConnection of the component DB2 JDBC Handler. Executing manipulation of the argument clientRerouteServerListJNDIName can lead to deserialization. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-21	6.3	CVE-2025-10771
JetBrains--TeamCity	In JetBrains TeamCity before 2025.07.2 path traversal was possible during project archive upload	2025-09-17	5.5	CVE-2025-59456
JetBrains--TeamCity	In JetBrains TeamCity before 2025.07.2 project isolation bypass was possible due to race condition	2025-09-17	4.2	CVE-2025-59455
kidaze--CourseSelectionSystem	A vulnerability was identified in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. The affected element is an unknown function of the file /Profilers/PriProfile/eligibility.php. Such manipulation of the argument Branch leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	2025-09-15	6.3	CVE-2025-10477
kidaze--CourseSelectionSystem	A vulnerability was identified in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. Affected is an unknown function of the file /Profilers/PProfile/COUNT3s3.php. The manipulation of the argument csem leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided.	2025-09-18	6.3	CVE-2025-10665
kodezen--StoreEngine Powerful WordPress eCommerce Plugin for Payments, Memberships, Affiliates, Sales & More	The StoreEngine - Powerful WordPress eCommerce Plugin for Payments, Memberships, Affiliates, Sales & More plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.5.0 via the file_download() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	2025-09-17	6.5	CVE-2025-9215
kuaifan--DooTask	A vulnerability was found in kuaifan DooTask up to 1.2.49. Affected by this vulnerability is an unknown functionality of the file app/Http/Controllers/Api/UsersController.php. The manipulation of the argument keys[department] results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	2025-09-21	6.3	CVE-2025-10762
Kubernetes--Kubernetes CSharp Client	A vulnerability exists in the Kubernetes C# client where the certificate validation logic accepts properly constructed certificates from any Certificate Authority (CA) without properly verifying the trust chain. This flaw allows a malicious actor to present a forged certificate and potentially intercept or manipulate communication with the Kubernetes API server, leading to possible man-in-the-middle attacks and API impersonation.	2025-09-16	6.8	CVE-2025-9708

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
LDAPAccountManager--lam	LDAP Account Manager (LAM) is a webfrontend for managing entries stored in an LDAP directory. LAM before 9.3 allows stored cross-site scripting in the Profile section via the profile name field, which renders untrusted input as HTML and executes a supplied script (for example a script element). An authenticated user with permission to create or edit a profile can insert a script payload into the profile name and have it executed when the profile data is viewed in a browser. This issue is fixed in version 9.3. No known workarounds are mentioned.	2025-09-16	4.6	CVE-2025-58174
Libraesva--Email Security Gateway	Libraesva ESG 4.5 through 5.5.x before 5.5.7 allows command injection via a compressed e-mail attachment. For ESG 5.0 a fix has been released in 5.0.31. For ESG 5.1 a fix has been released in 5.1.20. For ESG 5.2 a fix has been released in 5.2.31. For ESG 5.4 a fix has been released in 5.4.8. For ESG 5.5. a fix has been released in 5.5.7.	2025-09-19	6.1	CVE-2025-59689
Mattermost--Mattermost	Mattermost versions 10.10.x <= 10.10.1 fail to properly sanitize user data during shared channel membership synchronization, which allows malicious or compromised remote clusters to access sensitive user information via unsanitized user objects. This vulnerability affects Mattermost Server instances with shared channels enabled.	2025-09-15	6.5	CVE-2025-9076
Mattermost--Mattermost	Mattermost versions 10.8.x <= 10.8.3, 10.5.x <= 10.5.8, 9.11.x <= 9.11.17, 10.10.x <= 10.10.1, 10.9.x <= 10.9.3 fail to properly validate cache keys for link metadata which allows authenticated users to access unauthorized posts and poison link previews via hash collision attacks on FNV-1 hashing	2025-09-15	4.3	CVE-2025-9078
Mevzuattr Software--MevzuatTR	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting'), Improper Restriction of Rendered UI Layers or Frames vulnerability in Mevzuattr Software MevzuatTR allows Phishing, iFrame Overlay, Clickjacking, Forceful Browsing. This issue needs high privileges. This issue affects MevzuatTR: before 12.02.2025.	2025-09-17	4.7	CVE-2025-0546
michaelbo--osTicket WP Bridge	The osTicket WP Bridge plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.9.2. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-20	6.1	CVE-2025-9882
Microsoft--Microsoft Edge (Chromium-based)	Insufficient ui warning of dangerous operations in Microsoft Edge for Android allows an unauthorized attacker to perform spoofing over a network.	2025-09-16	4.7	CVE-2025-47967
Microsoft--Microsoft PC Manager	Cleartext storage of sensitive information in Microsoft PC Manager allows an unauthorized attacker to bypass a security feature locally.	2025-09-16	4	CVE-2025-49728
Mitsubishi Electric Corporation--MELSEC-Q Series Q03UDVCPU	Improper Handling of Length Parameter Inconsistency vulnerability in Mitsubishi Electric Corporation MELSEC-Q Series Q03UDVCPU, Q04UDVCPU, Q06UDVCPU, Q13UDVCPU, Q26UDVCPU, Q04UDPVCPU, Q06UDPVCPU, Q13UDPVCPU, and Q26UDPVCPU with the first 5 digits of serial No. "24082" to "27081" allows a remote attacker to cause an integer underflow by sending specially crafted packets to the affected product to stop Ethernet communication and the execution of control programs on the product, when the user authentication function is enabled. The user authentication function is enabled by default only when settings are configured by GX Works2, which complies with the Cybersecurity Law of the People's Republic of China, and is normally disabled.	2025-09-19	6.8	CVE-2025-8531
n/a--07FLYCMS	A flaw has been found in 07FLYCMS, 07FLY-CMS and 07FlyCRM up to 20250831. This affects an unknown part of the file /index.php. This manipulation of the argument Name causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been published and may be used. This product is	2025-09-19	4.3	CVE-2025-10710

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	published under multiple names. The vendor was contacted early about this disclosure but did not respond in any way.			
n/a--07FLYCMS	A vulnerability has been found in 07FLYCMS, 07FLY-CMS and 07FlyCRM up to 20250831. This vulnerability affects unknown code of the file /index.php/sysmanage/Login. Such manipulation of the argument Name leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. This product is published under multiple names. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-19	4.3	CVE-2025-10711
n/a--Airsonic-Advanced	A vulnerability was detected in Airsonic-Advanced up to 10.6.0. This vulnerability affects unknown code of the component Playlist Upload Handler. Performing manipulation results in unrestricted upload. It is possible to initiate the attack remotely. The exploit is now public and may be used.	2025-09-18	6.3	CVE-2025-10669
n/a--Harness	A flaw has been found in Harness 3.3.0. This impacts the function LookupRepo of the file app/api/controller/gitspace/lookup_repo.go. Executing manipulation of the argument url can lead to server-side request forgery. The attack may be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-21	6.3	CVE-2025-10760
n/a--JeecgBoot	A weakness has been identified in JeecgBoot up to 3.8.2. Affected is an unknown function of the file /message/sysMessageTemplate/sendMsg. Executing manipulation can lead to improper authorization. The attack may be launched remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-19	6.3	CVE-2025-10707
n/a--newbee-mall	A vulnerability has been found in newbee-mall up to 613a662adf1da7623ec34459bc83e3c1b12d8ce7. This issue affects the function paySuccess of the file /paySuccess of the component Order Status Handler. The manipulation of the argument orderNo leads to improper authorization. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided.	2025-09-15	4.3	CVE-2025-10422
n/a--SeaCMS	A vulnerability has been found in SeaCMS up to 13.3. The impacted element is an unknown function of the file /admin_members.php?ac=editsave. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This affects another injection point than CVE-2025-25513.	2025-09-18	4.7	CVE-2025-10662
n/a--SpyShelter	A weakness has been identified in SpyShelter up to 15.4.0.1015. Affected is an unknown function in the library SpyShelter.sys of the component IOCTL Handler. This manipulation causes denial of service. The attack needs to be launched locally. The exploit has been made available to the public and could be exploited. Upgrading to version 15.4.0.1028 is able to address this issue. It is advisable to upgrade the affected component.	2025-09-15	5.5	CVE-2025-10475
n/a--ZKEACMS	A vulnerability was detected in ZKEACMS 4.3. Impacted is the function Proxy of the file src/ZKEACMS/Controllers/MediaController.cs. Performing manipulation of the argument url results in server-side request forgery. It is possible to initiate the attack remotely. The exploit is now public and may be used.	2025-09-15	6.3	CVE-2025-10471
n8n-io--n8n	n8n is an open source workflow automation platform. From 1.24.0 to before 1.107.0, there is a stored cross-site scripting (XSS) vulnerability in @n8n/n8n-nodes-langchain.chatTrigger. An authorized user can configure the LangChain Chat Trigger node with malicious JavaScript in the initialMessages field and enable public access so that the payload is executed in the browser of any user who visits the resulting public chat URL. This can be used for phishing or to steal cookies or other sensitive data from users accessing the public chat link. The issue is fixed in	2025-09-15	5.4	CVE-2025-58177

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	version 1.107.0. Updating to 1.107.0 or later is recommended. As a workaround, the affected chatTrigger node can be disabled. No other workarounds are known.			
NetApp--StorageGRID	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8.0.15 and 11.9.0.8 are susceptible to a Reflected Cross-Site Scripting vulnerability. Successful exploit could allow an attacker to view or modify configuration settings or add or modify user accounts but requires the attacker to know specific information about the target instance and then trick a privileged user into clicking a specially crafted link.	2025-09-19	6.4	CVE-2025-26514
NetApp--StorageGRID	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8.0.15 and 11.9.0.8 are susceptible to a Denial of Service vulnerability. Successful exploit could allow an unauthenticated attacker to cause a Denial of Service on the Admin node.	2025-09-19	5.3	CVE-2025-26516
NetApp--StorageGRID	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8.0.15 and 11.9.0.8 are susceptible to a privilege escalation vulnerability. Successful exploit could allow an unauthorized authenticated attacker to discover Grid node names and IP addresses or modify Storage Grades.	2025-09-19	5.4	CVE-2025-26517
nko--Ghost Kit Page Builder Blocks, Motion Effects & Extensions	The Ghost Kit - Page Builder Blocks, Motion Effects & Extensions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom JS field in all versions up to, and including, 3.4.3 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.	2025-09-18	6.4	CVE-2025-9992
NVIDIA--HGX GB200, HGX GB300, HGC B300	NVIDIA HGX & DGX GB200, GB300, B300 contain a vulnerability in the HGX Management Controller (HMC) that may allow a malicious actor with administrative access on the BMC to access the HMC as an administrator. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2025-09-17	6.7	CVE-2025-23337
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server for Windows and Linux contains a vulnerability where an attacker could cause a denial of service by loading a misconfigured model. A successful exploit of this vulnerability might lead to denial of service.	2025-09-17	4.4	CVE-2025-23336
OMRON SOCIAL SOLUTIONS CO., Ltd.--PowerAttendant Standard Edition	A vulnerability (CWE-428) has been identified in the Uninterruptible Power Supply (UPS) management application provided by OMRON SOCIAL SOLUTIONS Co., Ltd., where the executable file paths of Windows services are not enclosed in quotation marks. If the installation folder path of this product contains spaces, there is a possibility that unauthorized files may be executed under the service privileges by using paths containing spaces.	2025-09-17	6.7	CVE-2025-9818
Ooma--Office Business Phone App	A vulnerability was found in Ooma Office Business Phone App up to 7.2.2 on Android. This affects an unknown part of the component com.ooma.office2. The manipulation results in improper export of android application components. The attack needs to be approached locally. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-19	5.3	CVE-2025-10718
openwebanalytics--Open Web Analytics	Open Web Analytics (OWA) before 1.8.1 allows SQL injection.	2025-09-15	5	CVE-2025-59397
Oracle Corporation--OpenGrok	OpenGrok 1.14.1 has a reflected Cross-Site Scripting (XSS) issue when producing the cross reference page. This happens through improper handling of the revision parameter. The application reflects unsanitized user input into the HTML output.	2025-09-18	6.1	CVE-2025-30755
ovh--the-bastion	The Bastion provides authentication, authorization, traceability and auditability for SSH accesses. Session-recording ttyrec files, may be handled by the provided osh-encrypt-rsync script that is a helper to rotate, encrypt, sign, copy, and optionally move them to a remote storage periodically, if configured to. When running, the	2025-09-17	4.4	CVE-2025-59339

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	script properly rotates and encrypts the files using the provided GPG key(s), but silently fails to sign them, even if asked to.			
Parat Software--Bizmu	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Paraşüt Software Bizmu allows Cross-Site Scripting (XSS).This issue affects Bizmu: from 2.27.0 through 20250212.	2025-09-18	4.7	CVE-2025-0547
Parat Software--Parat	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Paraşüt Software Paraşüt allows Cross-Site Scripting (XSS).This issue affects Paraşüt: from 0.0.0.65efa44e through 20250204.	2025-09-17	4.7	CVE-2025-0420
Patika Global Technologies--HumanSuite	Authorization Bypass Through User-Controlled Key, Externally Controlled Reference to a Resource in Another Sphere, Improper Authorization vulnerability in Patika Global Technologies HumanSuite allows Exploiting Trust in Client.This issue affects HumanSuite: before 53.21.0.	2025-09-16	6.5	CVE-2025-8057
PilotGaea Technologies--O'View MapServer	O'View MapServer developed by PilotGaea Technologies has a Server-Side Request Forgery vulnerability, allowing unauthenticated remote attackers to exploit this vulnerability to probe internal network.	2025-09-15	5.3	CVE-2025-10453
pojoin--h3blog	A vulnerability has been found in pojoin h3blog up to 5bf704425ebc11f4c24da51f32f36bb17ae20489. Affected by this issue is the function ppt_log of the file /login of the component HTTP Header Handler. Such manipulation of the argument X-Forwarded-For leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed.	2025-09-15	4.3	CVE-2025-10485
Portabilis--i-Educar	A vulnerability was detected in Portabilis i-Educar up to 2.10. The affected element is an unknown function of the file /enrollment-history/. Performing manipulation results in improper access controls. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2025-09-17	6.3	CVE-2025-10608
Portabilis--i-Educar	A security flaw has been discovered in Portabilis i-Educar up to 2.10. The impacted element is an unknown function of the file /intranet/educar_usuario_det.php. The manipulation of the argument ref_pessoa results in cross site scripting. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	2025-09-17	4.3	CVE-2025-10590
Portabilis--i-Educar	A security flaw has been discovered in Portabilis i-Educar up to 2.10. This vulnerability affects unknown code of the file /agenda_preferencias.php. The manipulation of the argument tipoacao results in cross site scripting. The attack may be launched remotely. The exploit has been released to the public and may be exploited.	2025-09-17	4.3	CVE-2025-10605
Portabilis--i-Educar	A weakness has been identified in Portabilis i-Educar up to 2.10. This issue affects some unknown processing of the file /module/Configuracao/ConfiguracaoMovimentoGeral. This manipulation of the argument tipoacao causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	2025-09-17	4.3	CVE-2025-10606
Portabilis--i-Educar	A security vulnerability has been detected in Portabilis i-Educar up to 2.10. Impacted is an unknown function of the file /module/Avaliacao/diarioApi. Such manipulation leads to information disclosure. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	2025-09-17	4.3	CVE-2025-10607
prasunsen--Chained Quiz	The Chained Quiz plugin for WordPress is vulnerable to Insecure Direct Object Reference in version 1.3.4 and below via the quiz submission and completion mechanisms due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to hijack and modify other users' quiz attempts by manipulating the chained_completion_id cookie value, allowing them	2025-09-18	5.3	CVE-2025-10493

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to alter quiz answers, scores, and results of any user. The vulnerability was partially patched in versions 1.3.4 and 1.3.5.			
productiveminds--Productive Style Optimisations & Content Publishing Support	The Productive Style plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's display_productive_breadcrumb shortcode in all versions up to, and including, 1.1.23 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.	2025-09-17	6.4	CVE-2025-8394
psmplugins--SupportCandy Helpdesk & Customer Support Ticket System	The SupportCandy - Helpdesk & Customer Support Ticket System plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 3.3.7. This is due to missing rate limiting on the OTP verification for guest login. This makes it possible for unauthenticated attackers to bypass authentication and gain unauthorized access to customer support tickets by brute forcing the 6-digit OTP code.	2025-09-20	6.5	CVE-2025-10658
Pusula Communication Information Internet Industry and Trade Ltd. Co.--Manageable Email Sending System	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Pusula Communication Information Internet Industry and Trade Ltd. Co. Manageable Email Sending System allows Exploiting Trust in Client.This issue affects Manageable Email Sending System: from <=2025.06 before 2025.08.06.	2025-09-19	4.7	CVE-2025-7702
robcore89--Robcore Netatmo	The Robcore Netatmo plugin for WordPress is vulnerable to SQL Injection via the 'module_id' attribute of the robcore-netatmo shortcode in all versions up to, and including, 1.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-20	6.5	CVE-2025-10652
Saysis Computer Systems Trade Ltd. Co.--StarCities E-Municipality Management	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Saysis Computer Systems Trade Ltd. Co. StarCities E-Municipality Management allows Cross-Site Scripting (XSS).This issue affects StarCities E-Municipality Management: before 20250825.	2025-09-19	6.3	CVE-2025-8664
SecHard Information Technologies--SecHard	Authorization Bypass Through User-Controlled Key vulnerability in SecHard Information Technologies SecHard allows Parameter Injection.This issue affects SecHard: before 3.6.2-20250805.	2025-09-17	5.3	CVE-2025-8463
Selleo--Mentingo	A security vulnerability has been detected in Selleo Mentingo up to 2025.08.27. The affected element is an unknown function of the component Profile Picture Handler. The manipulation of the argument userAvatar leads to unrestricted upload. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-20	6.3	CVE-2025-10741
Selleo--Mentingo	A vulnerability was detected in Selleo Mentingo 2025.08.27. The impacted element is an unknown function of the component Content-Type Handler. The manipulation of the argument userAvatar results in unrestricted upload. The attack may be performed from remote. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-20	6.3	CVE-2025-10755
sequa-ai--sequa-mcp	A vulnerability was detected in sequa-ai sequa-mcp up to 1.0.13. This affects the function redirectToAuthorization of the file src/helpers/node-oauth-client-provider.ts of the component OAuth Server Discovery. Performing manipulation results in os command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used. Upgrading to version 1.0.14 is able to	2025-09-17	6.3	CVE-2025-10619

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mitigate this issue. The patch is named e569815854166db5f71c2e722408f8957fb9e804. It is recommended to upgrade the affected component. The vendor explains: "We only promote that mcp server with our own URLs that have a valid response, but yes if someone would use it with a non sequa url, this is a valid attack vector. We have released a new version (1.0.14) that fixes this and validates that only URLs can be opened."			
SeriaWei--ZKEACMS	A vulnerability was identified in SeriaWei ZKEACMS up to 4.3. This affects the function Edit of the file src/ZKEACMS.EventAction/Controllers/PendingTaskController.cs of the component Event Action System. Such manipulation of the argument Data leads to server-side request forgery. The attack may be performed from remote. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-21	6.3	CVE-2025-10764
SeriaWei--ZKEACMS	A security flaw has been discovered in SeriaWei ZKEACMS up to 4.3. This vulnerability affects the function CheckPage/Suggestions in the library cms-v4.3\wwwroot\Plugins\ZKEACMS.SEOSuggestions\ZKEACMS.SEOSuggestions.dll of the component SEOSuggestions. Performing manipulation results in server-side request forgery. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-21	4.7	CVE-2025-10765
SeriaWei--ZKEACMS	A weakness has been identified in SeriaWei ZKEACMS up to 4.3. This issue affects the function Download of the file EventViewerController.cs. Executing manipulation of the argument ID can lead to path traversal. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-21	4.3	CVE-2025-10766
shenyanzhi--USS Upyun	The USS Upyun plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5.0. This is due to missing or incorrect nonce validation on the uss_setting_page function when processing the uss_set form type. This makes it possible for unauthenticated attackers to modify critical Upyun cloud storage settings including bucket name, operator credentials, upload paths, and image processing parameters via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-17	4.3	CVE-2025-9629
Shopside Software--Shopside App	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Shopside Software Shopside App allows Cross-Site Scripting (XSS). This issue requires high privileges.This issue affects Shopside App: before 17.02.2025.	2025-09-17	4.7	CVE-2025-0879
SKTLab--Mukbee App	A vulnerability was detected in SKTLab Mukbee App 1.01.196 on Android. This affects an unknown function of the file AndroidManifest.xml of the component com.dw.android.mukbee. The manipulation results in improper export of android application components. The attack must be initiated from a local position. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-19	5.3	CVE-2025-10722
SMCI--MBD-X12STW	There is a vulnerability in the Supermicro BMC firmware validation logic at Supermicro MBD-X12STW . An attacker can update the system firmware with a specially crafted image.	2025-09-19	6.6	CVE-2025-7937
SMCI--X13SEM-F	There is a vulnerability in the Supermicro BMC firmware validation logic at Supermicro MBD-X13SEM-F . An attacker can update the system firmware with a specially crafted image.	2025-09-19	6.4	CVE-2025-6198
SMSEagle--SMSEagle	SMSEagle before 6.11 allows reflected XSS via a username or contact phone number.	2025-09-19	4.8	CVE-2025-59715

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
snipeitapp--Snipe-IT	Snipe-IT before 8.1.18 allows XSS.	2025-09-19	6.4	CVE-2025-59712
snipeitapp--Snipe-IT	Snipe-IT before 8.1.18 allows unsafe deserialization.	2025-09-19	6.8	CVE-2025-59713
SourceCodester--Online Exam Form Submission	A vulnerability was found in SourceCodester Online Exam Form Submission 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/delete_s1.php. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	2025-09-17	6.3	CVE-2025-10602
SourceCodester--Online Exam Form Submission	A vulnerability was detected in SourceCodester Online Exam Form Submission 1.0. Affected by this vulnerability is an unknown functionality of the file /user/dashboard.php?page=update_profile. The manipulation of the argument phone results in sql injection. The attack may be launched remotely. The exploit is now public and may be used. Other parameters might be affected as well.	2025-09-17	6.3	CVE-2025-10625
SourceCodester--Online Exam Form Submission	A flaw has been found in SourceCodester Online Exam Form Submission 1.0. Affected by this issue is some unknown functionality of the file /admin/update_s3.php. This manipulation of the argument credits causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	2025-09-17	6.3	CVE-2025-10626
SourceCodester--Online Exam Form Submission	A vulnerability has been found in SourceCodester Online Exam Form Submission 1.0. This affects an unknown part of the file /admin/delete_user.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	2025-09-17	6.3	CVE-2025-10627
SourceCodester--Online Polling System	A weakness has been identified in SourceCodester Online Polling System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/positions.php. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	2025-09-17	6.3	CVE-2025-10617
SourceCodester--Online Student File Management System	A weakness has been identified in SourceCodester Online Student File Management System 1.0. This affects an unknown function of the file /save_file.php. Executing manipulation can lead to unrestricted upload. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	2025-09-15	6.3	CVE-2025-10480
SourceCodester--Online Student File Management System	A security vulnerability has been detected in SourceCodester Online Student File Management System 1.0. This impacts an unknown function of the file /remove_file.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	2025-09-15	6.3	CVE-2025-10481
SourceCodester--Online Student File Management System	A flaw has been found in SourceCodester Online Student File Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/save_user.php. This manipulation of the argument firstname causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. Other parameters might be affected as well.	2025-09-15	6.3	CVE-2025-10483
SourceCodester--Online Student File Management System	A vulnerability was detected in SourceCodester Online Student File Management System 1.0. Affected is an unknown function of the file /admin/update_student.php. Performing manipulation of the argument stud_id results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	2025-09-17	6.3	CVE-2025-10593
SourceCodester--Online Student File	A flaw has been found in SourceCodester Online Student File Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/delete_student.php. Executing manipulation of the argument stud_id can	2025-09-17	6.3	CVE-2025-10594

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.			
SourceCodester--Online Student File Management System	A vulnerability has been found in SourceCodester Online Student File Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/delete_user.php. The manipulation of the argument user_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-09-17	6.3	CVE-2025-10595
SourceCodester--Pet Grooming Management Software	A weakness has been identified in SourceCodester Pet Grooming Management Software 1.0. This impacts an unknown function of the file /admin/operation/user.php. Executing manipulation of the argument website_image can lead to unrestricted upload. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited.	2025-09-15	6.3	CVE-2025-10427
SourceCodester--Pet Grooming Management Software	A security vulnerability has been detected in SourceCodester Pet Grooming Management Software 1.0. Affected is an unknown function of the file /admin/seo_setting.php of the component Setting Handler. The manipulation of the argument website_image leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	2025-09-15	6.3	CVE-2025-10428
SourceCodester--Pet Grooming Management Software	A vulnerability was detected in SourceCodester Pet Grooming Management Software 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/ajax_product.php. The manipulation of the argument drop_services results in sql injection. The attack can be launched remotely. The exploit is now public and may be used.	2025-09-15	6.3	CVE-2025-10429
SourceCodester--Pet Grooming Management Software	A flaw has been found in SourceCodester Pet Grooming Management Software 1.0. Affected by this issue is some unknown functionality of the file /admin/barcode.php. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	2025-09-15	6.3	CVE-2025-10430
SourceCodester--Pet Grooming Management Software	A vulnerability has been found in SourceCodester Pet Grooming Management Software 1.0. This affects an unknown part of the file /admin/ajax_represent.php. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2025-09-15	6.3	CVE-2025-10431
SourceCodester--Student Grading System	A weakness has been identified in SourceCodester Student Grading System 1.0. Affected by this vulnerability is an unknown functionality of the file /view_students.php. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	2025-09-15	6.3	CVE-2025-10418
SourceCodester--Student Grading System	A security vulnerability has been detected in SourceCodester Student Grading System 1.0. Affected by this issue is some unknown functionality of the file /del_promote.php. Such manipulation of the argument sy leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	2025-09-15	6.3	CVE-2025-10419
SourceCodester--Student Grading System	A vulnerability was detected in SourceCodester Student Grading System 1.0. This affects an unknown part of the file /form137.php. Performing manipulation of the argument ID results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used.	2025-09-15	6.3	CVE-2025-10420
SourceCodester--Student Grading System	A flaw has been found in SourceCodester Student Grading System 1.0. This vulnerability affects unknown code of the file /update_account.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	2025-09-15	6.3	CVE-2025-10421

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
strangerstudios--Memberlite Shortcodes	The Memberlite Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugins's 'row' shortcode in all versions up to, and including, 1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-17	6.4	CVE-2025-10125
SUSE--neuvector	NeuVector stores user passwords and API keys using a simple, unsalted hash. This method is vulnerable to rainbow table attack (offline attack where hashes of known passwords are precomputed).	2025-09-17	5.3	CVE-2025-53884
SUSE--neuvector	When a Java command with password parameters is executed and terminated by NeuVector for Process rule violation the password will appear in the NeuVector security event log.	2025-09-17	5.3	CVE-2025-54467
Tenda--AC9	A vulnerability was determined in Tenda AC9 and AC15 15.03.05.14. This affects the function formexeCommand of the file /goform/exeCommand. This manipulation of the argument cmdinput causes os command injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	2025-09-15	6.3	CVE-2025-10442
theeventscalendar--The Events Calendar	The The Events Calendar plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 6.15.2 via the REST endpoint. This makes it possible for unauthenticated attackers to extract information about password-protected vendors or venues.	2025-09-16	5.3	CVE-2025-9808
tvcnet--The Hack Repair Guy's Plugin Archiver	The The Hack Repair Guy's Plugin Archiver plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.4. This is due to missing or incorrect nonce validation on the bulk_remove() function. This makes it possible for unauthenticated attackers to arbitrary directory deletion in /wp-content via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-17	5.4	CVE-2025-10188
tw2113--Social Media Shortcodes	The Social Media Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'twitter' shortcode in all versions up to, and including, 1.3.1 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.	2025-09-17	6.4	CVE-2025-10166
Ubit Information Technologies--STOYS	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ubit Information Technologies STOYS allows Cross-Site Scripting (XSS).This issue affects STOYS: from 2 before 20250916.	2025-09-16	4.3	CVE-2025-2404
WAGO--CC100 0751-9301	During a short time frame while the device is booting an unauthenticated remote attacker can send traffic to unauthorized networks due to the switch operating in an undefined state until a CPU-induced reset allows proper configuration.	2025-09-15	6.5	CVE-2025-41713
Webkul--QloApps	A vulnerability was detected in Webkul QloApps up to 1.7.0. This affects an unknown function of the component CSRF Token Handler. Performing manipulation of the argument token results in authorization bypass. The attack may be initiated remotely. The exploit is now public and may be used. The vendor explains: "As We are already aware about this vulnerability and our Internal team are already working on this issue. (...) We'll implement the fix for this vulnerability in our next major release."	2025-09-21	5.3	CVE-2025-10759
webraketen--Internal Links Manager	The Internal Links Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.1. This is due to missing or incorrect nonce validation on the link deletion functionality in the process_bulk_action() function. This makes it possible for unauthenticated	2025-09-20	4.3	CVE-2025-9949

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to delete SEO links via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.			
Webull--Investing & Trading App	A vulnerability was determined in Webull Investing & Trading App 11.2.5.63 on Android. This vulnerability affects unknown code of the file AndroidManifest.xml. This manipulation causes improper export of android application components. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-19	5.3	CVE-2025-10721
Wind River Systems Inc--VxWorks 7	A crafted system call argument can cause memory corruption.	2025-09-18	6.7	CVE-2025-26503
WisdomGarden--Tronclass	Tronclass developed by WisdomGarden has an Insecure Direct object Reference vulnerability, allowing remote attackers with regular privilege to modify a specific parameter to access other users' files.	2025-09-19	4.3	CVE-2025-10719
yangzongzhuan--RuoYi	A security flaw has been discovered in yangzongzhuan RuoYi up to 4.8.1. This impacts the function filterKeyword of the file /com/ruoyi/common/utils/sql/SqlUtil.java of the component Blacklist Handler. The manipulation results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be exploited.	2025-09-15	6.3	CVE-2025-10473
zephyrproject-rtos--Zephyr	The function responsible for handling BLE connection responses does not verify whether a response is expected-that is, whether the device has initiated a connection request. Instead, it relies solely on identifier matching.	2025-09-19	4.3	CVE-2025-10457
Zirve Information Technologies Inc.--Zirve Nova	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Zirve Information Technologies Inc. Zirve Nova allows Cross-Site Scripting (XSS).This issue affects Zirve Nova: from 235 through 20250131.	2025-09-17	4.7	CVE-2025-0419
ZTE--T5400	There is an unauthorized access vulnerability in ZTE T5400. Due to improper permission control of the Web module interface, an unauthorized attacker can obtain sensitive information through the interface.	2025-09-16	5.7	CVE-2025-26711
100plugins--Open User Map	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 100plugins Open User Map allows DOM-Based XSS. This issue affects Open User Map: from n/a through 1.4.14.	2025-09-22	6.5	CVE-2025-57953
8theme--XStore	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in 8theme XStore allows Code Injection. This issue affects XStore: from n/a through 9.5.3.	2025-09-26	5.3	CVE-2025-60100
Academy LMS--Academy LMS	Authorization Bypass Through User-Controlled Key vulnerability in Academy LMS Academy LMS allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Academy LMS: from n/a through 3.3.4.	2025-09-22	5.5	CVE-2025-59562
Acclectic Media--Acclectic Media Organizer	Missing Authorization vulnerability in Acclectic Media Acclectic Media Organizer allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Acclectic Media Organizer: from n/a through 1.4.	2025-09-26	6.5	CVE-2025-48326
activewebsight--SEO Backlink Monitor	Cross-Site Request Forgery (CSRF) vulnerability in activewebsight SEO Backlink Monitor allows Cross Site Request Forgery. This issue affects SEO Backlink Monitor: from n/a through 1.6.0.	2025-09-22	4.3	CVE-2025-53456
activewebsight--SEO Backlink Monitor	Server-Side Request Forgery (SSRF) vulnerability in activewebsight SEO Backlink Monitor allows Server Side Request Forgery. This issue affects SEO Backlink Monitor: from n/a through 1.6.0.	2025-09-22	4.4	CVE-2025-53457

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Ads by WPQuads--Ads by WPQuads	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ads by WPQuads Ads by WPQuads allows Stored XSS. This issue affects Ads by WPQuads: from n/a through 2.0.92.	2025-09-22	5.9	CVE-2025-53459
AdvancedCoding--wpDiscuz	Missing Authorization vulnerability in AdvancedCoding wpDiscuz allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects wpDiscuz: from n/a through 7.6.33.	2025-09-22	4.3	CVE-2025-59591
Agency Dominion Inc.--Fusion Page Builder : Extension – Gallery	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Agency Dominion Inc. Fusion Page Builder : Extension – Gallery allows Stored XSS. This issue affects Fusion Page Builder : Extension – Gallery: from n/a through 1.7.6.	2025-09-22	6.5	CVE-2025-58965
akdevs--Genealogical Tree	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in akdevs Genealogical Tree allows Stored XSS. This issue affects Genealogical Tree: from n/a through 2.2.5.	2025-09-22	6.5	CVE-2025-58023
Akll Ticaret Software Technologies Ltd. Co.--Smart Trade E-Commerce	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Akıllı Ticaret Software Technologies Ltd. Co. Smart Trade E-Commerce allows Reflected XSS.This issue affects Smart Trade E-Commerce: before 4.5.0.0.1.	2025-09-22	4.6	CVE-2025-8079
Alex Moss--Google+ Comments	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alex Moss Google+ Comments allows Stored XSS. This issue affects Google+ Comments: from n/a through 1.0.	2025-09-26	5.9	CVE-2025-60186
Alex--Content Mask	Server-Side Request Forgery (SSRF) vulnerability in Alex Content Mask allows Server Side Request Forgery. This issue affects Content Mask: from n/a through 1.8.5.2.	2025-09-22	6.4	CVE-2025-58011
Alexander Lueken--Podlove Subscribe button	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alexander Lueken Podlove Subscribe button allows Stored XSS. This issue affects Podlove Subscribe button: from n/a through 1.3.11.	2025-09-22	6.5	CVE-2025-58227
algoliasearch-helper -- v2.00 and before 3.11.2	Versions of the package algoliasearch-helper from 2.0.0-rc1 and before 3.11.2 are vulnerable to Prototype Pollution in the _merge() function in merge.js, which allows constructor.prototype to be written even though doing so throws an error. In the "extreme edge-case" that the resulting error is caught, code injected into the user-supplied search parameter may be exeucted. This is related to but distinct from the issue reported in [CVE-2021-23433](https://security.snyk.io/vuln/SNYK-JS-ALGOLIASEARCHHELPER-1570421). **NOTE:** This vulnerability is not exploitable in the default configuration of InstantSearch since searchParameters are not modifiable by users.	2025-09-27	5.9	CVE-2025-3193
AMD--AMD Instinct MI300X	Improper input validation in Satellite Management Controller (SMC) may allow an attacker with privileges to use certain special characters in manipulated Redfish® API commands, causing service processes like OpenBMC to crash and reset, potentially resulting in denial of service.	2025-09-23	5	CVE-2024-21927
AMD--AMD Instinct MI300X	Improper input validation in Satellite Management Controller (SMC) may allow an attacker with privileges to manipulate Redfish® API commands to remove files from the local root directory, potentially resulting in data corruption.	2025-09-23	5	CVE-2024-21935
Amin Y--AgreeMe Checkboxes For WooCommerce	Cross-Site Request Forgery (CSRF) vulnerability in Amin Y AgreeMe Checkboxes For WooCommerce allows Cross Site Request Forgery. This issue affects AgreeMe Checkboxes For WooCommerce: from n/a through 1.1.3.	2025-09-22	4.3	CVE-2025-57905
Amit Verma--Map Categories to Pages	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Amit Verma Map Categories to Pages allows Stored XSS. This issue affects Map Categories to Pages: from n/a through 1.3.2.	2025-09-26	5.9	CVE-2025-60146

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Anadolu Hayat Emeklilik Inc.--AHE Mobile	Authorization Bypass Through User-Controlled Key vulnerability in Anadolu Hayat Emeklilik Inc. AHE Mobile allows Privilege Abuse.This issue affects AHE Mobile: from 1.9.7 before 1.9.9.	2025-09-23	6.5	CVE-2025-9342
andy_moyle--Emergency Password Reset	Cross-Site Request Forgery (CSRF) vulnerability in andy_moyle Emergency Password Reset allows Cross Site Request Forgery. This issue affects Emergency Password Reset: from n/a through 9.0.	2025-09-22	4.3	CVE-2025-57942
AnyClip Video Platform--AnyClip Luminous Studio	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AnyClip Video Platform AnyClip Luminous Studio allows Stored XSS. This issue affects AnyClip Luminous Studio: from n/a through 1.3.3.	2025-09-22	6.5	CVE-2025-57910
AnyClip Video Platform--AnyClip Luminous Studio	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AnyClip Video Platform AnyClip Luminous Studio allows Stored XSS. This issue affects AnyClip Luminous Studio: from n/a through 1.3.3.	2025-09-22	5.9	CVE-2025-58271
AppMySite--AppMySite	Missing Authorization vulnerability in AppMySite AppMySite allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects AppMySite: from n/a through 3.14.0.	2025-09-22	5.3	CVE-2025-58679
AresIT--WP Compress	Missing Authorization vulnerability in AresIT WP Compress allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects WP Compress: from n/a through 6.50.54.	2025-09-22	5.3	CVE-2025-57899
artbees--JupiterX Core	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in artbees JupiterX Core allows Stored XSS. This issue affects JupiterX Core: from n/a through 4.10.1.	2025-09-22	6.5	CVE-2025-58264
Artifex--Ghostscript	Artifex Ghostscript through 10.05.1 has a stack-based buffer overflow in pdf_write_cmap in devices/vector/gdevpdtw.c.	2025-09-22	4.3	CVE-2025-59798
Artifex--Ghostscript	Artifex Ghostscript through 10.05.1 has a stack-based buffer overflow in pdfmark_coerce_dest in devices/vector/gdevpdfm.c via a large size value.	2025-09-22	4.3	CVE-2025-59799
Artifex--Ghostscript	In Artifex Ghostscript through 10.05.1, ocr_begin_page in devices/gdevpdfocr.c has an integer overflow that leads to a heap-based buffer overflow in ocr_line8.	2025-09-22	4.3	CVE-2025-59800
Artifex--GhostXPS	In Artifex GhostXPS before 10.06.0, there is a stack-based buffer overflow in xps_unpredict_tiff in xpstiff.c because the samplesperpixel value is not checked.	2025-09-22	4.3	CVE-2025-59801
ArtistScope--CopySafe Web Protection	Missing Authorization vulnerability in ArtistScope CopySafe Web Protection allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects CopySafe Web Protection: from n/a through 4.3.	2025-09-26	5.4	CVE-2025-60127
Ataur R--GutenKit	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ataur R GutenKit allows Stored XSS. This issue affects GutenKit: from n/a through 2.4.2.	2025-09-22	6.5	CVE-2025-57900
Aum Watcharapon--Designil PDPA Thailand	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aum Watcharapon Designil PDPA Thailand allows Stored XSS. This issue affects Designil PDPA Thailand: from n/a through 2.0.	2025-09-22	6.5	CVE-2025-58028
Aurlien LWS--LWS Affiliation	Cross-Site Request Forgery (CSRF) vulnerability in Aurélien LWS LWS Affiliation allows Cross Site Request Forgery. This issue affects LWS Affiliation: from n/a through 2.3.6.	2025-09-22	4.3	CVE-2025-57934
AutomationDirect--CLICK PLUS C0-0x CPU firmware	An authorization bypass vulnerability has been discovered in the Click Plus C2-03CPU2 device firmware version 3.60. Through the KOPR protocol utilized by the Remote PLC application, authenticated users with low-level access permissions can exploit this vulnerability to read and modify PLC variables beyond their intended authorization level.	2025-09-23	6.8	CVE-2025-55038

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
AutomationDirect--CLICK PLUS C0-0x CPU firmware	An improper resource shutdown or release vulnerability has been identified in the Click Plus C2-03CPU-2 device running firmware version 3.60. The vulnerability allows an unauthenticated attacker to perform a denial-of-service attack by exhausting all available device sessions in the Remote PLC application.	2025-09-23	5.9	CVE-2025-57882
AutomationDirect--CLICK PLUS C0-0x CPU firmware	The use of a hard-coded cryptographic key was discovered in firmware version 3.60 of the Click Plus PLC. The vulnerability relies on the fact that the software contains a hard-coded AES key used to protect the initial messages of a new KOPS session.	2025-09-23	5.3	CVE-2025-58069
AutomationDirect--CLICK PLUS C0-0x CPU firmware	An improper resource shutdown or release vulnerability has been identified in the Click Plus C2-03CPU-2 device running firmware version 3.60. The vulnerability allows an unauthenticated attacker to perform a denial-of-service attack by exhausting all available device sessions of the Click Programming Software.	2025-09-23	5.9	CVE-2025-58473
AutomationDirect--CLICK PLUS C0-0x CPU firmware	Cleartext storage of sensitive information was discovered in Click Programming Software version v3.60. The vulnerability can be exploited by a local user with access to the file system, while an administrator session is active, to steal credentials stored in clear text.	2025-09-23	4.2	CVE-2025-54855
Automattic--Developer	Cross-Site Request Forgery (CSRF) vulnerability in Automattic Developer allows Cross Site Request Forgery. This issue affects Developer: from n/a through 1.2.6.	2025-09-22	4.3	CVE-2025-57924
Automattic--WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic WordPress allows Stored XSS. WordPress core security team is aware of the issue and working on a fix. This is low severity vulnerability that requires an attacker to have Author or higher user privileges to execute the attack vector. This issue affects WordPress: from n/a through 6.8.2.	2025-09-23	5.9	CVE-2025-58674
Automattic--WordPress	Insertion of Sensitive Information Into Sent Data vulnerability in Automattic WordPress allows Retrieve Embedded Sensitive Data. The WordPress Core security team is aware of the issue and is already working on a fix. This is a low-severity vulnerability. Contributor-level privileges required in order to exploit it. This issue affects WordPress: from n/a through 6.8.2	2025-09-23	4.3	CVE-2025-58246
averta--Master Slider	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in averta Master Slider allows Stored XSS. This issue affects Master Slider: from n/a through 3.11.0.	2025-09-22	6.5	CVE-2025-58025
awsm.in--Embed Any Document	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in awsm.in Embed Any Document allows Stored XSS. This issue affects Embed Any Document: from n/a through 2.7.7.	2025-09-26	6.5	CVE-2025-60099
axboe--fio	A vulnerability was determined in axboe fio up to 3.41. This impacts the function __parse_jobs_ini of the file init.c. Executing manipulation can lead to use after free. The attack needs to be launched locally. The exploit has been publicly disclosed and may be utilized.	2025-09-23	5.3	CVE-2025-10824
Ays Pro--Photo Gallery by Ays	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Photo Gallery by Ays allows DOM-Based XSS. This issue affects Photo Gallery by Ays: from n/a through 6.3.6.	2025-09-22	6.5	CVE-2025-57947
Ays Pro--Poll Maker	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Poll Maker allows DOM-Based XSS. This issue affects Poll Maker: from n/a through 6.0.1.	2025-09-22	6.5	CVE-2025-57954
Ays Pro--Quiz Maker	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Ays Pro Quiz Maker allows Retrieve Embedded Sensitive Data. This issue affects Quiz Maker: from n/a through 6.7.0.61.	2025-09-22	5.3	CVE-2025-58015
Ays Pro--Quiz Maker	Cross-Site Request Forgery (CSRF) vulnerability in Ays Pro Quiz Maker allows Cross Site Request Forgery. This issue affects Quiz Maker: from n/a through 6.7.0.61.	2025-09-22	4.3	CVE-2025-58014

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Azizul Hasan--Text To Speech TTS Accessibility	Missing Authorization vulnerability in Azizul Hasan Text To Speech TTS Accessibility allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Text To Speech TTS Accessibility: from n/a through 1.9.20.	2025-09-22	4.3	CVE-2025-58664
Bage--Flexible FAQ	Cross-Site Request Forgery (CSRF) vulnerability in Bage Flexible FAQ allows Cross Site Request Forgery. This issue affects Flexible FAQ: from n/a through 0.2.	2025-09-22	4.3	CVE-2025-58200
Barry--Event Rocket	Missing Authorization vulnerability in Barry Event Rocket allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Event Rocket: from n/a through 3.3.	2025-09-22	4.3	CVE-2025-53452
bdthemes--Ultimate Store Kit Elementor Addons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bdthemes Ultimate Store Kit Elementor Addons allows Stored XSS. This issue affects Ultimate Store Kit Elementor Addons: from n/a through 2.8.2.	2025-09-22	6.5	CVE-2025-58017
bdthemes--ZoloBlocks	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bdthemes ZoloBlocks allows DOM-Based XSS. This issue affects ZoloBlocks: from n/a through 2.3.9.	2025-09-22	6.5	CVE-2025-58230
bdthemes--ZoloBlocks	Server-Side Request Forgery (SSRF) vulnerability in bdthemes ZoloBlocks allows Server Side Request Forgery. This issue affects ZoloBlocks: from n/a through 2.3.9.	2025-09-26	5.4	CVE-2025-60161
BehaviorTree -- BehaviorTree up to 4.7.0	A vulnerability was determined in BehaviorTree up to 4.7.0. This affects the function ParseScript of the file /src/script_parser.cpp of the component Diagnostic Message Handler. Executing manipulation of the argument error_msgs_buffer can lead to stack-based buffer overflow. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized. This patch is called cb6c7514efa628adb8180b58b4c9ccdebbe096e3. A patch should be applied to remediate this issue.	2025-09-26	5.3	CVE-2025-11012
Benjamin Intal--Stackable	Missing Authorization vulnerability in Benjamin Intal Stackable allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Stackable: from n/a through 3.18.1.	2025-09-26	4.3	CVE-2025-60094
Benjamin Intal--Stackable	Insertion of Sensitive Information Into Sent Data vulnerability in Benjamin Intal Stackable allows Retrieve Embedded Sensitive Data. This issue affects Stackable: from n/a through 3.18.1.	2025-09-26	4.3	CVE-2025-60095
Benjamin Pick--Geolocation IP Detection	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Benjamin Pick Geolocation IP Detection allows Stored XSS. This issue affects Geolocation IP Detection: from n/a through 5.5.0.	2025-09-22	6.5	CVE-2025-57993
bestweblayout--Portfolio	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bestweblayout Portfolio allows DOM-Based XSS. This issue affects Portfolio : from n/a through 2.58.	2025-09-22	5.9	CVE-2025-58245
Binsaifullah--Beaf	Server-Side Request Forgery (SSRF) vulnerability in Binsaifullah Beaf allows Server Side Request Forgery. This issue affects Beaf: from n/a through 1.6.2.	2025-09-22	4.4	CVE-2025-53461
bitlydeveloper--Bitly	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bitlydeveloper Bitly allows Stored XSS. This issue affects Bitly: from n/a through 2.7.4.	2025-09-22	6.5	CVE-2025-58231
Blocksera--Image Hover Effects Elementor Addon	Missing Authorization vulnerability in Blocksera Image Hover Effects - Elementor Addon allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Image Hover Effects - Elementor Addon: from n/a through 1.4.4.	2025-09-22	5.3	CVE-2025-57939
Brajesh Singh--WordPress Widgets Shortcode	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brajesh Singh WordPress Widgets Shortcode allows Stored XSS. This issue affects WordPress Widgets Shortcode: from n/a through 1.0.3.	2025-09-22	6.5	CVE-2025-57989

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
brandexponents--Oshine Core	Missing Authorization vulnerability in brandexponents Oshine Core allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Oshine Core: from n/a through 1.5.5.	2025-09-22	5.4	CVE-2025-58660
brijeshk89--IP Based Login	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in brijeshk89 IP Based Login allows Stored XSS. This issue affects IP Based Login: from n/a through 2.4.3.	2025-09-22	5.9	CVE-2025-58960
BuddyDev--BuddyPress Notification Widget	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BuddyDev BuddyPress Notification Widget allows Stored XSS. This issue affects BuddyPress Notification Widget: from n/a through 1.3.3.	2025-09-22	6.5	CVE-2025-58263
Bytes.co--WP Compiler	Cross-Site Request Forgery (CSRF) vulnerability in Bytes.co WP Compiler allows Cross Site Request Forgery. This issue affects WP Compiler: from n/a through 1.0.0.	2025-09-22	4.3	CVE-2025-58032
Campcodes--Farm Management System	A security flaw has been discovered in Campcodes Farm Management System 1.0. Affected by this issue is some unknown functionality. The manipulation results in file and directory information exposure. The attack may be performed from remote. The exploit has been released to the public and may be exploited.	2025-09-27	5.3	CVE-2025-11079
Campcodes--Online Beauty Parlor Management System	A vulnerability was found in Campcodes Online Beauty Parlor Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/add-customer.php. Performing manipulation of the argument mobilenum results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	2025-09-22	6.3	CVE-2025-10804
Campcodes--Online Beauty Parlor Management System	A vulnerability was determined in Campcodes Online Beauty Parlor Management System 1.0. This affects an unknown part of the file /admin/add-services.php. Executing manipulation of the argument sername can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-22	6.3	CVE-2025-10805
Campcodes--Online Beauty Parlor Management System	A vulnerability was identified in Campcodes Online Beauty Parlor Management System 1.0. This vulnerability affects unknown code of the file /admin/bwdates-reports-details.php. The manipulation of the argument fromdate/todate leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	2025-09-22	6.3	CVE-2025-10806
Campcodes--Online Beauty Parlor Management System	A security flaw has been discovered in Campcodes Online Beauty Parlor Management System 1.0. This issue affects some unknown processing of the file /admin/edit-customer-detailed.php. The manipulation of the argument editid results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be exploited.	2025-09-22	6.3	CVE-2025-10807
Campcodes--Online Beauty Parlor Management System	A vulnerability was identified in Campcodes Online Beauty Parlor Management System 1.0. Affected is an unknown function of the file /admin/view-appointment.php. The manipulation of the argument viewid leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	2025-09-23	6.3	CVE-2025-10825
Campcodes--Online Beauty Parlor Management System	A security flaw has been discovered in Campcodes Online Beauty Parlor Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/sales-reports-detail.php. The manipulation of the argument fromdate/todate results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	2025-09-23	6.3	CVE-2025-10826
Campcodes--Society Membership Information System	A vulnerability was identified in Campcodes Society Membership Information System 1.0. This issue affects some unknown processing of the file /check_student.php. Such manipulation of the argument student_id leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	2025-09-23	6.3	CVE-2025-10848

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
CardCom--CardCom Payment Gateway	Missing Authorization vulnerability in CardCom CardCom Payment Gateway allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects CardCom Payment Gateway: from n/a through 3.5.0.4.	2025-09-22	5.3	CVE-2025-57976
cartpauj--User Notes	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cartpauj User Notes allows Stored XSS. This issue affects User Notes: from n/a through 1.0.2.	2025-09-26	5.9	CVE-2025-60136
CashBill--CashBill.pl – Patnoci WooCommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CashBill CashBill.pl – Płatności WooCommerce allows Stored XSS. This issue affects CashBill.pl – Płatności WooCommerce: from n/a through 3.2.1.	2025-09-22	5.9	CVE-2025-53455
catchsquare--WP Social Widget	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in catchsquare WP Social Widget allows Stored XSS. This issue affects WP Social Widget: from n/a through 2.3.1.	2025-09-22	6.5	CVE-2025-57981
cecabank--Cecabank WooCommerce Plugin	Missing Authorization vulnerability in cecabank Cecabank WooCommerce Plugin allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Cecabank WooCommerce Plugin: from n/a through 0.3.4.	2025-09-22	5.3	CVE-2025-58685
cedcommerce--WP Advanced PDF	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cedcommerce WP Advanced PDF allows Stored XSS. This issue affects WP Advanced PDF: from n/a through 1.1.7.	2025-09-22	5.9	CVE-2025-57945
Chad Butler--WP-Members	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chad Butler WP-Members allows Stored XSS. This issue affects WP-Members: from n/a through 3.5.4.2.	2025-09-22	5.5	CVE-2025-57973
Chandrika Sista--WP Category Dropdown	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chandrika Sista WP Category Dropdown allows Stored XSS. This issue affects WP Category Dropdown: from n/a through 1.9.	2025-09-22	6.5	CVE-2025-58239
Chris Taylor--VoucherPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chris Taylor VoucherPress allows Stored XSS. This issue affects VoucherPress: from n/a through 1.5.7.	2025-09-22	5.9	CVE-2025-58223
Christiaan Pieterse--MaxiBlocks	Missing Authorization vulnerability in Christiaan Pieterse MaxiBlocks allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects MaxiBlocks: from n/a through 2.1.3.	2025-09-22	5	CVE-2025-58968
chtombleson--Mobi2Go	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in chtombleson Mobi2Go allows Stored XSS. This issue affects Mobi2Go: from n/a through 1.0.0.	2025-09-22	5.9	CVE-2025-58646
CIRCL--vulnerability-lookup	vulnerability-lookup 2.16.0 allows XSS in bundle.py, comment.py, and user.py, by a user on a vulnerability-lookup instance who can add bundles, comments, or sightings. A cross-site scripting (XSS) vulnerability was discovered in the handling of user-supplied input in the Bundles, Comments, and Sightings components. Untrusted data was not properly sanitized before being rendered in templates and tables, which could allow attackers to inject arbitrary JavaScript into the application. The issue was due to unsafe use of innerHTML and insufficient validation of dynamic URLs and model fields. This vulnerability has been fixed by escaping untrusted data, replacing innerHTML assignments with safer DOM methods, encoding URLs with encodeURIComponent, and improving input validation in the affected models.	2025-09-25	6.4	CVE-2025-60249
Cisco--Cisco Adaptive Security Appliance (ASA) Software	A vulnerability in the VPN web server of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to access restricted URL endpoints that are related to remote access VPN that should otherwise be inaccessible without authentication. This vulnerability is due to improper validation	2025-09-25	6.5	CVE-2025-20362

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of user-supplied input in HTTP(S) requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted web server on a device. A successful exploit could allow the attacker to access a restricted URL without authentication.			
Cisco--Cisco Aironet Access Point Software (IOS XE Controller)	A vulnerability in the Device Analytics action frame processing of Cisco Wireless Access Point (AP) Software could allow an unauthenticated, adjacent attacker to inject wireless 802.11 action frames with arbitrary information. This vulnerability is due to insufficient verification checks of incoming 802.11 action frames. An attacker could exploit this vulnerability by sending 802.11 Device Analytics action frames with arbitrary parameters. A successful exploit could allow the attacker to inject Device Analytics action frames with arbitrary information, which could modify the Device Analytics data of valid wireless clients that are connected to the same wireless controller.	2025-09-24	4.3	CVE-2025-20364
Cisco--Cisco Aironet Access Point Software (IOS XE Controller)	A vulnerability in the IPv6 Router Advertisement (RA) packet processing of Cisco Access Point Software could allow an unauthenticated, adjacent attacker to modify the IPv6 gateway on an affected device. This vulnerability is due to a logic error in the processing of IPv6 RA packets that are received from wireless clients. An attacker could exploit this vulnerability by associating to a wireless network and sending a series of crafted IPv6 RA packets. A successful exploit could allow the attacker to temporarily change the IPv6 gateway of an affected device. This could also lead to intermittent packet loss for any wireless clients that are associated with the affected device.	2025-09-24	4.3	CVE-2025-20365
Cisco--Cisco IOS XE Software	A vulnerability in the Web Authentication feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting attack (XSS) on an affected device. This vulnerability is due to improper sanitization of user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to execute a reflected XSS attack and steal user cookies from the affected device.	2025-09-24	6.1	CVE-2025-20240
Cisco--Cisco IOS XE Software	Multiple vulnerabilities in Cisco IOS XE Software of could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. These vulnerabilities are due path traversal and improper image integrity validation. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Because this allows the attacker to bypass a major security feature of the device, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. For more information about these vulnerabilities, see the Details ["#details"] section of this advisory. ERP	2025-09-24	6.7	CVE-2025-20313
Cisco--Cisco IOS XE Software	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to an affected device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to improper validation of software packages. An attacker could exploit this vulnerability by placing a crafted file into a specific location on an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Because this vulnerability allows an attacker to bypass a major security feature of a device, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.	2025-09-24	6.7	CVE-2025-20314
Cisco--Cisco IOS XE Software	A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with administrative privileges to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by logging in to the device CLI with valid administrative (level 15) credentials and using crafted commands at	2025-09-24	6	CVE-2025-20338

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the CLI prompt. A successful exploit could allow the attacker to execute arbitrary commands as root.			
Cisco--Cisco IOS XE Software	A vulnerability in the Day One setup process of Cisco IOS XE Software for Catalyst 9800 Series Wireless Controllers for Cloud (9800-CL) could allow an unauthenticated, remote attacker to access the public-key infrastructure (PKI) server that is running on an affected device. This vulnerability is due to incomplete cleanup upon completion of the Day One setup process. An attacker could exploit this vulnerability by sending Simple Certificate Enrollment Protocol (SCEP) requests to an affected device. A successful exploit could allow the attacker to request a certificate from the virtual wireless controller and then use the acquired certificate to join an attacker-controlled device to the virtual wireless controller.	2025-09-24	5.3	CVE-2025-20293
Cisco--Cisco IOS XE Software	A vulnerability in the access control list (ACL) programming of Cisco IOS XE Software for Cisco Catalyst 9500X and 9600X Series Switches could allow an unauthenticated, remote attacker to bypass a configured ACL on an affected device. This vulnerability is due to the flooding of traffic from an unlearned MAC address on a switch virtual interface (SVI) that has an egress ACL applied. An attacker could exploit this vulnerability by causing the VLAN to flush its MAC address table. This condition can also occur if the MAC address table is full. A successful exploit could allow the attacker to bypass an egress ACL on an affected device.	2025-09-24	5.3	CVE-2025-20316
Cisco--Cisco SD-WAN vEdge Cloud	A vulnerability in the access control list (ACL) processing of IPv4 packets of Cisco SD-WAN vEdge Software could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to the improper enforcement of the implicit deny all at the end of a configured ACL. An attacker could exploit this vulnerability by attempting to send unauthorized traffic to an interface on an affected device. A successful exploit could allow the attacker to bypass an ACL on the affected device.	2025-09-24	5.8	CVE-2025-20339
Cisco--IOS	A vulnerability in the CLI of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to a buffer overflow. An attacker with a low-privileged account could exploit this vulnerability by using crafted commands at the CLI prompt. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2025-09-24	6.5	CVE-2025-20149
CK MacLeod--Category Featured Images Extended	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CK MacLeod Category Featured Images Extended allows Stored XSS. This issue affects Category Featured Images Extended: from n/a through 1.52.	2025-09-22	5.9	CVE-2025-57920
Clariti--Clariti	Missing Authorization vulnerability in Clariti Clariti allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Clariti: from n/a through 1.2.1.	2025-09-22	5.4	CVE-2025-57991
CodeAstro--Electricity Billing System	A vulnerability was detected in CodeAstro Electricity Billing System 1.0. Affected by this issue is some unknown functionality of the file /admin/bill.php. The manipulation of the argument uid results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	2025-09-28	6.3	CVE-2025-11104
CodeAstro--Online Leave Application	A vulnerability was detected in CodeAstro Online Leave Application 1.0. Affected is an unknown function of the file /signup.php. Performing manipulation of the argument city results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used. Other parameters might be affected as well.	2025-09-28	6.3	CVE-2025-11113
CodeAstro--Online Leave Application	A flaw has been found in CodeAstro Online Leave Application 1.0. Affected by this vulnerability is an unknown functionality of the file /leaveAplicationForm.php. Executing manipulation of the argument absence[] can lead to sql injection. The	2025-09-28	6.3	CVE-2025-11114

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attack may be launched remotely. The exploit has been published and may be used.			
CodeAstro--Simple Pharmacy Management	A vulnerability was determined in CodeAstro Simple Pharmacy Management 1.0. This affects an unknown function of the file /view.php. This manipulation of the argument bar_code causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	2025-09-22	6.3	CVE-2025-10780
codefish--Pinterest Pinboard Widget	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codefish Pinterest Pinboard Widget allows Stored XSS. This issue affects Pinterest Pinboard Widget: from n/a through 1.0.7.	2025-09-22	6.5	CVE-2025-58248
Coderz Studio--Custom iFrame for Elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Coderz Studio Custom iFrame for Elementor allows DOM-Based XSS. This issue affects Custom iFrame for Elementor: from n/a through 1.0.13.	2025-09-22	6.5	CVE-2025-59553
CodeSolz--Better Find and Replace	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodeSolz Better Find and Replace allows Stored XSS. This issue affects Better Find and Replace: from n/a through 1.7.6.	2025-09-22	5.9	CVE-2025-53466
Codexpert, Inc--CF7 Submissions	Missing Authorization vulnerability in Codexpert, Inc CF7 Submissions allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects CF7 Submissions: from n/a through 0.26.	2025-09-22	4.3	CVE-2025-58016
Codexpert, Inc--CoDesigner	Missing Authorization vulnerability in Codexpert, Inc CoDesigner allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects CoDesigner: from n/a through 4.25.2.	2025-09-22	4.3	CVE-2025-57961
CodexThemes--TheGem	Missing Authorization vulnerability in CodexThemes TheGem allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects TheGem: from n/a through 5.10.5.	2025-09-26	5.4	CVE-2025-60097
CodexThemes--TheGem (Elementor)	Missing Authorization vulnerability in CodexThemes TheGem (Elementor) allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects TheGem (Elementor): from n/a through 5.10.5.	2025-09-26	5.4	CVE-2025-60096
compojoom--cForms Light speed fast Form Builder	The cForms - Light speed fast Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.0. This is due to missing or incorrect nonce validation on the cforms_api function. This makes it possible for unauthenticated attackers to modify forms and their settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-27	4.3	CVE-2025-9898
conventional-changelog--conventional-changelog	Conventional Changelog generates changelogs and release notes from a project's commit messages and metadata. Prior to version 2.0.0, @conventional-changelog/git-client has an argument injection vulnerability. This vulnerability manifests with the library's getTags() API, which allows extra parameters to be passed to the git log command. In another API by this library, getRawCommits(), there are secure practices taken to ensure that the extra parameter path is unable to inject an argument by ending the git log command with the special shell syntax --. However, the library does not follow the same practice for getTags() as it does not attempt to sanitize for user input, validate the given params, or restrict them to an allow list. Nor does it properly pass command-line flags to the git binary using the double-dash POSIX characters (--) to communicate the end of options. Thus, allowing users to exploit an argument injection vulnerability in Git due to the --output= command-line option that results with overwriting arbitrary files. This issue has been patched in version 2.0.0.	2025-09-22	5.3	CVE-2025-59433
Coordinadora Mercantil S.A.--Envos	Insertion of Sensitive Information Into Sent Data vulnerability in Coordinadora Mercantil S.A. Envíos Coordinadora Woocommerce allows Retrieve Embedded	2025-09-22	5.3	CVE-2025-57922

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Coordinadora Woocommerce	Sensitive Data. This issue affects Envíos Coordinadora Woocommerce: from n/a through 1.1.31.			
CoSchedule--CoSchedule	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in CoSchedule CoSchedule allows Retrieve Embedded Sensitive Data. This issue affects CoSchedule: from n/a through 3.3.10.	2025-09-26	5.3	CVE-2025-60119
CozyThemes--Cozy Blocks	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in CozyThemes Cozy Blocks allows Code Injection. This issue affects Cozy Blocks: from n/a through 2.1.29.	2025-09-22	5.3	CVE-2025-59573
creativemindssolutions--CM Business Directory Optimise and showcase local business	The CM Business Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'cmbd_featured_image' shortcode in all versions up to, and including, 1.5.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-26	6.4	CVE-2025-10178
CridioStudio--ListingPro	Missing Authorization vulnerability in CridioStudio ListingPro allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects ListingPro: from n/a through 2.9.8.	2025-09-26	5.4	CVE-2025-60103
CridioStudio--ListingPro Reviews	Missing Authorization vulnerability in CridioStudio ListingPro Reviews allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects ListingPro Reviews: from n/a through 1.6.	2025-09-22	5.4	CVE-2025-58667
cristianr909090--Sync Feedly	The Sync Feedly plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing or incorrect nonce validation on the crsf_cron_job_func function. This makes it possible for unauthenticated attackers to trigger content synchronization from Feedly, potentially creating multiple posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-27	4.3	CVE-2025-9894
CRM Perks--WP Gravity Forms Keap/Infusionsoft	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks WP Gravity Forms Keap/Infusionsoft allows Phishing. This issue affects WP Gravity Forms Keap/Infusionsoft: from n/a through 1.2.4.	2025-09-22	4.7	CVE-2025-58006
Csar Martn--TOCHAT.BE	Cross-Site Request Forgery (CSRF) vulnerability in César Martín TOCHAT.BE allows Cross Site Request Forgery. This issue affects TOCHAT.BE: from n/a through 1.3.4.	2025-09-22	4.3	CVE-2025-57915
cubecart--v6	CubeCart is an ecommerce software solution. Prior to version 6.5.11, a logic flaw exists in the newsletter subscription endpoint that allows an attacker to unsubscribe any user without their consent. By changing the value of the force_unsubscribe parameter in the POST request to 1, an attacker can force the removal of any valid subscriber's email address. This issue has been patched in version 6.5.11.	2025-09-22	6.5	CVE-2025-59413
cubecart--v6	CubeCart is an ecommerce software solution. Prior to version 6.5.11, the contact form's Enquiry field accepts raw HTML and that HTML is included verbatim in the email sent to the store admin. By submitting HTML in the Enquiry, the admin receives an email containing that HTML. This indicates user input is not being escaped or sanitized before being output in email (and possibly when re-rendering the form), leading to Cross-Site Scripting / HTML injection risk in email clients or admin UI. This issue has been patched in version 6.5.11.	2025-09-22	5.4	CVE-2025-59411
cubecart--v6	CubeCart is an ecommerce software solution. Prior to version 6.5.11, a vulnerability exists in the product reviews feature where user-supplied input is not properly sanitized before being displayed. An attacker can submit HTML tags inside the review description field. Once the administrator approves the review, the injected HTML is rendered on the product page for all visitors. This could be used to redirect users to malicious websites or to display unwanted content. This issue has been patched in version 6.5.11.	2025-09-22	5.4	CVE-2025-59412

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cyberlord92--OAuth Single Sign On SSO (OAuth Client)	The OAuth Single Sign On - SSO (OAuth Client) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.26.12. This is due to using a predictable state parameter (base64 encoded app name) without any randomness in the OAuth flow. This makes it possible for unauthenticated attackers to forge OAuth authorization requests and potentially hijack the OAuth flow via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-26	4.3	CVE-2025-10752
D-Link--DIR-823X	A vulnerability was determined in D-Link DIR-823X 240126/240802/250416. Affected by this vulnerability is an unknown functionality of the file /usr/sbin/goahead. This manipulation of the argument port causes command injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-22	6.3	CVE-2025-10814
D-Link--DIR-823X	A weakness has been identified in D-Link DIR-823X 250416. Affected by this issue is the function sub_412E7C of the file /goform/set_switch_settings. This manipulation of the argument port causes command injection. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	2025-09-28	6.3	CVE-2025-11092
D-Link--DIR-823X	A vulnerability was detected in D-Link DIR-823X 250416. This vulnerability affects unknown code of the file /goform/delete_offline_device. Performing manipulation of the argument delvalue results in command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	2025-09-28	6.3	CVE-2025-11095
D-Link--DIR-823X	A flaw has been found in D-Link DIR-823X 250416. This issue affects some unknown processing of the file /goform/diag_traceroute. Executing manipulation of the argument target_addr can lead to command injection. The attack can be executed remotely. The exploit has been published and may be used.	2025-09-28	6.3	CVE-2025-11096
D-Link--DIR-823X	A vulnerability has been found in D-Link DIR-823X 250416. Impacted is an unknown function of the file /goform/set_device_name. The manipulation of the argument mac leads to command injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	2025-09-28	6.3	CVE-2025-11097
D-Link--DIR-823X	A vulnerability was found in D-Link DIR-823X 250416. The affected element is an unknown function of the file /goform/set_wifi_blacklists. The manipulation of the argument macList results in command injection. The attack may be performed from remote. The exploit has been made public and could be used.	2025-09-28	6.3	CVE-2025-11098
D-Link--DIR-823X	A vulnerability was determined in D-Link DIR-823X 250416. The impacted element is the function uci_del of the file /goform/delete_prohibiting. This manipulation of the argument delvalue causes command injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-28	6.3	CVE-2025-11099
D-Link--DIR-823X	A vulnerability was identified in D-Link DIR-823X 250416. This affects the function uci_set of the file /goform/set_wifi_blacklists. Such manipulation leads to command injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	2025-09-28	6.3	CVE-2025-11100
DAEXT--Import Markdown	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DAEXT Import Markdown allows Stored XSS. This issue affects Import Markdown: from n/a through 1.14.	2025-09-22	6.5	CVE-2025-57901
DaganLev--Simple Meta Tags	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DaganLev Simple Meta Tags allows DOM-Based XSS. This issue affects Simple Meta Tags: from n/a through 1.5.	2025-09-26	6.5	CVE-2025-60142
Damian--BP Disable Activation Reloaded	Cross-Site Request Forgery (CSRF) vulnerability in Damian BP Disable Activation Reloaded allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects BP Disable Activation Reloaded: from n/a through 1.2.1.	2025-09-22	6.5	CVE-2025-57983

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
danieliser--Popup Maker Boost Sales, Conversions, Optins, Subscribers with the Ultimate WP Popups Builder	The Popup Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' parameter in all versions up to, and including, 1.20.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-26	6.4	CVE-2025-9490
Darren Cooney--Ajax Load More	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Darren Cooney Ajax Load More allows Retrieve Embedded Sensitive Data. This issue affects Ajax Load More: from n/a through 7.6.0.2.	2025-09-22	5.3	CVE-2025-59582
DataTables -- DataTables up to V1.10.13	A flaw has been found in DataTables up to 1.10.13. The affected element is an unknown function of the file /examples/resources/examples.php. This manipulation of the argument src causes path traversal. It is possible to initiate the attack remotely. The exploit has been published and may be used. Upgrading to version 1.10.15 is sufficient to fix this issue. Patch name: 3b24f99ac4ddb7f9072076b0d07f0b1a408f177a. Upgrading the affected component is advised. This vulnerability was initially reported for code-projects Faculty Management System but appears to affect DataTables as an upstream component instead. The vendor of DataTables explains: "I would suggest that the author upgrade to the latest versions of DataTables (actually, they shouldn't really be deploying that file to their own server at all - it is only relevant for the DataTables examples)."	2025-09-26	5.3	CVE-2025-11031
davaxi--Goracash	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in davaxi Goracash allows Stored XSS. This issue affects Goracash: from n/a through 1.1.	2025-09-22	5.9	CVE-2025-53458
David Lingren--Media Library Assistant	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Lingren Media Library Assistant allows Stored XSS. This issue affects Media Library Assistant: from n/a through 3.28.	2025-09-22	5.9	CVE-2025-59590
Dell--BSAFE Crypto-J	Dell Crypto-J generates an error message that includes sensitive information about its environment and associated data. A remote attacker could potentially exploit this vulnerability, leading to information exposure.	2025-09-25	5.9	CVE-2025-26333
Dell--Cloud Disaster Recovery	Dell Cloud Disaster Recovery, version(s) prior to 19.20, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary commands with root privileges.	2025-09-25	6.7	CVE-2025-43943
Dell--PowerEdge R770	Dell PowerEdge Server BIOS and Dell iDRAC9, all versions, contains an Information Disclosure vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information Disclosure.	2025-09-25	4.9	CVE-2025-26482
Dell--PowerScale OneFS	Dell PowerScale OneFS, versions 9.5.0.0 through 9.11.0.0, contains an exposure of sensitive information to an unauthorized actor vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to Information disclosure.	2025-09-25	4	CVE-2025-36601
DELUCKS--DELUCKS SEO	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DELUCKS DELUCKS SEO allows Stored XSS. This issue affects DELUCKS SEO: from n/a through 2.7.0.	2025-09-22	6.5	CVE-2025-53570
Detheme--DethemeKit For Elementor	Missing Authorization vulnerability in Detheme DethemeKit For Elementor allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects DethemeKit For Elementor: from n/a through 2.1.10.	2025-09-22	4.3	CVE-2025-57995
Di Themes--Di Themes Demo Site Importer	Cross-Site Request Forgery (CSRF) vulnerability in Di Themes Di Themes Demo Site Importer allows Cross Site Request Forgery. This issue affects Di Themes Demo Site Importer: from n/a through 1.2.	2025-09-26	4.3	CVE-2025-58914

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dialogity--Dialogity Free Live Chat	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dialogity Dialogity Free Live Chat allows Stored XSS. This issue affects Dialogity Free Live Chat: from n/a through 1.0.3.	2025-09-22	5.9	CVE-2025-57912
Dibo--Data Decision Making System	A vulnerability was found in Dibo Data Decision Making System up to 2.7.0. The affected element is the function downloadImpTemplet of the file /common/dep/common_dep.action.jsp. The manipulation of the argument filePath results in path traversal. It is possible to launch the attack remotely. The exploit has been made public and could be used.	2025-09-26	4.3	CVE-2025-11034
Diego Pereira--PowerFolio	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Diego Pereira PowerFolio allows Stored XSS. This issue affects PowerFolio: from n/a through 3.2.1.	2025-09-22	6.5	CVE-2025-57932
DivvyDrive Information Technologies Inc.--DivvyDrive Web	Observable Timing Discrepancy vulnerability in DivvyDrive Information Technologies Inc. DivvyDrive Web allows Cross-Domain Search Timing.This issue affects DivvyDrive Web: from 4.8.2.2 before 4.8.2.15.	2025-09-24	4.3	CVE-2025-9031
DJ-Extensions.com--PE Easy Slider	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DJ-Extensions.com PE Easy Slider allows Stored XSS. This issue affects PE Easy Slider: from n/a through 1.1.0.	2025-09-26	5.9	CVE-2025-60133
dnnsoftware--Dnn.Platform	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.1.0, arbitrary themes can be loaded through query parameters. If an installed theme had a vulnerability, even if it was not used on any page, this could be loaded on unsuspecting clients without knowledge of the site owner. This issue has been patched in version 10.1.0.	2025-09-22	6.5	CVE-2025-59535
dnnsoftware--Dnn.Platform	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.1.0, when embedding information in the Biography field, even if that field is not rich-text, users could inject javascript code that would run in the context of the website and to any other user that can view the profile including administrators and/or superusers. This issue has been patched in version 10.1.0.	2025-09-23	6.3	CVE-2025-59539
dnnsoftware--Dnn.Platform	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.1.0, DNN's URL/path handling and template rendering can allow specially crafted input to be reflected into a user profile that is returned to the browser. In these cases, the application does not sufficiently neutralize or encode characters that are meaningful in HTML, so an attacker can cause a victim's browser to interpret attacker-controlled content as part of the page's HTML. This issue has been patched in version 10.1.0.	2025-09-23	6.5	CVE-2025-59821
dnnsoftware--Dnn.Platform	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.1.0, the CKEditor file upload endpoint has insufficient sanitization for filenames allowing probing network endpoints. A specially crafted request can be made to upload a file with Unicode characters, which would be translated into a path that could expose resources in the internal network of the hosted site. This issue has been patched in version 10.1.0.	2025-09-23	5.3	CVE-2025-59547
douglaskarr--List Child Pages Shortcode	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in douglaskarr List Child Pages Shortcode allows Stored XSS. This issue affects List Child Pages Shortcode: from n/a through 1.3.1.	2025-09-22	6.5	CVE-2025-58021
douglaskarr--TweetThis Shortcode	The TweetThis Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'tweetthis' shortcode in all versions up to, and including, 1.8.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-	2025-09-26	6.4	CVE-2025-10136

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
dtbaker--StylePress for Elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dtbaker StylePress for Elementor allows Stored XSS. This issue affects StylePress for Elementor: from n/a through 1.2.1.	2025-09-22	6.5	CVE-2025-58254
dylanjkotze--Zephyr Project Manager	The Zephyr Project Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.3.202 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2025-09-26	4.4	CVE-2025-10490
e-plugins--Directory Pro	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins Directory Pro allows DOM-Based XSS. This issue affects Directory Pro: from n/a through 2.5.5.	2025-09-22	6.5	CVE-2025-57948
e4jvikwp--VikRestaurants Table Reservations and Take-Away	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikRestaurants Table Reservations and Take-Away allows Stored XSS. This issue affects VikRestaurants Table Reservations and Take-Away: from n/a through 1.4.	2025-09-22	5.9	CVE-2025-57962
eleopard--Behance Portfolio Manager	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eleopard Behance Portfolio Manager allows Stored XSS. This issue affects Behance Portfolio Manager: from n/a through 1.7.4.	2025-09-22	6.5	CVE-2025-57913
Elliot Sowersby / RelyWP--Coupon Affiliates	Missing Authorization vulnerability in Elliot Sowersby / RelyWP Coupon Affiliates allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Coupon Affiliates: from n/a through 6.8.0.	2025-09-22	4.3	CVE-2025-59567
emarket-design--WP Ticket Customer Service Software & Support Ticket System	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in emarket-design WP Ticket Customer Service Software & Support Ticket System allows Stored XSS. This issue affects WP Ticket Customer Service Software & Support Ticket System: from n/a through 6.0.2.	2025-09-26	6.5	CVE-2025-60157
Emarket-design--YouTube Showcase	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Emarket-design YouTube Showcase youtube-showcase allows Stored XSS.This issue affects YouTube Showcase: from n/a through 3.5.0.	2025-09-23	6.5	CVE-2025-58915
Emraan Cheema--CubeWP	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Emraan Cheema CubeWP allows Stored XSS. This issue affects CubeWP: from n/a through 1.1.26.	2025-09-22	6.5	CVE-2025-59569
epeken--Epeken All Kurir	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in epeken Epeken All Kurir allows Stored XSS. This issue affects Epeken All Kurir: from n/a through 2.0.2.	2025-09-22	5.9	CVE-2025-57906
Essekia--Helpie FAQ	Use of Hard-coded Credentials vulnerability in Essekia Helpie FAQ allows Retrieve Embedded Sensitive Data. This issue affects Helpie FAQ: from n/a through 1.39.	2025-09-22	5.3	CVE-2025-58659
etruel--WPeMatico RSS Feed Fetcher	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in etruel WPeMatico RSS Feed Fetcher allows Retrieve Embedded Sensitive Data. This issue affects WPeMatico RSS Feed Fetcher: from n/a through 2.8.10.	2025-09-22	4.3	CVE-2025-57937
Ex-Themes--WooEvents	Missing Authorization vulnerability in Ex-Themes WooEvents allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WooEvents: from n/a through 4.1.7.	2025-09-26	5.3	CVE-2025-60121

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eZee Technosys--eZee Online Hotel Booking Engine	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eZee Technosys eZee Online Hotel Booking Engine allows Stored XSS. This issue affects eZee Online Hotel Booking Engine: from n/a through 1.0.0.	2025-09-22	5.9	CVE-2025-58661
Fastly--Fastly	Cross-Site Request Forgery (CSRF) vulnerability in Fastly Fastly allows Cross Site Request Forgery. This issue affects Fastly: from n/a through 1.2.28.	2025-09-22	4.3	CVE-2025-58199
fatcatapps--GetResponse Forms	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fatcatapps GetResponse Forms allows Stored XSS. This issue affects GetResponse Forms: from n/a through 2.6.0.	2025-09-22	6.5	CVE-2025-59549
Fernando Acosta--Make Column Clickable Elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fernando Acosta Make Column Clickable Elementor allows Stored XSS. This issue affects Make Column Clickable Elementor: from n/a through 1.6.0.	2025-09-22	6.5	CVE-2025-59592
fkrauthan--wp-mpdf	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fkrauthan wp-mpdf allows Stored XSS. This issue affects wp-mpdf: from n/a through 3.9.1.	2025-09-26	6.5	CVE-2025-60040
Four-Faith--Water Conservancy Informatization Platform	A flaw has been found in Four-Faith Water Conservancy Informatization Platform 1.0. This affects an unknown function of the file /sysRole/index.do/../../generalReport/download.do;usrlogout.do.do. Executing manipulation of the argument fileName can lead to path traversal. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-26	5.3	CVE-2025-11018
Fumiki Takahashi--Gianism	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fumiki Takahashi Gianism allows Stored XSS. This issue affects Gianism: from n/a through 5.2.2.	2025-09-22	5.9	CVE-2025-58266
funnnny--HidePost	The HidePost plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.3.8. This is due to missing or incorrect nonce validation on the options.php settings page. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-27	4.3	CVE-2025-9896
fuyang_lipengjun--platform	A security vulnerability has been detected in fuyang_lipengjun platform 1.0. This issue affects the function UserCouponController of the file /usercoupon/queryAll. The manipulation leads to improper authorization. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	2025-09-22	4.3	CVE-2025-10819
fuyang_lipengjun--platform	A vulnerability was detected in fuyang_lipengjun platform 1.0. Impacted is the function TopicController of the file /topic/queryAll. The manipulation results in improper authorization. The attack can be executed remotely. The exploit is now public and may be used.	2025-09-22	4.3	CVE-2025-10820
fuyang_lipengjun--platform	A flaw has been found in fuyang_lipengjun platform 1.0. The affected element is the function TopicCategoryController of the file /topiccategory/queryAll. This manipulation causes improper authorization. The attack is possible to be carried out remotely. The exploit has been published and may be used.	2025-09-22	4.3	CVE-2025-10821
fuyang_lipengjun--platform	A vulnerability has been found in fuyang_lipengjun platform 1.0. The impacted element is the function SysSmsLogController of the file /sys/smslog/queryAll. Such manipulation leads to improper authorization. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	2025-09-22	4.3	CVE-2025-10822
Galaxy Weblinks--Post Featured Video	Cross-Site Request Forgery (CSRF) vulnerability in Galaxy Weblinks Post Featured Video allows Cross Site Request Forgery. This issue affects Post Featured Video: from n/a through 1.7.	2025-09-26	4.3	CVE-2025-60137

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
geyang--ml-logger	A vulnerability was determined in geyang ml-logger up to acf255bade5be6ad88d90735c8367b28cbe3a743. Affected is the function log_handler of the file ml_logger/server.py of the component Ping Handler. This manipulation of the argument data causes deserialization. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	2025-09-25	6.3	CVE-2025-10950
geyang--ml-logger	A security flaw has been discovered in geyang ml-logger up to acf255bade5be6ad88d90735c8367b28cbe3a743. Affected by this issue is the function stream_handler of the file ml_logger/server.py of the component File Handler. Performing manipulation of the argument key results in information disclosure. The attack can be initiated remotely. The exploit has been released to the public and may be exploited. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	2025-09-25	5.3	CVE-2025-10952
GhozyLab--Gallery Lightbox	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GhozyLab Gallery Lightbox allows Stored XSS. This issue affects Gallery Lightbox: from n/a through 1.0.0.41.	2025-09-22	6.5	CVE-2025-57966
giantspatula--SewKinect	A vulnerability has been found in giantspatula SewKinect up to 7fd963ceb3385af3706af02b8a128a13399dffb1. This affects the function pickle.loads of the file /calculate of the component Endpoint. Such manipulation of the argument body_parts/point_cloud leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases.	2025-09-25	6.3	CVE-2025-10974
GitLab--GitLab	A privilege escalation issue has been discovered in GitLab EE affecting all versions from 16.6 prior to 18.2.7, 18.3 prior to 18.3.3, and 18.4 prior to 18.4.1 that could have allowed a developer with specific group management permissions to escalate their privileges and obtain unauthorized access to additional system capabilities.	2025-09-26	6.5	CVE-2025-7691
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 14.10 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1, that could have allowed Guest users to access sensitive information stored in virtual registry configurations.	2025-09-26	6.5	CVE-2025-9958
GitLab--GitLab	An issue was discovered in GitLab CE/EE affecting all versions starting from 17.2 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1, that allows an attacker to cause uncontrolled CPU consumption, potentially leading to a Denial of Service (DoS) condition while using specific GraphQL queries.	2025-09-26	4.3	CVE-2025-11042
givanz--Vvveb	A security flaw has been discovered in givanz Vvveb up to 1.0.7.2. This affects an unknown part of the component Image Handler. Performing manipulation results in information disclosure. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited. Once again the project maintainer reacted very professional: "I accept the existence of these vulnerabilities. (...) I fixed the code to remove these vulnerabilities and will push the code to github and make a new release."	2025-09-26	5.3	CVE-2025-11028
givanz--Vvveb	A weakness has been identified in givanz Vvveb up to 1.0.7.2. This vulnerability affects unknown code. Executing manipulation can lead to cross-site request forgery. The attack can be executed remotely. The exploit has been made available to the public and could be exploited. Once again the project maintainer reacted very professional: "I accept the existence of these vulnerabilities. (...) I fixed the code to remove these vulnerabilities and will push the code to github and make a new release."	2025-09-26	4.3	CVE-2025-11029

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Glen Scott--Plugin Security Scanner	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Glen Scott Plugin Security Scanner allows Stored XSS. This issue affects Plugin Security Scanner: from n/a through 2.0.2.	2025-09-22	5.9	CVE-2025-57950
glib-networking's OpenSSL backend --N/A	glib-networking's OpenSSL backend fails to properly check the return value of a call to BIO_write(), resulting in an out of bounds read.	2025-09-25	4.8	CVE-2025-60018
GNU--Binutils	A flaw has been found in GNU Binutils 2.45. Impacted is the function _bfd_elf_parse_eh_frame of the file bfd/elf-eh-frame.c of the component Linker. Executing manipulation can lead to heap-based buffer overflow. The attack is restricted to local execution. The exploit has been published and may be used. This patch is called ea1a0737c7692737a644af0486b71e4a392cbca8. A patch should be applied to remediate this issue. The code maintainer replied with "[f]ixed for 2.46".	2025-09-27	5.3	CVE-2025-11082
GNU--Binutils	A vulnerability has been found in GNU Binutils 2.45. The affected element is the function elf_swap_shdr in the library bfd/elfcode.h of the component Linker. The manipulation leads to heap-based buffer overflow. The attack must be carried out locally. The exploit has been disclosed to the public and may be used. The identifier of the patch is 9ca499644a21ceb3f946d1c179c38a83be084490. To fix this issue, it is recommended to deploy a patch. The code maintainer replied with "[f]ixed for 2.46".	2025-09-27	5.3	CVE-2025-11083
Gravitate--Gravitate Automated Tester	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Gravitate Gravitate Automated Tester allows Stored XSS. This issue affects Gravitate Automated Tester: from n/a through 1.4.5.	2025-09-22	5.9	CVE-2025-58645
Greg Winiarski--Custom Login URL	Missing Authorization vulnerability in Greg Winiarski Custom Login URL allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Custom Login URL: from n/a through 1.0.2.	2025-09-22	5.3	CVE-2025-58969
grooni--Groovy Menu	Cross-Site Request Forgery (CSRF) vulnerability in grooni Groovy Menu allows Cross Site Request Forgery. This issue affects Groovy Menu: from n/a through 1.4.3.	2025-09-26	4.3	CVE-2025-60113
GSYT-Productions--BunnyPad-SRC	BunnyPad is a note taking software. Prior to version 11.0.27000.0915, opening files greater than or equal to 20MB causes buffer overflow to occur. This issue has been patched in version 11.0.27000.0915. Users who wish not to upgrade should refrain from opening files larger than 10MB.	2025-09-22	5.5	CVE-2025-59418
GuanxingLu--vlarl	A vulnerability was found in GuanxingLu vlarl up to 31abc0baf53ef8f5db666a1c882e1ea64def2997. This vulnerability affects the function experiments.robot.bridge.reasoning_server::run_reasoning_server of the file experiments/robot/bridge/reasoning_server.py of the component ZeroMQ. Performing manipulation of the argument Message results in deserialization. Remote exploitation of the attack is possible. The exploit has been made public and could be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided.	2025-09-25	6.3	CVE-2025-10975
Guaven Labs--SQL Chart Builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Guaven Labs SQL Chart Builder allows DOM-Based XSS. This issue affects SQL Chart Builder: from n/a through 2.3.7.2.	2025-09-22	6.5	CVE-2025-58233
guihom--Wide Banner	Missing Authorization vulnerability in guihom Wide Banner allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Wide Banner: from n/a through 1.0.4.	2025-09-26	5.3	CVE-2025-58919
gutentor--Gutentor	Missing Authorization vulnerability in gutentor Gutentor allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Gutentor: from n/a through 3.5.2.	2025-09-22	6.5	CVE-2025-58680
Hamid Reza Yazdani--E-namad	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hamid Reza Yazdani E-namad & Shamed Logo	2025-09-22	5.9	CVE-2025-57998

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
& Shamed Logo Manager	Manager allows Stored XSS. This issue affects E-namad & Shamed Logo Manager: from n/a through 2.2.			
HaruTheme--Frames	Missing Authorization vulnerability in HaruTheme Frames allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Frames: from n/a through 1.5.7.	2025-09-26	4.3	CVE-2025-60165
hashthemes--Smart Blocks	Missing Authorization vulnerability in hashthemes Smart Blocks allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Smart Blocks: from n/a through 2.4.	2025-09-22	4.3	CVE-2025-59561
Heureka Group--Heureka	Missing Authorization vulnerability in Heureka Group Heureka allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Heureka: from n/a through 1.1.0.	2025-09-22	5.3	CVE-2025-57907
HivePress--HivePress Claim Listings	Missing Authorization vulnerability in HivePress HivePress Claim Listings allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects HivePress Claim Listings: from n/a through 1.1.3.	2025-09-26	4.3	CVE-2025-60122
HivePress--HivePress Claim Listings	Missing Authorization vulnerability in HivePress HivePress Claim Listings allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects HivePress Claim Listings: from n/a through 1.1.3.	2025-09-26	4.3	CVE-2025-60123
honzat--Page Manager for Elementor	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in honzat Page Manager for Elementor allows Retrieve Embedded Sensitive Data. This issue affects Page Manager for Elementor: from n/a through 2.0.5.	2025-09-26	4.3	CVE-2025-60167
Horato Internet Technologies Ind. and Trade Inc.--Virtual Library Platform	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Horato Internet Technologies Ind. And Trade Inc. Virtual Library Platform allows Reflected XSS.This issue affects Virtual Library Platform: before v202.	2025-09-22	5.4	CVE-2025-9035
horilla-opensource--horilla	Horilla is a free and open source Human Resource Management System (HRMS). A stored cross-site scripting (XSS) vulnerability in Horilla HRM 1.3.0 allows authenticated admin or privileged users to inject malicious JavaScript payloads into multiple fields in the Project and Task modules. These payloads persist in the database and are executed when viewed by an admin or other privileged users through the web interface. Although the issue is not exploitable by unauthenticated users, it still poses a high risk of session hijacking and unauthorized action within high-privilege accounts. At time of publication there is no known patch.	2025-09-24	4.8	CVE-2025-48867
HT Plugins--HT Feed	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HT Plugins HT Feed allows Stored XSS. This issue affects HT Feed: from n/a through 1.3.0.	2025-09-26	6.5	CVE-2025-60147
HT Plugins--HT Mega Absolute Addons for WPBakery Page Builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HT Plugins HT Mega - Absolute Addons for WPBakery Page Builder allows DOM-Based XSS. This issue affects HT Mega - Absolute Addons for WPBakery Page Builder: from n/a through 1.0.9.	2025-09-22	6.5	CVE-2025-53463
husani--WP Subtitle	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in husani WP Subtitle allows Stored XSS. This issue affects WP Subtitle: from n/a through 3.4.1.	2025-09-22	6.5	CVE-2025-57986
iberezansky--3D FlipBook PDF Flipbook Viewer,	Insertion of Sensitive Information Into Sent Data vulnerability in iberezansky 3D FlipBook - PDF Flipbook Viewer, Flipbook Image Gallery allows Retrieve Embedded Sensitive Data. This issue affects 3D FlipBook - PDF Flipbook Viewer, Flipbook Image Gallery: from n/a through 1.16.16.	2025-09-22	5.3	CVE-2025-58226

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Flipbook Image Gallery				
IBM--Sterling Connect:Express for Microsoft Windows	IBM Sterling Connect:Express for Microsoft Windows 3.1.0.0 through 3.1.0.22 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials.	2025-09-22	5.9	CVE-2025-36064
IBM--Storage TS4500 Library	IBM Storage TS4500 Library 1.11.0.0 and 2.11.0.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	2025-09-27	6.5	CVE-2024-43192
IBM--Storage TS4500 Library	IBM Storage TS4500 Library 1.11.0.0 and 2.11.0.0 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-09-27	6.1	CVE-2025-36239
IBM--Watson Studio on Cloud Pak for Data	IBM Watson Studio 4.0 through 5.2.0 on Cloud Pak for Data is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-09-25	4.4	CVE-2025-33116
IBM--webMethods Integration	IBM webMethods Integration 10.15 and 11.1 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	2025-09-22	5.4	CVE-2025-36037
Ickata--Image Editor by Pixo	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ickata Image Editor by Pixo allows DOM-Based XSS. This issue affects Image Editor by Pixo: from n/a through 2.3.8.	2025-09-22	6.5	CVE-2025-58232
icopydoc--Maps for WP	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in icopydoc Maps for WP allows Stored XSS. This issue affects Maps for WP: from n/a through 1.2.5.	2025-09-22	5.9	CVE-2025-57952
Ideal Postcodes--UK Address Postcode Validation	Insertion of Sensitive Information Into Sent Data vulnerability in Ideal Postcodes UK Address Postcode Validation allows Retrieve Embedded Sensitive Data. This issue affects UK Address Postcode Validation: from n/a through 3.9.2.	2025-09-22	5.3	CVE-2025-57923
impleCode--Product Catalog Simple	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in impleCode Product Catalog Simple allows Stored XSS. This issue affects Product Catalog Simple: from n/a through 1.8.2.	2025-09-22	6.5	CVE-2025-58992
inc2734--Snow Monkey	The Snow Monkey theme for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 29.1.5 via the request() function. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	2025-09-26	5.4	CVE-2025-10137
instapagedev--Instapage Plugin	Cross-Site Request Forgery (CSRF) vulnerability in instapagedev Instapage Plugin allows Cross Site Request Forgery. This issue affects Instapage Plugin: from n/a through 3.5.12.	2025-09-26	4.3	CVE-2025-60115
InterServer--Mail Baby SMTP	Cross-Site Request Forgery (CSRF) vulnerability in InterServer Mail Baby SMTP allows Cross Site Request Forgery. This issue affects Mail Baby SMTP: from n/a through 2.8.	2025-09-22	4.3	CVE-2025-57992
Ironikus--WP Mailto Links	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ironikus WP Mailto Links allows Stored XSS. This issue affects WP Mailto Links: from n/a through 3.1.4.	2025-09-22	5.9	CVE-2025-53464

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
itsourcecode--Hostel Management System	A security flaw has been discovered in itsourcecode Hostel Management System 1.0. Impacted is an unknown function of the file /justines/index.php of the component POST Request Handler. Performing manipulation of the argument from results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	2025-09-28	4.3	CVE-2025-11119
itsourcecode--Online Clinic Management System	A weakness has been identified in itsourcecode Online Clinic Management System 1.0. Affected is an unknown function of the file /details.php?action=post. Executing manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	2025-09-26	6.3	CVE-2025-11038
itsourcecode--Open Source Job Portal	A vulnerability has been found in itsourcecode Open Source Job Portal 1.0. Affected by this issue is some unknown functionality of the file /admin/user/index.php?view=edit. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	2025-09-26	6.3	CVE-2025-11041
itsourcecode--Open Source Job Portal	A security vulnerability has been detected in itsourcecode Open Source Job Portal 1.0. This impacts an unknown function of the file /jobportal/admin/category/index.php?view=edit. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	2025-09-27	6.3	CVE-2025-11054
itsourcecode--Open Source Job Portal	A vulnerability was identified in itsourcecode Open Source Job Portal 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/user/controller.php?action=photos. The manipulation of the argument photo leads to unrestricted upload. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	2025-09-27	6.3	CVE-2025-11078
itsourcecode--Open Source Job Portal	A weakness has been identified in itsourcecode Open Source Job Portal 1.0. Impacted is an unknown function of the file /admin/vacancy/index.php?view=edit. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	2025-09-27	6.3	CVE-2025-11088
itsourcecode--Open Source Job Portal	A vulnerability was identified in itsourcecode Open Source Job Portal 1.0. Affected is an unknown function of the file /admin/employee/index.php?view=edit. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	2025-09-28	6.3	CVE-2025-11090
javothemes--Javo Core	Missing Authorization vulnerability in javothemes Javo Core allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Javo Core: from n/a through 3.0.0.266.	2025-09-22	5.3	CVE-2025-58003
Jeff Farthing--Theme My Login	Missing Authorization vulnerability in Jeff Farthing Theme My Login allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Theme My Login: from n/a through 7.1.12.	2025-09-26	6.5	CVE-2025-60098
Jennifer Moss--MWW Disclaimer Buttons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jennifer Moss MWW Disclaimer Buttons allows Stored XSS. This issue affects MWW Disclaimer Buttons: from n/a through 3.41.	2025-09-26	5.9	CVE-2025-60154
Jeremy Saxey--Hide WP Toolbar	Missing Authorization vulnerability in Jeremy Saxey Hide WP Toolbar allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Hide WP Toolbar: from n/a through 2.7.	2025-09-22	4.3	CVE-2025-57969
Jeroen Schmit--Theater for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeroen Schmit Theater for WordPress allows Stored XSS. This issue affects Theater for WordPress: from n/a through 0.18.8.	2025-09-22	6.5	CVE-2025-58020

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jetmonsters--Getwid	Insertion of Sensitive Information Into Sent Data vulnerability in jetmonsters Getwid allows Retrieve Embedded Sensitive Data. This issue affects Getwid: from n/a through 2.1.2.	2025-09-22	4.3	CVE-2025-58252
jhoppe--Markdown Shortcode	The Markdown Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'markdown' shortcode in all versions up to, and including, 0.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-26	6.4	CVE-2025-10180
Jinher--OA	A vulnerability was determined in Jinher OA 2.0. The impacted element is an unknown function of the file /c6/Jhsoft.Web.module/ToolBar/ManageWord.aspx/?text=GetUrl&style=1. This manipulation causes xml external entity reference. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-26	6.3	CVE-2025-11035
Jonathan Brinley--DOAJ Export	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jonathan Brinley DOAJ Export allows Stored XSS. This issue affects DOAJ Export: from n/a through 1.0.4.	2025-09-22	5.9	CVE-2025-58256
JonathanMH--Append Link on Copy	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JonathanMH Append Link on Copy allows Stored XSS. This issue affects Append Link on Copy: from n/a through 0.2.	2025-09-22	5.9	CVE-2025-57941
JoomSky--JS Job Manager	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JoomSky JS Job Manager allows Stored XSS. This issue affects JS Job Manager: from n/a through 2.0.2.	2025-09-22	6.5	CVE-2025-58234
Joovii--Sendle Shipping	Cross-Site Request Forgery (CSRF) vulnerability in Joovii Sendle Shipping allows Cross Site Request Forgery. This issue affects Sendle Shipping: from n/a through 6.02.	2025-09-26	4.3	CVE-2025-60139
Jordy Meow--Gallery Custom Links	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jordy Meow Gallery Custom Links allows Stored XSS. This issue affects Gallery Custom Links: from n/a through 2.2.5.	2025-09-26	5.9	CVE-2025-60104
Jose Vega--WP Frontend Admin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jose Vega WP Frontend Admin allows Stored XSS. This issue affects WP Frontend Admin: from n/a through 1.22.6.	2025-09-22	6.5	CVE-2025-57898
Jrgen Mller--Easy Quotes	Missing Authorization vulnerability in Jürgen Müller Easy Quotes allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Easy Quotes: from n/a through 1.2.4.	2025-09-22	5.3	CVE-2025-58681
JS Morisset--JSM file_get_contents() Shortcode	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JS Morisset JSM file_get_contents() Shortcode allows Stored XSS. This issue affects JSM file_get_contents() Shortcode: from n/a through 2.7.1.	2025-09-22	6.5	CVE-2025-58653
JSC R7--R7-Office Document Server	A flaw has been found in JSC R7 R7-Office Document Server up to 20250820. Impacted is an unknown function of the file /downloadas/. Executing manipulation of the argument cmd can lead to path traversal. The attack can be launched remotely. Upgrading to version 2025.3.1.923 is recommended to address this issue. The affected component should be upgraded. R7-Office is a fork of OpenOffice and at the moment it remains unclear if OpenOffice is affected as well. The OpenOffice team was not able to reproduce the issue in their codebase. The vendor replied: "We confirm that this vulnerability has been verified and patched in release 2025.3.1.923. During our security testing, it was not possible to exploit the issue - the server consistently returns proper error responses to the provided scenarios."	2025-09-22	6.3	CVE-2025-10777

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kalcaddle--kodbox	A security vulnerability has been detected in kalcaddle kodbox up to 1.61.09. The affected element is the function fileOut of the file app/controller/explorer/index.class.php. Such manipulation of the argument path leads to path traversal. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-26	4.3	CVE-2025-11016
kanwei_doublethedonation--Double the Donation	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kanwei_doublethedonation Double the Donation allows Stored XSS. This issue affects Double the Donation: from n/a through 2.0.0.	2025-09-22	5.9	CVE-2025-57929
kanwei_doublethedonation--Double the Donation	Cross-Site Request Forgery (CSRF) vulnerability in kanwei_doublethedonation Double the Donation allows Cross Site Request Forgery. This issue affects Double the Donation: from n/a through 2.0.0.	2025-09-22	4.3	CVE-2025-57930
kelderic--Professional Contact Form	The Professional Contact Form plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing or incorrect nonce validation on the watch_for_contact_form_submit function. This makes it possible for unauthenticated attackers to trigger test email sending via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-27	4.3	CVE-2025-9944
ken107--SiteNarrator Text-to-Speech Widget	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ken107 SiteNarrator Text-to-Speech Widget allows Stored XSS. This issue affects SiteNarrator Text-to-Speech Widget: from n/a through 1.9.	2025-09-22	5.9	CVE-2025-57951
Keyfactor--RG-EW5100BE	A vulnerability was detected in Keyfactor RG-EW5100BE EW_3.0B11P280_EW5100BE-PRO_12183019. The affected element is an unknown function of the file /cgi-bin/luci/api/cmd of the component HTTP POST Request Handler. The manipulation of the argument url results in command injection. The attack can be launched remotely. The exploit is now public and may be used.	2025-09-27	4.7	CVE-2025-11073
Kommo--Website Chat Button: Kommo integration	Missing Authorization vulnerability in Kommo Website Chat Button: Kommo integration allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Website Chat Button: Kommo integration: from n/a through 1.3.1.	2025-09-22	4.3	CVE-2025-58666
kontur.us--kontur Admin Style	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kontur.us kontur Admin Style allows Stored XSS. This issue affects kontur Admin Style: from n/a through 1.0.4.	2025-09-26	5.9	CVE-2025-60185
kraftplugins--Mega Elements Addons for Elementor	The Mega Elements - Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown Timer widget in all versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-26	6.4	CVE-2025-8200
kstover--Ninja Forms The Contact Form Builder That Grows With You	The Ninja Forms - The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.12.0. This is due to missing or incorrect nonce validation when exporting CSV files. This makes it possible for unauthenticated attackers to delete those files granted they can trick an administrator into performing an action such as clicking on a link.	2025-09-27	4.3	CVE-2025-10498
kstover--Ninja Forms The Contact Form Builder That Grows With You	The Ninja Forms - The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.12.0. This is due to missing or incorrect nonce validation on the maybe_opt_in() function. This makes it possible for unauthenticated attackers to opt an affected site into usage statistics collection via a forged request granted	2025-09-27	4.3	CVE-2025-10499

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	they can trick a site administrator into performing an action such as clicking on a link.			
langleyfcu--Online Banking System	A vulnerability was found in langleyfcu Online Banking System up to 57437e6400ce0ae240e692c24e6346b8d0c17d7a. Affected by this vulnerability is an unknown functionality of the file /connection_error.php of the component Error Message Handler. Performing manipulation of the argument Error results in cross site scripting. Remote exploitation of the attack is possible. The exploit has been made public and could be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided.	2025-09-28	4.3	CVE-2025-11125
LazyAGI--LazyLLM	A security vulnerability has been detected in LazyAGI LazyLLM up to 0.6.1. Affected by this issue is the function lazyllm_call of the file lazyllm/components/deploy/relay/server.py. Such manipulation leads to deserialization. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	2025-09-25	6.3	CVE-2025-10965
leeshadle--Draft	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in leeshadle Draft allows Stored XSS. This issue affects Draft: from n/a through 3.0.9.	2025-09-22	5.9	CVE-2025-58033
LIJE--Show Pages List	Cross-Site Request Forgery (CSRF) vulnerability in LIJE Show Pages List allows Cross Site Request Forgery. This issue affects Show Pages List: from n/a through 1.2.0.	2025-09-22	4.3	CVE-2025-58219
LizardByte--Sunshine	Sunshine is a self-hosted game stream host for Moonlight. Prior to version 2025.923.33222, the Windows service SunshineService is installed with an unquoted executable path. If Sunshine is installed in a directory whose name includes a space, the Service Control Manager (SCM) interprets the path incrementally and may execute a malicious binary placed earlier in the search string. This issue has been patched in version 2025.923.33222.	2025-09-23	6.7	CVE-2025-54081
lobehub--lobe-chat	Lobe Chat is an open-source artificial intelligence chat framework. Prior to version 1.130.1, the project's OIDC redirect handling logic constructs the host and protocol of the final redirect URL based on the X-Forwarded-Host or Host headers and the X-Forwarded-Proto value. In deployments where a reverse proxy forwards client-supplied X-Forwarded-* headers to the origin as-is, or where the origin trusts them without validation, an attacker can inject an arbitrary host and trigger an open redirect that sends users to a malicious domain. This issue has been patched in version 1.130.1.	2025-09-25	4.3	CVE-2025-59426
Loc Bui--payOS	Cross-Site Request Forgery (CSRF) vulnerability in Loc Bui payOS allows Cross Site Request Forgery. This issue affects payOS: from n/a through 1.0.61.	2025-09-22	5.4	CVE-2025-57946
loopus--WP Virtual Assistant	Missing Authorization vulnerability in loopus WP Virtual Assistant allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Virtual Assistant: from n/a through 3.0.	2025-09-26	5.3	CVE-2025-60155
Luke Mlsna--Last Updated Shortcode	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Luke Mlsna Last Updated Shortcode allows Stored XSS. This issue affects Last Updated Shortcode: from n/a through 1.0.1.	2025-09-22	6.5	CVE-2025-58683
Maidul--Team Manager	Missing Authorization vulnerability in Maidul Team Manager allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Team Manager: from n/a through 2.3.14.	2025-09-22	5.3	CVE-2025-58222
MantraBrain--Ultimate Watermark	Missing Authorization vulnerability in MantraBrain Ultimate Watermark allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Ultimate Watermark: from n/a through 1.1.	2025-09-22	4.3	CVE-2025-57985
mapster--Mapster WP Maps	The Mapster WP Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple fields in versions up to, and including, 1.20.0 due to insufficient input sanitization and output escaping. This makes it possible for	2025-09-26	6.4	CVE-2025-9044

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated attackers with contributor-level permissions and above to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
marceljm--Featured Image from URL (FIFU)	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the fifu_api_debug_posts() function in all versions up to, and including, 5.2.7. This makes it possible for unauthenticated attackers to read private/password protected posts.	2025-09-26	5.3	CVE-2025-9984
marceljm--Featured Image from URL (FIFU)	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 5.2.7 through publicly exposed log files. This makes it possible for unauthenticated attackers to view potentially sensitive information contained in the exposed log files.	2025-09-26	5.3	CVE-2025-9985
marceljm--Featured Image from URL (FIFU)	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to SQL Injection via the get_all_urls() function in all versions up to, and including, 5.2.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-26	4.9	CVE-2025-10036
marceljm--Featured Image from URL (FIFU)	The Featured Image from URL (FIFU) plugin for WordPress is vulnerable to SQL Injection via the get_posts_with_internal_featured_image() function in all versions up to, and including, 5.2.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2025-09-26	4.9	CVE-2025-10037
Marketing Fire, LLC--Widget Options - Extended	The Widget Options - Extended plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'do_sidebar' shortcode in all versions up to, and including, 5.2.1 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.	2025-09-23	6.4	CVE-2025-8902
Matat Technologies--Deliver via Shipos for WooCommerce	Cross-Site Request Forgery (CSRF) vulnerability in Matat Technologies Deliver via Shipos for WooCommerce allows Cross Site Request Forgery. This issue affects Deliver via Shipos for WooCommerce: from n/a through 3.0.2.	2025-09-22	4.3	CVE-2025-57914
matthewordie--Buckets	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in matthewordie Buckets allows Stored XSS. This issue affects Buckets: from n/a through 0.3.9.	2025-09-22	6.5	CVE-2025-57996
Mattia Roccoberton--Category Featured Images	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mattia Roccoberton Category Featured Images allows Stored XSS. This issue affects Category Featured Images: from n/a through 1.1.8.	2025-09-22	5.9	CVE-2025-58655
maxpagels--ShortCode	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in maxpagels ShortCode allows Stored XSS. This issue affects ShortCode: from n/a through 0.8.1.	2025-09-22	6.5	CVE-2025-58022
Mayo Moriyama--Force Update Translations	Cross-Site Request Forgery (CSRF) vulnerability in Mayo Moriyama Force Update Translations allows Cross Site Request Forgery. This issue affects Force Update Translations: from n/a through 0.5.	2025-09-22	4.3	CVE-2025-58236
Md Taufiqur Rahman--RIS	Cross-Site Request Forgery (CSRF) vulnerability in Md Taufiqur Rahman RIS Version Switcher – Downgrade or Upgrade WP Versions Easily allows Cross Site	2025-09-22	6.5	CVE-2025-57902

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Version Switcher – Downgrade or Upgrade WP Versions Easily	Request Forgery. This issue affects RIS Version Switcher – Downgrade or Upgrade WP Versions Easily: from n/a through 1.0.			
Meitar--Subresource Integrity (SRI) Manager	Missing Authorization vulnerability in Meitar Subresource Integrity (SRI) Manager allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Subresource Integrity (SRI) Manager: from n/a through 0.4.0.	2025-09-22	4.3	CVE-2025-57936
memberful--Memberful	Missing Authorization vulnerability in memberful Memberful allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Memberful: from n/a through 1.75.0.	2025-09-22	5.3	CVE-2025-58000
metaphorcreations--Ditty	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in metaphorcreations Ditty allows Stored XSS. This issue affects Ditty: from n/a through 3.1.58.	2025-09-26	6.5	CVE-2025-60105
Michael Ott--Notely	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michael Ott Notely allows Stored XSS. This issue affects Notely: from n/a through 1.8.0.	2025-09-26	5.9	CVE-2025-60149
Michel - xiligroup dev--xili-language	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michel - xiligroup dev xili-language allows DOM-Based XSS. This issue affects xili-language: from n/a through 2.21.3.	2025-09-22	6.5	CVE-2025-58654
Michel - xiligroup dev--xili-tidy-tags	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michel - xiligroup dev xili-tidy-tags allows Stored XSS. This issue affects xili-tidy-tags: from n/a through 1.12.06.	2025-09-22	6.5	CVE-2025-58240
mihdan--Mihdan: No External Links	Cross-Site Request Forgery (CSRF) vulnerability in mihdan Mihdan: No External Links allows Cross Site Request Forgery. This issue affects Mihdan: No External Links: from n/a through 5.1.4.	2025-09-22	5.4	CVE-2025-53451
Milan Petrovic--GD bbPress Tools	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Milan Petrovic GD bbPress Tools allows DOM-Based XSS. This issue affects GD bbPress Tools: from n/a through 3.5.3.	2025-09-22	6.5	CVE-2025-58002
milankyada--VM Menu Reorder plugin	The VM Menu Reorder plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.0. This is due to missing or incorrect nonce validation on the vm_set_to_default function. This makes it possible for unauthenticated attackers to reset all menu reordering settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-27	4.3	CVE-2025-9893
Modern Minds--Magento 2 WordPress Integration	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Modern Minds Magento 2 WordPress Integration allows Stored XSS. This issue affects Magento 2 WordPress Integration: from n/a through 1.4.1.	2025-09-22	5.9	CVE-2025-58669
Mortgage Calculator--BMI Adult & Kid Calculator	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mortgage Calculator BMI Adult & Kid Calculator allows Stored XSS. This issue affects BMI Adult & Kid Calculator: from n/a through 1.2.2.	2025-09-22	5.9	CVE-2025-53469
N-Media--Frontend File Manager	Missing Authorization vulnerability in N-Media Frontend File Manager allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Frontend File Manager: from n/a through 23.2.	2025-09-22	5.3	CVE-2025-57921
n/a--github.com/nyaruka/phonenumbers	Versions of the package github.com/nyaruka/phonenumbers before 1.2.2 are vulnerable to Improper Validation of Syntactic Correctness of Input in the	2025-09-27	5.3	CVE-2025-10954

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	phonenumbers.Parse() function. An attacker can cause a panic by providing crafted input causing a "runtime error: slice bounds out of range".			
n/a--JeecgBoot	A security flaw has been discovered in JeecgBoot up to 3.8.2. The affected element is an unknown function of the file /sys/user/exportXls of the component Filter Handler. The manipulation results in improper authorization. The attack may be performed from remote. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	4.3	CVE-2025-10978
n/a--JeecgBoot	A weakness has been identified in JeecgBoot up to 3.8.2. The impacted element is an unknown function of the file /sys/role/exportXls. This manipulation causes improper authorization. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	4.3	CVE-2025-10979
n/a--JeecgBoot	A security vulnerability has been detected in JeecgBoot up to 3.8.2. This affects an unknown function of the file /sys/position/exportXls. Such manipulation leads to improper authorization. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	4.3	CVE-2025-10980
n/a--JeecgBoot	A vulnerability was detected in JeecgBoot up to 3.8.2. This impacts an unknown function of the file /sys/tenant/exportXls. Performing manipulation results in improper authorization. The attack can be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-26	4.3	CVE-2025-10981
n/a--MuYuCMS	A vulnerability was found in MuYuCMS up to 2.7. Impacted is an unknown function of the file /index/index.html of the component Add Fiend Link Handler. Performing manipulation of the argument Link URL results in server-side request forgery. The attack may be initiated remotely. The exploit has been made public and could be used.	2025-09-22	6.3	CVE-2025-10787
n/a--MuYuCMS	A security flaw has been discovered in MuYuCMS up to 2.7. Affected by this issue is some unknown functionality of the file /admin.php of the component Template Management. The manipulation results in code injection. It is possible to launch the attack remotely.	2025-09-26	4.7	CVE-2025-10993
n/a--SeaCMS	A security vulnerability has been detected in SeaCMS 13.3.20250820. Impacted is an unknown function of the file /admin_cron.php of the component Cron Task Management Module. The manipulation of the argument resourcefrom/collectID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	2025-09-27	4.7	CVE-2025-11071
NerdPress--Social Pug	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in NerdPress Social Pug allows Retrieve Embedded Sensitive Data. This issue affects Social Pug: from n/a through 1.35.1.	2025-09-22	4.3	CVE-2025-58007
netgsm--Netgsm	Missing Authorization vulnerability in netgsm Netgsm allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Netgsm: from n/a through 2.9.58.	2025-09-26	4.3	CVE-2025-60143
Nextendweb--Nextend Facebook Connect	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nextendweb Nextend Facebook Connect allows Stored XSS. This issue affects Nextend Facebook Connect : from n/a through 3.1.19.	2025-09-22	6.5	CVE-2025-58031
Niaj Morshed--LC Wizard	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Niaj Morshed LC Wizard allows Stored XSS. This issue affects LC Wizard: from n/a through 1.3.0.	2025-09-22	6.5	CVE-2025-58237
Nick Verwymeren--Quantities and	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nick Verwymeren Quantities and Units for	2025-09-26	6.5	CVE-2025-58917

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Units for WooCommerce	WooCommerce allows Stored XSS. This issue affects Quantities and Units for WooCommerce: from n/a through 1.0.13.			
Nicu Micle--Simple JWT Login	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nicu Micle Simple JWT Login allows Stored XSS. This issue affects Simple JWT Login: from n/a through 3.6.4.	2025-09-22	6.5	CVE-2025-58648
nK--Lazy Blocks	Missing Authorization vulnerability in nK Lazy Blocks allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Lazy Blocks: from n/a through 4.1.0.	2025-09-22	4.3	CVE-2025-58258
NNCP--NNCP	nncp before 8.12.0 allows path traversal (for reading or writing) during freqing and file saving via a crafted path in packet data.	2025-09-24	6.4	CVE-2025-60020
Noumaan Yaqoob--Compact Archives	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noumaan Yaqoob Compact Archives allows Stored XSS. This issue affects Compact Archives: from n/a through 4.1.0.	2025-09-22	6.5	CVE-2025-58001
Nurul Amin--WP System Information	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Nurul Amin WP System Information allows Retrieve Embedded Sensitive Data. This issue affects WP System Information: from n/a through 1.5.	2025-09-22	4.3	CVE-2025-57916
NVIDIA--NVIDIA CUDA Toolkit	NVIDIA nvJPEG library contains a vulnerability where an attacker can cause an out-of-bounds read by means of a specially crafted JPEG file. A successful exploit of this vulnerability might lead to information disclosure or denial of service.	2025-09-24	5.7	CVE-2025-23272
NVIDIA--NVIDIA CUDA Toolkit	NVIDIA nvJPEG contains a vulnerability in jpeg encoding where a user may cause an out-of-bounds read by providing a maliciously crafted input image with dimensions that cause integer overflows in array index calculations. A successful exploit of this vulnerability may lead to denial of service.	2025-09-24	4.5	CVE-2025-23274
NVIDIA--NVIDIA CUDA Toolkit	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in nvJPEG where a local authenticated user may cause a GPU out-of-bounds write by providing certain image dimensions. A successful exploit of this vulnerability may lead to denial of service and information disclosure.	2025-09-24	4.2	CVE-2025-23275
oggix--Ongkoskirim.id	Missing Authorization vulnerability in oggix Ongkoskirim.id allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Ongkoskirim.id: from n/a through 1.0.6.	2025-09-22	5.4	CVE-2025-57949
OGRECave--Ogre	A security flaw has been discovered in OGRECave Ogre up to 14.4.1. This issue affects the function STBIImageCodec::encode of the file /ogre/PlugIns/STBICodec/src/OgreSTBICodec.cpp of the component Image Handler. The manipulation results in heap-based buffer overflow. The attack is only possible with local access. The exploit has been released to the public and may be exploited.	2025-09-26	5.3	CVE-2025-11014
OGRECave--Ogre	A weakness has been identified in OGRECave Ogre up to 14.4.1. Impacted is the function STBIImageCodec::encode of the file /ogre/PlugIns/STBICodec/src/OgreSTBICodec.cpp. This manipulation causes mismatched memory management routines. The attack is restricted to local execution. The exploit has been made available to the public and could be exploited.	2025-09-26	5.3	CVE-2025-11015
ONTRAPORT--PilotPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ONTRAPORT PilotPress allows Stored XSS. This issue affects PilotPress: from n/a through 2.0.35.	2025-09-22	6.5	CVE-2025-58238
ONTRAPORT--PilotPress	Missing Authorization vulnerability in ONTRAPORT PilotPress allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects PilotPress: from n/a through 2.0.35.	2025-09-22	4.3	CVE-2025-58221

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Open Babel -- Up to v3.1.1	A weakness has been identified in Open Babel up to 3.1.1. This affects the function GAMESSOutputFormat::ReadMolecule of the file gamessformat.cpp. This manipulation causes use after free. It is possible to launch the attack on the local host. The exploit has been made available to the public and could be exploited.	2025-09-26	5.3	CVE-2025-10994
Open Babel -- Up to v3.1.1	A security vulnerability has been detected in Open Babel up to 3.1.1. This vulnerability affects the function zlib_stream::basic_unzip_streambuf::underflow in the library /src/zipstreamimpl.h. Such manipulation leads to memory corruption. Local access is required to approach this attack. The exploit has been disclosed publicly and may be used.	2025-09-26	5.3	CVE-2025-10995
Open Babel -- Up to v3.1.1	A vulnerability was detected in Open Babel up to 3.1.1. This issue affects the function OBSmilesParser::ParseSmiles of the file /src/formats/smilesformat.cpp. Performing manipulation results in heap-based buffer overflow. The attack needs to be approached locally. The exploit is now public and may be used.	2025-09-26	5.3	CVE-2025-10996
Open Babel -- Up to v3.1.1	A flaw has been found in Open Babel up to 3.1.1. Impacted is the function ChemKinFormat::CheckSpecies of the file /src/formats/chemkinformat.cpp. Executing manipulation can lead to heap-based buffer overflow. The attack can only be executed locally. The exploit has been published and may be used.	2025-09-26	5.3	CVE-2025-10997
payrexx--Payrexx Payment Gateway for WooCommerce	Missing Authorization vulnerability in payrexx Payrexx Payment Gateway for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Payrexx Payment Gateway for WooCommerce: from n/a through 3.1.5.	2025-09-22	4.3	CVE-2025-59559
Pdfcrowd Dev Team--Save as PDF	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pdfcrowd Dev Team Save as PDF allows Stored XSS. This issue affects Save as PDF: from n/a through 4.5.2.	2025-09-22	6.5	CVE-2025-59552
PenciDesign--Penci Filter Everything	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Filter Everything allows DOM-Based XSS. This issue affects Penci Filter Everything: from n/a through n/a.	2025-09-22	6.5	CVE-2025-59583
PenciDesign--Penci Podcast	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Podcast allows DOM-Based XSS. This issue affects Penci Podcast: from n/a through 1.6.	2025-09-22	6.5	CVE-2025-59584
PenciDesign--Penci Portfolio	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Portfolio allows DOM-Based XSS. This issue affects Penci Portfolio: from n/a through 3.5.	2025-09-22	6.5	CVE-2025-59586
PenciDesign--Penci Recipe	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Recipe allows DOM-Based XSS. This issue affects Penci Recipe: from n/a through 4.0.	2025-09-22	6.5	CVE-2025-59585
PenciDesign--Penci Shortcodes & Performance	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Shortcodes & Performance allows DOM-Based XSS. This issue affects Penci Shortcodes & Performance: from n/a through n/a.	2025-09-22	6.5	CVE-2025-59587
PenciDesign--Soledad	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Soledad allows DOM-Based XSS. This issue affects Soledad: from n/a through 8.6.8.	2025-09-22	6.5	CVE-2025-59589
photonicgnostic--Library Bookshelves	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in photonicgnostic Library Bookshelves allows Stored XSS. This issue affects Library Bookshelves: from n/a through 5.11.	2025-09-22	6.5	CVE-2025-57964
PHPGurukul--Car Rental Project	A flaw has been found in PHPGurukul Car Rental Project 3.0. Affected by this issue is some unknown functionality of the file /carrental/search.php. Executing manipulation of the argument autofocus can lead to cross site scripting. It is	2025-09-22	4.3	CVE-2025-10794

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	possible to launch the attack remotely. The exploit has been published and may be used.			
PHPGurukul--Employee Record Management System	A security vulnerability has been detected in PHPGurukul Employee Record Management System 1.3. This impacts an unknown function of the file /myprofile.php. Such manipulation of the argument First name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	2025-09-28	4.3	CVE-2025-11112
PHPJabbers--Restaurant Menu Maker	A weakness has been identified in PHPJabbers Restaurant Menu Maker up to 1.1. Affected by this issue is some unknown functionality of the file /preview.php. This manipulation of the argument theme causes cross site scripting. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	2025-09-23	4.3	CVE-2025-10827
PickPlugins--Accordion	Missing Authorization vulnerability in PickPlugins Accordion allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Accordion: from n/a through 2.3.14.	2025-09-22	6.5	CVE-2025-58678
PickPlugins--Job Board Manager	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PickPlugins Job Board Manager allows DOM-Based XSS. This issue affects Job Board Manager: from n/a through 2.1.61.	2025-09-26	6.5	CVE-2025-60162
Picture-Planet GmbH--Verowa Connect	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Picture-Planet GmbH Verowa Connect allows Stored XSS. This issue affects Verowa Connect: from n/a through 3.2.3.	2025-09-22	6.5	CVE-2025-58257
piotnetdotcom--Piotnet Forms	Cross-Site Request Forgery (CSRF) vulnerability in piotnetdotcom Piotnet Forms allows Cross Site Request Forgery. This issue affects Piotnet Forms: from n/a through 1.0.30.	2025-09-22	4.3	CVE-2025-57933
PlayerJS--PlayerJS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PlayerJS PlayerJS allows DOM-Based XSS. This issue affects PlayerJS: from n/a through 2.24.	2025-09-22	6.5	CVE-2025-58651
Plugin Devs--Post Carousel Slider for Elementor	Missing Authorization vulnerability in Plugin Devs Post Carousel Slider for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Post Carousel Slider for Elementor: from n/a through 1.7.0.	2025-09-22	6.5	CVE-2025-57955
Portabilis--i-Educar	A vulnerability has been found in Portabilis i-Educar up to 2.10. Affected by this issue is some unknown functionality of the file /module/Cadastro/aluno. The manipulation of the argument is leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	2025-09-23	6.3	CVE-2025-10844
Portabilis--i-Educar	A vulnerability was found in Portabilis i-Educar up to 2.10. This affects an unknown part of the file /module/ComponenteCurricular/view. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	2025-09-23	6.3	CVE-2025-10845
Portabilis--i-Educar	A vulnerability was determined in Portabilis i-Educar up to 2.10. This vulnerability affects unknown code of the file /module/ComponenteCurricular/edit. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-23	6.3	CVE-2025-10846
Portabilis--i-Educar	A weakness has been identified in Portabilis i-Educar up to 2.10. Affected is an unknown function of the file /module/Api/aluno. This manipulation of the argument aluno_id causes improper authorization. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	2025-09-26	6.3	CVE-2025-11047
Portabilis--i-Educar	A security vulnerability has been detected in Portabilis i-Educar up to 2.10. Affected by this vulnerability is an unknown functionality of the file /consulta-	2025-09-26	6.3	CVE-2025-11048

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	dispensas. Such manipulation leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.			
Portabilis--i-Educar	A vulnerability was detected in Portabilis i-Educar up to 2.10. Affected by this issue is some unknown functionality of the file /unificacao-aluno. Performing manipulation results in improper authorization. Remote exploitation of the attack is possible. The exploit is now public and may be used.	2025-09-27	6.3	CVE-2025-11049
Portabilis--i-Educar	A flaw has been found in Portabilis i-Educar up to 2.10. This affects an unknown part of the file /periodo-lancamento. Executing manipulation can lead to improper authorization. The attack can be executed remotely. The exploit has been published and may be used.	2025-09-27	6.3	CVE-2025-11050
POSIMYTH--Sticky Header Effects for Elementor	Missing Authorization vulnerability in POSIMYTH Sticky Header Effects for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Sticky Header Effects for Elementor: from n/a through 2.1.2.	2025-09-22	4.3	CVE-2025-58251
Pratik Ghela--MakeStories (for Google Web Stories)	Server-Side Request Forgery (SSRF) vulnerability in Pratik Ghela MakeStories (for Google Web Stories) allows Server Side Request Forgery. This issue affects MakeStories (for Google Web Stories): from n/a through 3.0.4.	2025-09-22	4.4	CVE-2025-57984
printcart--Printcart Web to Print Product Designer for WooCommerce	Missing Authorization vulnerability in printcart Printcart Web to Print Product Designer for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Printcart Web to Print Product Designer for WooCommerce: from n/a through 2.4.3.	2025-09-22	4.3	CVE-2025-57917
Printeers--Printeers Print & Ship	Cross-Site Request Forgery (CSRF) vulnerability in Printeers Printeers Print & Ship allows Cross Site Request Forgery. This issue affects Printeers Print & Ship: from n/a through 1.17.0.	2025-09-22	5.4	CVE-2025-58224
Profession Fit--Profession Fit	Profession Fit 5.0.99 Build 44910 allows authorization bypass via a direct request for /api/challenges/{id} and also URLs for eversports, the user-management page, and the plane page.	2025-09-22	5.8	CVE-2025-59797
ProjectsAndPrograms--School Management System	A flaw has been found in ProjectsAndPrograms School Management System 1.0. Affected by this vulnerability is an unknown functionality of the file owner_panel/fetch-data/select-students.php. This manipulation of the argument select causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	2025-09-27	6.3	CVE-2025-11056
Projectworlds--Online Tours and Travels	A security vulnerability has been detected in Projectworlds Online Tours and Travels 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/change-image.php. The manipulation of the argument packageimage leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	2025-09-28	4.7	CVE-2025-11103
PROLIZ Computer Software Hardware Service Trade Ltd. Co.--OBS (Student Affairs Information System)	Authorization Bypass Through User-Controlled Key vulnerability in PROLIZ Computer Software Hardware Service Trade Ltd. Co. OBS (Student Affairs Information System) allows Parameter Injection.This issue affects OBS (Student Affairs Information System): before v26.0328.	2025-09-22	4.2	CVE-2025-0875
Proof Factor LLC--Proof Factor – Social Proof Notifications	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Proof Factor LLC Proof Factor – Social Proof Notifications allows Stored XSS. This issue affects Proof Factor – Social Proof Notifications: from n/a through 1.0.5.	2025-09-22	5.9	CVE-2025-58658
ProWCPlugins--Product Time	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ProWCPlugins Product Time Countdown for	2025-09-22	5.9	CVE-2025-57908

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Countdown for WooCommerce	WooCommerce allows Stored XSS. This issue affects Product Time Countdown for WooCommerce: from n/a through 1.6.4.			
publitio--Publitio	Server-Side Request Forgery (SSRF) vulnerability in publitio Publitio allows Server Side Request Forgery. This issue affects Publitio: from n/a through 2.2.1.	2025-09-22	6.4	CVE-2025-58962
qriouslad--System Dashboard	The System Dashboard plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.8.20. This is due to missing nonce validation on the sd_toggle_logs() function. This makes it possible for unauthenticated attackers to toggle critical logging settings including Page Access Logs, Error Logs, and Email Delivery Logs via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-26	4.3	CVE-2025-10377
Qualcomm, Inc.--Snapdragon	information disclosure while invoking calibration data from user space to update firmware size.	2025-09-24	6.1	CVE-2025-27030
Qualcomm, Inc.--Snapdragon	Information disclosure while running video usecase having rogue firmware.	2025-09-24	6.1	CVE-2025-27033
Qualcomm, Inc.--Snapdragon	Information disclosure when Video engine escape input data is less than expected minimum size.	2025-09-24	6.1	CVE-2025-27036
RadiusTheme--Team	Missing Authorization vulnerability in RadiusTheme Team allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Team: from n/a through 5.0.6.	2025-09-22	4.3	CVE-2025-57975
Rameez Iqbal--Real Estate Manager	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rameez Iqbal Real Estate Manager allows DOM-Based XSS. This issue affects Real Estate Manager: from n/a through 7.3.	2025-09-22	6.5	CVE-2025-58253
Red Hat--OpenShift Service Mesh 3	A flaw was found in the live query subscription mechanism of the database engine. This vulnerability allows record or guest users to observe unauthorized records within the same table, bypassing access controls, via crafted LIVE SELECT subscriptions when other users alter or delete records.	2025-09-26	5.7	CVE-2025-11060
Red Hat--Red Hat Enterprise v6,v7,v8,v9,10	A use-after-free vulnerability was found in libxslt while parsing xsl nodes that may lead to the dereference of expired pointers and application crash.	2025-09-25	5.5	CVE-2025-10911
Ren Ventura--WP Delete User Accounts	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ren Ventura WP Delete User Accounts allows Stored XSS. This issue affects WP Delete User Accounts: from n/a through 1.2.4.	2025-09-22	6.5	CVE-2025-58704
Richard Leishman--Mail Subscribe List	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Richard Leishman Mail Subscribe List allows Stored XSS. This issue affects Mail Subscribe List: from n/a through 2.1.10.	2025-09-22	6.5	CVE-2025-58018
Ricky Dawn--Bot Block – Stop Spam Referrals in Google Analytics	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ricky Dawn Bot Block – Stop Spam Referrals in Google Analytics allows Stored XSS. This issue affects Bot Block – Stop Spam Referrals in Google Analytics: from n/a through 2.6.	2025-09-22	5.9	CVE-2025-57935
Risto Niinemets--Estonian Shipping Methods for WooCommerce	Use of Hard-coded Credentials vulnerability in Risto Niinemets Estonian Shipping Methods for WooCommerce allows Retrieve Embedded Sensitive Data. This issue affects Estonian Shipping Methods for WooCommerce: from n/a through 1.7.2.	2025-09-22	5.3	CVE-2025-58656
Robin W--bbp topic count	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Robin W bbp topic count allows DOM-Based XSS. This issue affects bbp topic count: from n/a through 3.1.	2025-09-26	6.5	CVE-2025-60163
Ronald Huereca--Highlight and	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ronald Huereca Highlight and Share - Social Text and	2025-09-22	6.5	CVE-2025-58260

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Share Social Text and Image Sharing	Image Sharing allows Stored XSS. This issue affects Highlight and Share - Social Text and Image Sharing: from n/a through 5.1.1.			
roncoo--roncoo-pay	A vulnerability was determined in roncoo roncoo-pay up to 9428382af21cd5568319eae7429b7e1d0332ff40. Affected is an unknown function of the file /user/info/lookupList. Executing manipulation can lead to improper authorization. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-26	5.3	CVE-2025-10992
Rouergue Cration--Editor Custom Color Palette	Missing Authorization vulnerability in Rouergue Création Editor Custom Color Palette allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Editor Custom Color Palette: from n/a through 3.4.8.	2025-09-22	6.5	CVE-2025-57909
Roxnor--EmailKit	Missing Authorization vulnerability in Roxnor EmailKit allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects EmailKit: from n/a through 1.6.0.	2025-09-26	4.9	CVE-2025-60106
rozx--Recaptcha – wp	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rozx Recaptcha – wp allows Stored XSS. This issue affects Recaptcha – wp: from n/a through 0.2.6.	2025-09-26	5.9	CVE-2025-60177
Ruijie--6000-E10	A weakness has been identified in Ruijie 6000-E10 up to 2.4.3.6-20171117. This affects an unknown part of the file /view/vpn/autovpn/sub_commit.php. This manipulation of the argument key causes os command injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-22	4.7	CVE-2025-10774
Russell Jamieson--AuthorSure	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Russell Jamieson AuthorSure allows Stored XSS. This issue affects AuthorSure: from n/a through 2.3.	2025-09-22	5.9	CVE-2025-57979
Russell Jamieson--Genesis Club Lite	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Russell Jamieson Genesis Club Lite allows Stored XSS. This issue affects Genesis Club Lite: from n/a through 1.17.	2025-09-22	6.5	CVE-2025-58691
Rustaurius--Front End Users	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rustaurius Front End Users allows Stored XSS. This issue affects Front End Users: from n/a through 3.2.33.	2025-09-22	6.5	CVE-2025-58235
Rustaurius--Ultimate WP Mail	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rustaurius Ultimate WP Mail allows Stored XSS. This issue affects Ultimate WP Mail: from n/a through 1.3.8.	2025-09-22	6.5	CVE-2025-53454
Ryan Hellyer--Simple Colorbox	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ryan Hellyer Simple Colorbox allows Stored XSS. This issue affects Simple Colorbox: from n/a through 1.6.1.	2025-09-26	6.5	CVE-2025-60124
SALESmanago--SALESmanago	Missing Authorization vulnerability in SALESmanago SALESmanago allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects SALESmanago: from n/a through 3.8.1.	2025-09-22	5.3	CVE-2025-57971
SALESmanago--SALESmanago	Cross-Site Request Forgery (CSRF) vulnerability in SALESmanago SALESmanago allows Cross Site Request Forgery. This issue affects SALESmanago: from n/a through 3.8.1.	2025-09-22	4.3	CVE-2025-57970
Samsung Mobile--Retail Mode	Improper input validation in Retail Mode prior to version 5.59.4 allows self attackers to execute privileged commands on their own devices.	2025-09-25	6.6	CVE-2025-21056

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SAP_SE--SAP BI Platform	SAP BI Platform allows an attacker to modify the IP address of the LogonToken for the OpenDoc. On accessing the modified link in the browser a different server could get the ping request. This has low impact on integrity with no impact on confidentiality and availability of the system.	2025-09-23	4.3	CVE-2025-42907
SAPO--SAPO Feed	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SAPO SAPO Feed allows Stored XSS. This issue affects SAPO Feed: from n/a through 2.4.2.	2025-09-22	5.9	CVE-2025-53462
Sayful Islam--Upcoming Events Lists	Authorization Bypass Through User-Controlled Key vulnerability in Sayful Islam Upcoming Events Lists allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Upcoming Events Lists: from n/a through 1.4.0.	2025-09-22	5.4	CVE-2025-57994
Search Atlas--Search Atlas SEO	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Search Atlas Search Atlas SEO allows Stored XSS. This issue affects Search Atlas SEO: from n/a through 2.5.4.	2025-09-22	6.5	CVE-2025-58019
Shahjada--Download Manager	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Shahjada Download Manager allows Retrieve Embedded Sensitive Data. This issue affects Download Manager: from n/a through 3.3.24.	2025-09-26	5.3	CVE-2025-60092
Shahjada--Download Manager	Cross-Site Request Forgery (CSRF) vulnerability in Shahjada Download Manager allows Cross Site Request Forgery. This issue affects Download Manager: from n/a through 3.3.24.	2025-09-26	4.3	CVE-2025-60093
ShapedPlugin LLC--Quick View for WooCommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShapedPlugin LLC Quick View for WooCommerce allows Stored XSS. This issue affects Quick View for WooCommerce: from n/a through 2.2.16.	2025-09-22	6.5	CVE-2025-58228
sharkthemes--Smart Related Products	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sharkthemes Smart Related Products allows Stored XSS. This issue affects Smart Related Products: from n/a through 2.0.5.	2025-09-26	5.9	CVE-2025-60160
silence--Silencesoft RSS Reader	Server-Side Request Forgery (SSRF) vulnerability in silence Silencesoft RSS Reader allows Server Side Request Forgery. This issue affects Silencesoft RSS Reader: from n/a through 0.6.	2025-09-26	5.4	CVE-2025-60181
Sistemas Pleno--Gesto de Locao	A flaw has been found in Sistemas Pleno Gestão de Locação up to 2025.7.x. The impacted element is an unknown function of the file /api/areacliente/pessoa/validarCpf of the component CPF Handler. Executing manipulation of the argument pes_cpf can lead to authorization bypass. The attack can be executed remotely. The exploit has been published and may be used. Upgrading to version 2025.8.0 is sufficient to resolve this issue. It is advisable to upgrade the affected component.	2025-09-25	5.3	CVE-2025-10947
Skimlinks--Skimlinks Affiliate Marketing Tool	Missing Authorization vulnerability in Skimlinks Skimlinks Affiliate Marketing Tool allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Skimlinks Affiliate Marketing Tool: from n/a through 1.3.	2025-09-22	5.3	CVE-2025-57944
Skimlinks--Skimlinks Affiliate Marketing Tool	Server-Side Request Forgery (SSRF) vulnerability in Skimlinks Skimlinks Affiliate Marketing Tool allows Server Side Request Forgery. This issue affects Skimlinks Affiliate Marketing Tool: from n/a through 1.3.	2025-09-22	4.4	CVE-2025-57943
skyword--Skyword API Plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skyword Skyword API Plugin allows Stored XSS. This issue affects Skyword API Plugin: from n/a through 2.5.3.	2025-09-22	6.5	CVE-2025-58703
SmartDataSoft--DriCub	Missing Authorization vulnerability in SmartDataSoft DriCub allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects DriCub: from n/a through 2.9.	2025-09-22	5.3	CVE-2025-58004

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SmartDataSoft--DriCub	Server-Side Request Forgery (SSRF) vulnerability in SmartDataSoft DriCub allows Server Side Request Forgery. This issue affects DriCub: from n/a through 2.9.	2025-09-22	5.4	CVE-2025-58005
snapwidget--SnapWidget Social Photo Feed Widget	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in snapwidget SnapWidget Social Photo Feed Widget allows DOM-Based XSS. This issue affects SnapWidget Social Photo Feed Widget: from n/a through 1.1.0.	2025-09-22	6.5	CVE-2025-58241
softaculous--Backuply Backup, Restore, Migrate and Clone	The Backuply - Backup, Restore, Migrate and Clone plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete backup functionality in all versions up to, and including, 1.4.8. This makes it possible for authenticated attackers, with Administrator-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	2025-09-26	6.5	CVE-2025-10307
solwininfotech--Blog Designer	Missing Authorization vulnerability in solwininfotech Blog Designer allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Blog Designer: from n/a through 3.1.8.	2025-09-22	5.4	CVE-2025-57990
sonalsinha21--SKT Blocks	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sonalsinha21 SKT Blocks allows Stored XSS. This issue affects SKT Blocks: from n/a through 2.5.	2025-09-26	6.5	CVE-2025-60138
SourceCodester--Pet Grooming Management Software	A security vulnerability has been detected in SourceCodester Pet Grooming Management Software 1.0. This affects an unknown part of the file /admin/edit.php. 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.	2025-09-23	6.3	CVE-2025-10828
SourceCodester--Pet Grooming Management Software	A security flaw has been discovered in SourceCodester Pet Grooming Management Software 1.0. This impacts an unknown function of the file /admin/view_payorder.php. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	2025-09-23	6.3	CVE-2025-10835
SourceCodester--Pet Grooming Management Software	A security flaw has been discovered in SourceCodester Pet Grooming Management Software 1.0. The impacted element is an unknown function of the file /admin/inv-print.php. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	2025-09-23	6.3	CVE-2025-10839
SourceCodester--Pet Grooming Management Software	A weakness has been identified in SourceCodester Pet Grooming Management Software 1.0. This affects an unknown function of the file /admin/print-payment.php. This manipulation of the argument sql111 causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited.	2025-09-23	6.3	CVE-2025-10840
SourceCodester--Pet Grooming Management Software	A vulnerability has been found in SourceCodester Pet Grooming Management Software 1.0. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. The attack is possible to be carried out remotely.	2025-09-27	4.3	CVE-2025-11051
SourceCodester--Simple Forum Discussion System	A security flaw has been discovered in SourceCodester Simple Forum Discussion System 1.0. This affects an unknown function of the file /ajax.php?action=save_category. The manipulation of the argument Description results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	2025-09-22	6.3	CVE-2025-10790
Space Studio--Click & Tweet	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Space Studio Click & Tweet allows Stored XSS. This issue affects Click & Tweet: from n/a through 0.8.9.	2025-09-26	5.9	CVE-2025-60179

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
specialk--Banhammer Monitor Site Traffic, Block Bad Users and Bots	The Banhammer - Monitor Site Traffic, Block Bad Users and Bots plugin for WordPress is vulnerable to Blocking Bypass in all versions up to, and including, 3.4.8. This is due to a site-wide "secret key" being deterministically generated from a constant character set using md5() and base64_encode() and then stored in the `banhammer_secret_key` option. This makes it possible for unauthenticated attackers to bypass the plugin's logging and blocking by appending a GET parameter named `banhammer-process_{SECRET}` where `{SECRET}` is the predictable value, thereby causing Banhammer to abort its protections for that request.	2025-09-26	5.3	CVE-2025-10745
spwebguy--Team Members	The Team Members plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the first and last name fields in all versions up to, and including, 5.3.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-27	6.4	CVE-2025-8440
StellarWP--WPComplete	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in StellarWP WPComplete allows Stored XSS. This issue affects WPComplete: from n/a through 2.9.5.2.	2025-09-22	6.5	CVE-2025-58974
Stephanie Leary--Dashboard Notepad	Cross-Site Request Forgery (CSRF) vulnerability in Stephanie Leary Dashboard Notepad allows Cross Site Request Forgery. This issue affects Dashboard Notepad: from n/a through 1.42.	2025-09-22	4.3	CVE-2025-57927
Stonehenge Creations--Events Manager – OpenStreetMaps	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stonehenge Creations Events Manager – OpenStreetMaps allows Stored XSS. This issue affects Events Manager – OpenStreetMaps: from n/a through 4.2.1.	2025-09-22	6.5	CVE-2025-58265
straightvisions GmbH--SV Proven Expert	Cross-Site Request Forgery (CSRF) vulnerability in straightvisions GmbH SV Proven Expert allows Cross Site Request Forgery. This issue affects SV Proven Expert: from n/a through 2.0.06.	2025-09-22	4.3	CVE-2025-58010
Strategy11 Team--AWP Classifieds	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Strategy11 Team AWP Classifieds allows Code Injection. This issue affects AWP Classifieds: from n/a through 4.3.5.	2025-09-22	5.3	CVE-2025-57928
Stylemix--MasterStudy LMS	Missing Authorization vulnerability in Stylemix MasterStudy LMS allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects MasterStudy LMS: from n/a through 3.6.20.	2025-09-22	6.5	CVE-2025-59576
Stylemix--MasterStudy LMS	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in Stylemix MasterStudy LMS allows Leveraging Race Conditions. This issue affects MasterStudy LMS: from n/a through 3.6.20.	2025-09-22	4.3	CVE-2025-59577
Sumit Singh--Classic Widgets with Block-based Widgets	Missing Authorization vulnerability in Sumit Singh Classic Widgets with Block-based Widgets allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Classic Widgets with Block-based Widgets: from n/a through 1.0.1.	2025-09-22	5.3	CVE-2025-58029
Suresh Kumar Mukhiya--Append extensions on Pages	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Suresh Kumar Mukhiya Append extensions on Pages allows Stored XSS. This issue affects Append extensions on Pages: from n/a through 1.1.2.	2025-09-22	5.9	CVE-2025-57940
Syam Mohan--WPFront User Role Editor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Syam Mohan WPFront User Role Editor allows Stored XSS. This issue affects WPFront User Role Editor: from n/a through 4.2.3.	2025-09-26	6.5	CVE-2025-60102
Syed Balkhi--AffiliateWP	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Syed Balkhi AffiliateWP - External Referral Links allows	2025-09-22	5.9	CVE-2025-53460

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
External Referral Links	Stored XSS. This issue affects AffiliateWP - External Referral Links: from n/a through 1.2.0.			
Syed Balkhi--All In One SEO Pack	Missing Authorization vulnerability in Syed Balkhi All In One SEO Pack allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects All In One SEO Pack: from n/a through 4.8.7.	2025-09-22	5.4	CVE-2025-58650
Syed Balkhi--All In One SEO Pack	Insertion of Sensitive Information Into Sent Data vulnerability in Syed Balkhi All In One SEO Pack allows Retrieve Embedded Sensitive Data. This issue affects All In One SEO Pack: from n/a through 4.8.7.	2025-09-22	4.3	CVE-2025-58649
Syed Balkhi--aThemes Addons for Elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Syed Balkhi aThemes Addons for Elementor allows Stored XSS. This issue affects aThemes Addons for Elementor: from n/a through 1.1.3.	2025-09-26	6.5	CVE-2025-60112
TangibleWP--Vehica Core	Cross-Site Request Forgery (CSRF) vulnerability in TangibleWP Vehica Core allows Cross Site Request Forgery. This issue affects Vehica Core: from n/a through 1.0.100.	2025-09-26	4.3	CVE-2025-60117
tapfiliate--Tapfiliate	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tapfiliate Tapfiliate allows Stored XSS. This issue affects Tapfiliate: from n/a through 3.2.2.	2025-09-22	6.5	CVE-2025-58689
Tareq Hasan--WP User Frontend	Missing Authorization vulnerability in Tareq Hasan WP User Frontend allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP User Frontend: from n/a through 4.1.11.	2025-09-22	5.4	CVE-2025-58672
Tareq Hasan--WP User Frontend	Improper Control of Generation of Code ('Code Injection') vulnerability in Tareq Hasan WP User Frontend allows Code Injection. This issue affects WP User Frontend: from n/a through 4.1.11.	2025-09-22	5.4	CVE-2025-58673
Techeshta--Card Elements for WPBakery	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Techeshta Card Elements for WPBakery allows DOM-Based XSS. This issue affects Card Elements for WPBakery: from n/a through 1.0.8.	2025-09-22	6.5	CVE-2025-58220
templateinvaders--TI WooCommerce Wishlist	Missing Authorization vulnerability in templateinvaders TI WooCommerce Wishlist allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects TI WooCommerce Wishlist: from n/a through 2.10.0.	2025-09-22	5.3	CVE-2025-58247
Tenda--AC18	A security vulnerability has been detected in Tenda AC18 15.03.05.19. The impacted element is an unknown function of the file /goform/AdvSetLanip. The manipulation of the argument lanIp leads to command injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	2025-09-28	6.3	CVE-2025-11121
termageddon--Termageddon: Cookie Consent & Privacy Compliance	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in termageddon Termageddon: Cookie Consent & Privacy Compliance allows Stored XSS. This issue affects Termageddon: Cookie Consent & Privacy Compliance: from n/a through 1.8.1.	2025-09-22	6.5	CVE-2025-58026
Terry L.--SEO Search Permalink	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Terry L. SEO Search Permalink allows Stored XSS. This issue affects SEO Search Permalink: from n/a through 1.0.3.	2025-09-26	5.9	CVE-2025-60184
ThemeGoods--Grand Conference Theme Custom Post Type	Missing Authorization vulnerability in ThemeGoods Grand Conference Theme Custom Post Type allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Grand Conference Theme Custom Post Type: from n/a through 2.6.3.	2025-09-26	5.4	CVE-2025-60116

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
themelooks--FoodBook	Insertion of Sensitive Information Into Sent Data vulnerability in themelooks FoodBook allows Retrieve Embedded Sensitive Data. This issue affects FoodBook: from n/a through 4.7.1.	2025-09-26	5.3	CVE-2025-60125
themeplugs--Authorsy	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themeplugs Authorsy allows Stored XSS. This issue affects Authorsy: from n/a through 1.0.5.	2025-09-26	6.5	CVE-2025-27006
Themepoints--Carousel Ultimate	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Carousel Ultimate allows Stored XSS. This issue affects Carousel Ultimate: from n/a through 1.8.	2025-09-22	6.5	CVE-2025-58652
Themepoints--Logo Showcase	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Logo Showcase allows Stored XSS. This issue affects Logo Showcase: from n/a through 3.0.9.	2025-09-22	6.5	CVE-2025-58684
themespride--Advanced Appointment Booking & Scheduling	Cross-Site Request Forgery (CSRF) vulnerability in themespride Advanced Appointment Booking & Scheduling allows Cross Site Request Forgery. This issue affects Advanced Appointment Booking & Scheduling: from n/a through 1.9.	2025-09-22	4.3	CVE-2025-57978
Themeum--Qubely	Insertion of Sensitive Information Into Sent Data vulnerability in Themeum Qubely allows Retrieve Embedded Sensitive Data. This issue affects Qubely: from n/a through 1.8.14.	2025-09-22	4.3	CVE-2025-58249
Themeum--Qubely	Missing Authorization vulnerability in Themeum Qubely allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Qubely: from n/a through 1.8.14.	2025-09-22	4.3	CVE-2025-58663
themewant--Easy Hotel Booking	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themewant Easy Hotel Booking allows DOM-Based XSS. This issue affects Easy Hotel Booking: from n/a through 1.6.9.	2025-09-22	6.5	CVE-2025-57938
themifyme--Themify Builder	The Themify Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several parameters in all versions up to, and including, 7.6.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The vulnerability was partially patched in version 7.6.9.	2025-09-24	6.4	CVE-2025-9353
thetechtribe--The Tribal	Insertion of Sensitive Information Into Sent Data vulnerability in thetechtribe The Tribal allows Retrieve Embedded Sensitive Data. This issue affects The Tribal: from n/a through 1.3.3.	2025-09-26	5.3	CVE-2025-60140
thetechtribe--The Tribal	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in thetechtribe The Tribal allows Stored XSS. This issue affects The Tribal: from n/a through 1.3.3.	2025-09-26	5.9	CVE-2025-60141
ThimPress--WP Events Manager	Missing Authorization vulnerability in ThimPress WP Events Manager allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Events Manager: from n/a through 2.2.1.	2025-09-22	5.3	CVE-2025-57987
Timur Kamaev--Kama Click Counter	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Timur Kamaev Kama Click Counter allows Stored XSS. This issue affects Kama Click Counter: from n/a through 4.0.4.	2025-09-22	6.5	CVE-2025-58682
tmatsuur--Slightly troublesome permalink	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tmatsuur Slightly troublesome permalink allows Stored XSS. This issue affects Slightly troublesome permalink: from n/a through 1.2.0.	2025-09-22	5.9	CVE-2025-57959

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tmontg1--Form Generator for WordPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tmontg1 Form Generator for WordPress allows Stored XSS. This issue affects Form Generator for WordPress: from n/a through 1.5.2.	2025-09-22	5.9	CVE-2025-58665
Tomas Cordero--Safety Exit	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tomas Cordero Safety Exit allows Stored XSS. This issue affects Safety Exit: from n/a through 1.8.0.	2025-09-22	5.9	CVE-2025-57980
TravelMap--Travel Map	Cross-Site Request Forgery (CSRF) vulnerability in TravelMap Travel Map allows Cross Site Request Forgery. This issue affects Travel Map: from n/a through 1.0.3.	2025-09-22	4.3	CVE-2025-57960
trustindex--Widgets for Tiktok Feed	The Widgets for Tiktok Feed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'trustindex-feed' shortcode in all versions up to, and including, 1.7.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2025-09-26	6.4	CVE-2025-8906
Trustpilot--Trustpilot Reviews	Missing Authorization vulnerability in Trustpilot Trustpilot Reviews allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Trustpilot Reviews: from n/a through 2.5.925.	2025-09-22	4.3	CVE-2025-57997
trustreviews--Trust Reviews plugin for Google, Tripadvisor, Yelp, Airbnb and other platforms	The Trust Reviews plugin for Google, Tripadvisor, Yelp, Airbnb and other platforms plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incorrect nonce validation on the feed_save function. This makes it possible for unauthenticated attackers to create or modify feed entries via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2025-09-27	6.1	CVE-2025-9899
tryinteract--Interact: Embed A Quiz On Your Site	Cross-Site Request Forgery (CSRF) vulnerability in tryinteract Interact: Embed A Quiz On Your Site allows Cross Site Request Forgery. This issue affects Interact: Embed A Quiz On Your Site: from n/a through 3.1.	2025-09-22	4.3	CVE-2025-58675
tuyennv--TZ PlusGallery	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tuyennv TZ PlusGallery allows Stored XSS. This issue affects TZ PlusGallery: from n/a through 1.5.5.	2025-09-22	5.9	CVE-2025-57974
Uncanny Owl--Uncanny Toolkit for LearnDash	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Uncanny Owl Uncanny Toolkit for LearnDash allows Stored XSS. This issue affects Uncanny Toolkit for LearnDash: from n/a through 3.0.7.3.	2025-09-22	6.5	CVE-2025-57988
Unitree--Go2	Unitree Go2, G1, H1, and B2 devices through 2025-09-20 accept any handshake secret with the unitree substring.	2025-09-26	5	CVE-2025-60251
Unitree--Go2	Unitree Go2, G1, H1, and B2 devices through 2025-09-20 decrypt BLE packet data by using the df98b715d5c6ed2b25817b6f2554124a key and the 2841ae97419c2973296a0d4bdfe19a4f IV.	2025-09-26	4.7	CVE-2025-60250
Vadim Bogaiskov--Bg Church Memos	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vadim Bogaiskov Bg Church Memos allows DOM-Based XSS. This issue affects Bg Church Memos: from n/a through 1.1.	2025-09-22	6.5	CVE-2025-58242
VibeThemes--WPLMS	Missing Authorization vulnerability in VibeThemes WPLMS allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WPLMS : from n/a through 4.970.	2025-09-22	4.3	CVE-2025-58668
Vikas Ratudi--VPSUForm	Missing Authorization vulnerability in Vikas Ratudi VPSUForm allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects VPSUForm: from n/a through 3.2.20.	2025-09-22	4.3	CVE-2025-58957
Vimesoft Information	Insertion of Sensitive Information Into Sent Data vulnerability in Vimesoft Information Technologies and Software Inc. Vimesoft Corporate Messaging	2025-09-26	5.3	CVE-2025-11025

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Technologies and Software Inc.--Vimesoft Corporate Messaging Platform	Platform allows Retrieve Embedded Sensitive Data.This issue affects Vimesoft Corporate Messaging Platform: from V1.3.0 before V2.0.0.			
vstakhov--libucl	A vulnerability has been found in vstakhov libucl up to 0.9.2. Affected by this vulnerability is the function ucl_include_common of the file /src/ucl_util.c. Such manipulation leads to heap-based buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used.	2025-09-26	5.3	CVE-2025-11010
VW THEMES--Ibtana	Missing Authorization vulnerability in VW THEMES Ibtana allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Ibtana: from n/a through 1.2.5.3.	2025-09-22	6.5	CVE-2025-59581
WAGO--Solution Builder	The web application allows an unauthenticated remote attacker to learn information about existing user accounts with their corresponding role due to missing authentication for critical function.	2025-09-24	5.3	CVE-2025-41716
Wavlink--NU516U1	A flaw has been found in Wavlink NU516U1 M16U1_V240425. Impacted is the function sub_403010 of the file /cgi-bin/wireless.cgi of the component AddMac Page. This manipulation of the argument macAddr causes command injection. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	6.3	CVE-2025-10958
Wavlink--NU516U1	A vulnerability has been found in Wavlink NU516U1 M16U1_V240425. The affected element is the function sub_401778 of the file /cgi-bin/firewall.cgi. Such manipulation of the argument dmz_flag leads to command injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	6.3	CVE-2025-10959
Wavlink--NU516U1	A vulnerability was found in Wavlink NU516U1 M16U1_V240425. The impacted element is the function sub_402D1C of the file /cgi-bin/wireless.cgi of the component DeleteMac Page. Performing manipulation of the argument delete_list results in command injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	6.3	CVE-2025-10960
Wavlink--NU516U1	A vulnerability was identified in Wavlink NU516U1 M16U1_V240425. This impacts the function sub_403198 of the file /cgi-bin/wireless.cgi of the component SetName Page. The manipulation of the argument mac_5g leads to command injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	6.3	CVE-2025-10962
Wavlink--NU516U1	A security flaw has been discovered in Wavlink NU516U1 M16U1_V240425. Affected is the function sub_4016F0 of the file /cgi-bin/firewall.cgi. The manipulation of the argument del_flag results in command injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	6.3	CVE-2025-10963
Wavlink--NU516U1	A weakness has been identified in Wavlink NU516U1. Affected by this vulnerability is the function sub_401B30 of the file /cgi-bin/firewall.cgi. This manipulation of the argument remoteManagementEnabled causes command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	6.3	CVE-2025-10964

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Wavlink--NU516U1	A vulnerability was determined in Wavlink NU516U1 M16U1_V240425. This affects the function sub_4030C0 of the file /cgi-bin/wireless.cgi of the component Delete_Mac_list Page. Executing manipulation of the argument delete_list can lead to command injection. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	5.5	CVE-2025-10961
Wavlink--WL-NU516U1	A security vulnerability has been detected in Wavlink WL-NU516U1 240425. This vulnerability affects the function sub_4012A0 of the file /cgi-bin/login.cgi. Such manipulation of the argument ipaddr leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-22	4.7	CVE-2025-10775
wazuh--wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. In versions starting from 3.8.0 to before 4.11.0, wazuh-analysisd is vulnerable to a heap buffer overflow when parsing XML elements from Windows EventChannel messages. This issue has been patched in version 4.11.0.	2025-09-27	6.5	CVE-2025-59938
Webbeyaz Website Design--Website Software	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Webbeyaz Website Design Website Software allows Cross-Site Scripting (XSS).This issue affects Website Software: through 2025.07.14.	2025-09-26	6.1	CVE-2025-6396
webmaniabr--Nota Fiscal Eletrnica WooCommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webmaniabr Nota Fiscal Eletrônica WooCommerce allows Stored XSS. This issue affects Nota Fiscal Eletrônica WooCommerce: from n/a through 3.4.0.6.	2025-09-26	5.9	CVE-2025-60158
webmaniabr--Nota Fiscal Eletrnica WooCommerce	Missing Authorization vulnerability in webmaniabr Nota Fiscal Eletrônica WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Nota Fiscal Eletrônica WooCommerce: from n/a through 3.4.0.6.	2025-09-26	4.3	CVE-2025-60159
webvitaly--Login-Logout	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly Login-Logout allows Stored XSS. This issue affects Login-Logout: from n/a through 3.8.	2025-09-22	5.9	CVE-2025-53467
webvitaly--Page-list	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly Page-list allows Stored XSS. This issue affects Page-list: from n/a through 5.7.	2025-09-22	6.5	CVE-2025-58030
webvitaly--Sitekit	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly Sitekit allows Stored XSS. This issue affects Sitekit: from n/a through 2.0.	2025-09-22	6.5	CVE-2025-58229
WebWizards--MarketKing	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebWizards MarketKing allows Stored XSS. This issue affects MarketKing: from n/a through 2.0.92.	2025-09-22	6.5	CVE-2025-58702
weDevs--WP Project Manager	Use of Hard-coded Credentials vulnerability in weDevs WP Project Manager allows Retrieve Embedded Sensitive Data. This issue affects WP Project Manager: from n/a through 2.6.25.	2025-09-22	5.3	CVE-2025-58269
wedos.com--WEDOS Global	Missing Authorization vulnerability in wedos.com WEDOS Global allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects WEDOS Global: from n/a through 1.2.2.	2025-09-26	5.3	CVE-2025-60130
Will.I.am--Simple Restaurant Menu	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Will.I.am Simple Restaurant Menu allows Stored XSS. This issue affects Simple Restaurant Menu: from n/a through 1.2.	2025-09-22	5.9	CVE-2025-58647

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Woostify--Woostify	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Woostify Woostify allows Stored XSS. This issue affects Woostify: from n/a through 2.4.2.	2025-09-26	5.9	CVE-2025-60101
WP Chill--Passster	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Passster allows Stored XSS. This issue affects Passster: from n/a through 4.2.18.	2025-09-22	6.5	CVE-2025-57926
WP Chill--Revive.so	Missing Authorization vulnerability in WP Chill Revive.so allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Revive.so: from n/a through 2.0.6.	2025-09-22	4.3	CVE-2025-59551
WP CodeUs--WP Proposals	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP CodeUs WP Proposals allows Stored XSS. This issue affects WP Proposals: from n/a through 2.3.	2025-09-22	6.5	CVE-2025-57965
WP Delicious--Delisho	Missing Authorization vulnerability in WP Delicious Delisho allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Delisho: from n/a through 1.1.3.	2025-09-26	4.3	CVE-2025-60128
WP Swings--Upsell Order Bump Offer for WooCommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Swings Upsell Order Bump Offer for WooCommerce allows Stored XSS. This issue affects Upsell Order Bump Offer for WooCommerce: from n/a through 3.0.7.	2025-09-22	6.5	CVE-2025-59565
WP Travel Engine--WP Travel Engine	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Travel Engine WP Travel Engine allows Stored XSS. This issue affects WP Travel Engine: from n/a through 1.4.2.	2025-09-22	6.5	CVE-2025-59574
WP-EXPERTS.IN--Sales Count Manager for WooCommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP-EXPERTS.IN Sales Count Manager for WooCommerce allows Stored XSS. This issue affects Sales Count Manager for WooCommerce: from n/a through 2.5.	2025-09-22	5.9	CVE-2025-57904
WPBean--Advance Portfolio Grid	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBean Advance Portfolio Grid allows Stored XSS. This issue affects Advance Portfolio Grid: from n/a through 1.07.6.	2025-09-22	5.9	CVE-2025-57982
WPBean--WPB Quick View for WooCommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBean WPB Quick View for WooCommerce allows Stored XSS. This issue affects WPB Quick View for WooCommerce: from n/a through 2.1.8.	2025-09-22	6.5	CVE-2025-57967
wpcraft--WooMS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpcraft WooMS allows Stored XSS. This issue affects WooMS: from n/a through 9.12.	2025-09-22	5.9	CVE-2025-57956
wpcraft--WooMS	Missing Authorization vulnerability in wpcraft WooMS allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WooMS: from n/a through 9.12.	2025-09-22	5.3	CVE-2025-57957
wpdirectorykit--WP Directory Kit	Missing Authorization vulnerability in wpdirectorykit WP Directory Kit allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Directory Kit: from n/a through 1.3.8.	2025-09-26	5.3	CVE-2025-60120
WPFactory--Adverts	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Adverts allows DOM-Based XSS. This issue affects Adverts: from n/a through 1.4.	2025-09-22	6.5	CVE-2025-57911
WPFactory--Helpdesk Support	Missing Authorization vulnerability in WPFactory Helpdesk Support Ticket System for WooCommerce allows Exploiting Incorrectly Configured Access Control Security	2025-09-22	4.3	CVE-2025-57972

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Ticket System for WooCommerce	Levels. This issue affects Helpdesk Support Ticket System for WooCommerce: from n/a through 2.0.2.			
wpkoithemes--WPKoi Templates for Elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpkoithemes WPKoi Templates for Elementor allows DOM-Based XSS. This issue affects WPKoi Templates for Elementor: from n/a through 3.4.1.	2025-09-22	6.5	CVE-2025-57999
wpo-HR--NGG Smart Image Search	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpo-HR NGG Smart Image Search allows Stored XSS. This issue affects NGG Smart Image Search: from n/a through 3.4.3.	2025-09-22	6.5	CVE-2025-58027
wpshuffle--Subscribe to Download	Missing Authorization vulnerability in wpshuffle Subscribe to Download allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Subscribe to Download: from n/a through 2.0.9.	2025-09-26	4.3	CVE-2025-60148
wpshuffle--Subscribe To Unlock	Missing Authorization vulnerability in wpshuffle Subscribe To Unlock allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Subscribe To Unlock: from n/a through 1.1.5.	2025-09-26	4.3	CVE-2025-60152
wpshuffle--WP Subscription Forms PRO	Missing Authorization vulnerability in wpshuffle WP Subscription Forms PRO allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Subscription Forms PRO: from n/a through 2.0.5.	2025-09-26	4.3	CVE-2025-60166
WPSuperiors Developer--WooCommerce Additional Fees On Checkout (Free)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPSuperiors Developer WooCommerce Additional Fees On Checkout (Free) allows Stored XSS. This issue affects WooCommerce Additional Fees On Checkout (Free): from n/a through 1.5.0.	2025-09-22	5.9	CVE-2025-57903
WPXPO--WowAddons	Missing Authorization vulnerability in WPXPO WowAddons allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WowAddons: from n/a through 1.0.17.	2025-09-22	5.3	CVE-2025-57958
WSO2--WSO2 API Manager	An information disclosure vulnerability exists in multiple WSO2 products due to improper implementation of the enrich mediator. Authenticated users may be able to view unintended business data from other mediation contexts because the internal state is not properly isolated or cleared between executions. This vulnerability does not impact user credentials or access tokens but may lead to leakage of sensitive business information handled during message flows.	2025-09-23	6.5	CVE-2024-4598
WSO2--WSO2 API Manager	An authenticated remote code execution (RCE) vulnerability exists in multiple WSO2 products due to improper input validation in the event processor admin service. A user with administrative access to the SOAP admin services can exploit this flaw by deploying a Siddhi execution plan containing malicious Java code, resulting in arbitrary code execution on the server. Exploitation of this vulnerability requires a valid user account with administrative privileges, limiting the attack surface to authenticated but potentially malicious users.	2025-09-23	6.7	CVE-2025-5717
WSO2--WSO2 API Manager	An authenticated stored cross-site scripting (XSS) vulnerability exists in multiple WSO2 products due to improper validation of user-supplied input during API document upload in the Publisher portal. A user with publisher privileges can upload a crafted API document containing malicious JavaScript, which is later rendered in the browser when accessed by other users. A successful attack could result in redirection to malicious websites, unauthorized UI modifications, or exfiltration of browser-accessible data. However, session-related sensitive cookies are protected by the httpOnly flag, preventing session hijacking.	2025-09-23	4.8	CVE-2025-4760
WSO2--WSO2 Enterprise Integrator	An arbitrary file upload vulnerability exists in multiple WSO2 products due to improper validation of user-supplied filenames in the BPEL uploader SOAP service endpoint. A malicious actor with administrative privileges can upload arbitrary files to a user-controlled location on the server. By leveraging this vulnerability, an	2025-09-26	6.7	CVE-2025-1862

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker can upload a specially crafted payload and achieve remote code execution (RCE), potentially compromising the server and its data.			
WSO2--WSO2 Identity Server	A reflected cross-site scripting (XSS) vulnerability exists in the account registration flow of WSO2 Identity Server due to improper output encoding. A malicious actor can exploit this vulnerability by injecting a crafted payload that is reflected in the server response, enabling the execution of arbitrary JavaScript in the victim's browser. This vulnerability could allow attackers to redirect users to malicious websites, modify the user interface, or exfiltrate data from the browser. However, session-related sensitive cookies are protected using the httpOnly flag, which mitigates the risk of session hijacking.	2025-09-23	6.1	CVE-2025-0209
WSO2--WSO2 Identity Server as Key Manager	A content spoofing vulnerability exists in multiple WSO2 products due to improper error message handling. Under certain conditions, error messages are passed through URL parameters without validation, allowing malicious actors to inject arbitrary content into the UI. By exploiting this vulnerability, attackers can manipulate browser-displayed error messages, enabling social engineering attacks through deceptive or misleading content.	2025-09-23	4.3	CVE-2024-6429
WSO2--WSO2 Open Banking IAM	A cross-tenant authentication vulnerability exists in multiple WSO2 products due to improper cryptographic design in Adaptive Authentication. A single cryptographic key is used across all tenants to sign authentication cookies, allowing a privileged user in one tenant to forge authentication cookies for users in other tenants. Because the Auto-Login feature is enabled by default, this flaw may allow an attacker to gain unauthorized access and potentially take over accounts in other tenants. Successful exploitation requires access to Adaptive Authentication functionality, which is typically restricted to high-privileged users. The vulnerability is only exploitable when Auto-Login is enabled, reducing its practical impact in deployments where the feature is disabled.	2025-09-23	6.8	CVE-2025-0663
xnau webdesign--Participants Database	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in xnau webdesign Participants Database allows Stored XSS. This issue affects Participants Database: from n/a through 2.7.6.3.	2025-09-22	6.5	CVE-2025-58008
yangzongzhuan--RuoYi	A security flaw has been discovered in yangzongzhuan RuoYi up to 4.8.1. This vulnerability affects unknown code of the file /system/role/authUser/selectAll. Performing manipulation of the argument userIds results in improper authorization. The attack can be initiated remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-26	6.3	CVE-2025-10989
YayCommerce--YayCurrency	Improper Control of Generation of Code ('Code Injection') vulnerability in YayCommerce YayCurrency allows Code Injection. This issue affects YayCurrency: from n/a through 3.2.	2025-09-26	6.6	CVE-2025-60114
Yext--Yext	Missing Authorization vulnerability in Yext Yext allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Yext: from n/a through 1.1.3.	2025-09-26	5.3	CVE-2025-60129
yonifre--Lenix scss compiler	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in yonifre Lenix scss compiler allows Stored XSS. This issue affects Lenix scss compiler: from n/a through 1.2.	2025-09-26	5.9	CVE-2025-60144
yonifre--Lenix scss compiler	Cross-Site Request Forgery (CSRF) vulnerability in yonifre Lenix scss compiler allows Cross Site Request Forgery. This issue affects Lenix scss compiler: from n/a through 1.2.	2025-09-26	4.3	CVE-2025-60145
YunaiV--ruoyi-vue-pro	A vulnerability was identified in YunaiV ruoyi-vue-pro up to 2025.09. This affects an unknown part of the file /crm/business/transfer. Such manipulation leads to improper authorization. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-26	6.3	CVE-2025-10988

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
YunaiV--yudao-cloud	A vulnerability was determined in YunaiV yudao-cloud up to 2025.09. Affected by this issue is some unknown functionality of the file /crm/contact/transfer of the component HTTP Request Handler. This manipulation of the argument contactId causes improper authorization. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-26	6.3	CVE-2025-10987
zhuimengshaonian--wisdom-education	A security vulnerability has been detected in zhuimengshaonian wisdom-education up to 1.0.4. This vulnerability affects the function selectStudentExamInfoList of the file src/main/java/com/education/api/controller/student/ExamInfoController.java. Such manipulation of the argument subjectId leads to improper authorization. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	2025-09-27	4.3	CVE-2025-11080
Zoho Flow--Zoho Flow	Cross-Site Request Forgery (CSRF) vulnerability in Zoho Flow Zoho Flow allows Cross Site Request Forgery. This issue affects Zoho Flow: from n/a through 2.14.1.	2025-09-22	4.3	CVE-2025-59568
Zoho Subscriptions--Zoho Billing	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zoho Subscriptions Zoho Billing allows DOM-Based XSS. This issue affects Zoho Billing: from n/a through 4.1.	2025-09-22	6.5	CVE-2025-57963

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wp_all_export_project -- wp_all_export	The Export any WordPress data to XML/CSV WordPress plugin before 1.3.1 does not escape its Export's Name before outputting it in Manage Exports settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	2021-11-08	3.5	CVE-2021-24708
Alludo--MindManager	In Alludo MindManager before 25.0.208 on Windows, attackers could potentially execute code as other local users on the same machine if they could write DLL files to directories within victims' DLL search paths.	2025-09-16	2.2	CVE-2025-30075
clickstudios--Passwordstate	Click Studios Passwordstate before 9.9 Build 9972 has a potential authentication bypass for Passwordstate emergency access. By using a crafted URL while on the Emergency Access web page, an unauthorized person can gain access to the Passwordstate Administration section.	2025-09-16	3.2	CVE-2025-59453
EVerest--libocpp	The OCPP implementation in libocpp before 0.26.2 allows a denial of service (EVerest crash) via JSON input larger than 255 characters, because a CiString<255> object is created with StringTooLarge set to Throw.	2025-09-15	3.1	CVE-2025-59398
EVerest--libocpp	libocpp before 0.28.0 allows a denial of service (EVerest crash) because a secondary exception is thrown during error message generation.	2025-09-15	3.1	CVE-2025-59399
fedorindutny--ip	The ip (aka node-ip) package through 2.0.1 (in NPM) might allow SSRF because the IP address value 017700000001 is improperly categorized as globally routable via isPublic. NOTE: this issue exists because of an incomplete fix for CVE-2024-29415.	2025-09-16	3.2	CVE-2025-59436
fedorindutny--ip	The ip (aka node-ip) package through 2.0.1 (in NPM) might allow SSRF because the IP address value 0 is improperly categorized as globally routable via isPublic. NOTE: this issue exists because of an incomplete fix for CVE-2024-29415. NOTE: in current versions of several applications, connection attempts to the IP address 0 (interpreted as 0.0.0.0) are blocked with error messages such as net::ERR_ADDRESS_INVALID. However, in some situations that depend on both application version and operating system, connection attempts to 0 and 0.0.0.0 are considered connection attempts to 127.0.0.1 (and, for this reason, a false value of isPublic would be preferable).	2025-09-16	3.2	CVE-2025-59437
feiskyer--mcp-kubernetes-server	feiskyer mcp-kubernetes-server through 0.1.11 does not consider chained commands in the implementation of --disable-write and --disable-delete, e.g., it allows a "kubectl version; kubectl delete pod" command because the first word (i.e., "version") is not a write or delete operation.	2025-09-15	3.7	CVE-2025-59376
feiskyer--mcp-kubernetes-server	feiskyer mcp-kubernetes-server through 0.1.11 allows OS command injection, even in read-only mode, via /mcp/kubectl because shell=True is used. NOTE: this is unrelated to mcp-server-kubernetes and CVE-2025-53355.	2025-09-15	3.7	CVE-2025-59377
itsourcecode--Online Petshop Management System	A vulnerability was identified in itsourcecode Online Petshop Management System 1.0. Impacted is an unknown function of the file addcnp.php of the component Available Products Page. The manipulation of the argument name/description leads to cross site scripting. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	2025-09-18	3.5	CVE-2025-10631
itsourcecode--Online Petshop Management System	A security flaw has been discovered in itsourcecode Online Petshop Management System 1.0. The affected element is an unknown function of the file availableframe.php of the component Admin Dashboard. The manipulation of the argument name/address results in cross site scripting. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited.	2025-09-18	3.5	CVE-2025-10632
Mattermost--Mattermost	Mattermost versions 10.5.x <= 10.5.8, 9.11.x <= 9.11.17 fail to properly validate access controls which allows any authenticated user to download sensitive files via board file download endpoint using UUID enumeration	2025-09-19	3.1	CVE-2025-9081

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Mattermost--Mattermost	Mattermost versions 10.5.x <= 10.5.9 fail to properly validate redirect URLs which allows attackers to redirect users to malicious sites via crafted OAuth login URLs	2025-09-15	3.1	CVE-2025-9084
n/a--Harness	A vulnerability has been found in Harness 3.3.0. Affected is an unknown function of the file /api/v1/login of the component Login Endpoint. The manipulation leads to improper restriction of excessive authentication attempts. Remote exploitation of the attack is possible. The attack is considered to have high complexity. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-21	3.7	CVE-2025-10761
n/a--htmly	A security vulnerability has been detected in htmly up to 3.1.0. The impacted element is an unknown function of the file /htmly/admin/field/post of the component Custom Field Handler. Such manipulation of the argument label leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-21	2.4	CVE-2025-10758
n/a--IbuyuCMS	A vulnerability was identified in IbuyuCMS up to 2.6.3. Impacted is an unknown function of the file /admin/article.php?a=mod of the component Add Article Page. The manipulation of the argument Title leads to cross site scripting. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	2025-09-15	2.4	CVE-2025-10434
n/a--newbee-mall	A vulnerability was found in newbee-mall 1.0. Impacted is the function mallKaptcha of the file /common/mall/kaptcha. The manipulation results in guessable captcha. The attack can be executed remotely. A high complexity level is associated with this attack. The exploitability is considered difficult. The exploit has been made public and could be used.	2025-09-15	3.7	CVE-2025-10423
n/a--Tor	A security flaw has been discovered in Tor up to 0.4.7.16/0.4.8.17. Impacted is an unknown function of the component Onion Service Descriptor Handler. Performing manipulation results in resource consumption. The attack may be initiated remotely. The attack's complexity is rated as high. The exploitability is considered difficult. Upgrading to version 0.4.8.18 and 0.4.9.3-alpha is recommended to address this issue. It is recommended to upgrade the affected component.	2025-09-18	3.7	CVE-2025-4444
nuxt--nuxt	Nuxt is an open-source web development framework for Vue.js. Prior to 3.19.0 and 4.1.0, A client-side path traversal vulnerability in Nuxt's Island payload revival mechanism allowed attackers to manipulate client-side requests to different endpoints within the same application domain when specific prerendering conditions are met. The vulnerability occurs in the client-side payload revival process (revive-payload.client.ts) where Nuxt Islands are automatically fetched when encountering serialized __nuxt_island objects. During prerendering, if an API endpoint returns user-controlled data containing a crafted __nuxt_island object, he data gets serialized with devalue.stringify and stored in the prerendered page. When a client navigates to the prerendered page, devalue.parse deserializes the payload. The Island reviver attempts to fetch /__nuxt_island/${key}.json where key could contain path traversal sequences. Update to Nuxt 3.19.0+ or 4.1.0+.	2025-09-17	3.1	CVE-2025-59414
Portabilis--i-Educar	A vulnerability was identified in Portabilis i-Educar up to 2.10. Impacted is an unknown function of the file /intranet/educar_calendario_anotacao_cad.php. Such manipulation of the argument nm_anotacao/descricao leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	2025-09-17	3.5	CVE-2025-10584
Portabilis--i-Educar	A weakness has been identified in Portabilis i-Educar up to 2.10. This affects an unknown function of the file /intranet/educar_funcao_cad.php of the component Editar Função Page. This manipulation of the argument abreviatura/tipoacao causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	2025-09-17	3.5	CVE-2025-10591

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
PowerDNS--DNSdist	In some circumstances, when DNSdist is configured to use the nghttp2 library to process incoming DNS over HTTPS queries, an attacker might be able to cause a denial of service by crafting a DoH exchange that triggers an unbounded I/O read loop, causing an unexpected consumption of CPU resources.	2025-09-18	3.7	CVE-2025-30187
pspete--psPAS	psPAS PowerShell module does not explicitly enforce TLS 1.2 within the 'Get-PASSAMLResponse' function during the SAML authentication process. An unauthenticated attacker in a 'Man-in-the-Middle' position could manipulate the TLS handshake and downgrade TLS to a deprecated protocol. Fixed in 7.0.209.	2025-09-16	3.1	CVE-2025-59270
PureVPN--PureVPN	PureVPN client applications on Linux through September 2025 allow IPv6 traffic to leak outside the VPN tunnel upon network events such as Wi-Fi reconnect or system resume. In the CLI client, the VPN auto-reconnects and claims to be connected, but IPv6 traffic is no longer routed or blocked. In the GUI client, the IPv6 connection remains functional after disconnection until the user clicks Reconnect. In both cases, the real IPv6 address is exposed to external services, violating user privacy and defeating the advertised IPv6 leak protection. This affects CLI 2.0.1 and GUI 2.10.0.	2025-09-18	3.7	CVE-2025-59691
PureVPN--PureVPN	PureVPN client applications on Linux through September 2025 mishandle firewalling. They flush the system's existing iptables rules and apply default ACCEPT policies when connecting to a VPN server. This removes firewall rules that may have been configured manually or by other software (e.g., UFW, container engines, or system security policies). Upon VPN disconnect, the original firewall state is not restored. As a result, the system may become unintentionally exposed to network traffic that was previously blocked. This affects CLI 2.0.1 and GUI 2.10.0.	2025-09-18	3.7	CVE-2025-59692
wangchenyi1996--chat_forum	A vulnerability has been found in wangchenyi1996 chat_forum up to 80bdb92f5b460d36cab36e530a2c618acef5afd2. This impacts an unknown function of the file /q.php. Such manipulation of the argument path leads to cross site scripting. The attack may be launched remotely. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases.	2025-09-18	3.5	CVE-2025-10642
youth-is-as-pale-as-poetry--e-learning	A vulnerability has been found in youth-is-as-pale-as-poetry e-learning 1.0. Impacted is the function encryptSecret of the file e-learning-master\exam-api\src\main\java\com\yf\exam\ability\shiro\jwt\JwtUtils.java of the component JWT Token Handler. The manipulation leads to insufficiently random values. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitability is considered difficult. The exploit has been disclosed to the public and may be used.	2025-09-18	3.7	CVE-2025-10671
ZTE--T5400	There is an an information disclosure vulnerability in ZTE T5400. Due to improper configuration of the access control mechanism, attackers can obtain information through interfaces without authorization, causing the risk of information disclosure.	2025-09-16	3.5	CVE-2025-26710
Alex--Content Mask	Authorization Bypass Through User-Controlled Key vulnerability in Alex Content Mask allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Content Mask: from n/a through 1.8.5.2.	2025-09-22	3.8	CVE-2025-58012
axboe--fio	A vulnerability was found in axboe fio up to 3.41. This affects the function str_buffer_pattern_cb of the file options.c. Performing manipulation results in null pointer dereference. The attack must be initiated from a local position. The exploit has been made public and could be used.	2025-09-22	3.3	CVE-2025-10823
Changsha Developer Technology--iView Editor	A vulnerability was found in Changsha Developer Technology iView Editor up to 1.1.1. This impacts an unknown function of the component Markdown Handler. The manipulation results in cross site scripting. The attack may be performed from remote. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	2.4	CVE-2025-10949

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects--Project Monitoring System	A vulnerability has been found in code-projects Project Monitoring System 1.0. Affected is an unknown function of the file /onlineJobSearchEngine/postjob.php. Such manipulation of the argument txtapplyto leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	2025-09-28	3.5	CVE-2025-11124
code-projects--Simple Food Ordering System	A security vulnerability has been detected in code-projects Simple Food Ordering System 1.0. Affected by this vulnerability is an unknown functionality of the file /ordersimple/order.php. The manipulation of the argument ID leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	2025-09-23	3.5	CVE-2025-10837
codepeople--CP Multi View Event Calendar	Missing Authorization vulnerability in codepeople CP Multi View Event Calendar allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects CP Multi View Event Calendar : from n/a through 1.4.32.	2025-09-22	3.8	CVE-2025-58009
dnnsoftware--Dnn.Platform	DNN (formerly DotNetNuke) is an open-source web content management platform (CMS) in the Microsoft ecosystem. Prior to version 10.1.0, administrators and content editors can set html in module titles that could include javascript which could be used for XSS based attacks. This issue has been patched in version 10.1.0.	2025-09-23	2.4	CVE-2025-59546
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 18.1 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1 that could have allowed an authenticated user to create a denial-of-service condition by exploiting an unprotected GraphQL API through repeated requests.	2025-09-26	3.5	CVE-2025-10867
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 17.4 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1 where certain string conversion methods exhibit performance degradation with large inputs.	2025-09-26	3.5	CVE-2025-10868
GitLab--GitLab	An issue has been discovered in GitLab EE affecting all versions from 16.6 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1. Project Maintainers can exploit a vulnerability where they can assign custom roles to users with permissions exceeding their own, effectively granting themselves elevated privileges.	2025-09-26	3.8	CVE-2025-10871
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 17.10 before 18.2.7, 18.3 before 18.3.3, and 18.4 before 18.4.1 that could have allowed an authenticated user to gain unauthorized access to confidential issues by creating a project with an identical name to the victim's project.	2025-09-26	3.5	CVE-2025-5069
givanz--Vvveb	A vulnerability was determined in givanz Vvveb up to 1.0.7.2. Affected by this vulnerability is an unknown functionality of the component Configuration File Handler. This manipulation causes information disclosure. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. Once again the project maintainer reacted very professional: "I accept the existence of these vulnerabilities. (...) I fixed the code to remove these vulnerabilities and will push the code to github and make a new release."	2025-09-26	3.5	CVE-2025-11026
givanz--Vvveb	A vulnerability was identified in givanz Vvveb up to 1.0.7.2. Affected by this issue is some unknown functionality of the component SVG File Handler. Such manipulation leads to cross site scripting. The attack may be launched remotely. The exploit is publicly available and might be used. Once again the project maintainer reacted very professional: "I accept the existence of these vulnerabilities. (...) I fixed the code to remove these vulnerabilities and will push the code to github and make a new release."	2025-09-26	2.4	CVE-2025-11027
glib-networking's OpenSSL backend --N/A	glib-networking's OpenSSL backend fails to properly check the return value of memory allocation routines. An out of memory condition could potentially result in writing to an invalid memory location.	2025-09-25	3.7	CVE-2025-60019
GNU--Binutils	A vulnerability was detected in GNU Binutils 2.45. This issue affects the function dump_dwarf_section of the file binutils/objdump.c. Performing manipulation	2025-09-27	3.3	CVE-2025-11081

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	results in out-of-bounds read. The attack is only possible with local access. The exploit is now public and may be used. The patch is named f87a66db645caf8cc0e6fc87b0c28c78a38af59b. It is suggested to install a patch to address this issue.			
IBM--Cognos Controller	IBM Cognos Controller 11.0.0 through 11.0.1, and IBM Controller 11.1.0 through 11.1.1 could allow an attacker to obtain sensitive information due to the use of hardcoded cryptographic keys for signing session cookies.	2025-09-26	3.7	CVE-2025-36326
IBM--watsonx.data	IBM Lakehouse (watsonx.data 2.2) stores potentially sensitive information in log files that could be read by a local user.	2025-09-27	3.3	CVE-2025-36144
LionCoders--SalePro POS	A vulnerability was detected in LionCoders SalePro POS up to 5.5.0. This issue affects some unknown processing of the component Login. Performing manipulation results in cleartext transmission of sensitive information. The attack can be initiated remotely. The attack is considered to have high complexity. The exploitability is assessed as difficult. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-22	3.7	CVE-2025-10776
Mangati--NovoSGA	A security flaw has been discovered in Mangati NovoSGA up to 2.2.9. The impacted element is an unknown function of the file /admin of the component SVG File Handler. Performing manipulation of the argument logoNavbar/logoLogin results in cross site scripting. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-24	2.4	CVE-2025-10909
MikeCen--WeChat-Face-Recognition	A security flaw has been discovered in MikeCen WeChat-Face-Recognition up to 6e3f72bf8547d80b59e330f1137e4aa505f492c1. This vulnerability affects the function valid of the file wx.php. The manipulation of the argument echostr results in cross site scripting. The attack can be launched remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	3.5	CVE-2025-10943
n/a--BehaviorTree	A vulnerability was found in BehaviorTree up to 4.7.0. Affected by this issue is the function JsonExporter::fromJson of the file /src/json_export.cpp. Performing manipulation of the argument Source results in null pointer dereference. The attack needs to be approached locally. The exploit has been made public and could be used. The patch is named 4b23dcaf0ce951a31299ebdd61df69f9ce99a76d. It is suggested to install a patch to address this issue.	2025-09-26	3.3	CVE-2025-11011
n/a--BehaviorTree	A vulnerability was identified in BehaviorTree up to 4.7.0. This vulnerability affects the function XMLParser::PImpl::loadDocImpl of the file /src/xml_parsing.cpp of the component XML Parser. The manipulation leads to null pointer dereference. The attack can only be performed from a local environment. The exploit is publicly available and might be used.	2025-09-26	3.3	CVE-2025-11013
n/a--Coinomi	A vulnerability has been found in Coinomi up to 1.7.6. This issue affects some unknown processing. Such manipulation leads to cleartext transmission of sensitive information. The attack can be launched remotely. This attack is characterized by high complexity. The exploitability is assessed as difficult. The exploit has been disclosed to the public and may be used. The vendor replied with: "(...) there isn't any security implication associated with your findings."	2025-09-23	3.7	CVE-2017-20200
n/a--JeecgBoot	A vulnerability was determined in JeecgBoot up to 3.8.2. This issue affects some unknown processing of the file /api/getDepartUserList. Executing manipulation of the argument departId can lead to improper authorization. The attack can be executed remotely. This attack is characterized by high complexity. The exploitability is assessed as difficult. The exploit has been publicly disclosed and	2025-09-25	3.1	CVE-2025-10976

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.			
n/a--JeecgBoot	A vulnerability was identified in JeecgBoot up to 3.8.2. Impacted is an unknown function of the file /sys/tenant/deleteBatch. The manipulation of the argument ids leads to improper authorization. The attack is possible to be carried out remotely. The complexity of an attack is rather high. The exploitability is considered difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	3.1	CVE-2025-10977
n/a--Open Babel	A vulnerability has been found in Open Babel up to 3.1.1. The affected element is the function ChemKinFormat::ReadReactionQualifierLines of the file /src/formats/chemkinformat.cpp. The manipulation leads to null pointer dereference. The attack can only be performed from a local environment. The exploit has been disclosed to the public and may be used.	2025-09-26	3.3	CVE-2025-10998
n/a--Open Babel	A vulnerability was found in Open Babel up to 3.1.1. The impacted element is the function CacaoFormat::SetHilderbrandt of the file /src/formats/cacaoformat.cpp. The manipulation results in null pointer dereference. The attack is only possible with local access. The exploit has been made public and could be used.	2025-09-26	3.3	CVE-2025-10999
n/a--Open Babel	A vulnerability was determined in Open Babel up to 3.1.1. This affects the function PQSFormat::ReadMolecule of the file /src/formats/PQSformat.cpp. This manipulation causes null pointer dereference. The attack is restricted to local execution. The exploit has been publicly disclosed and may be utilized.	2025-09-26	3.3	CVE-2025-11000
n/a--Smartstore	A vulnerability has been found in Smartstore up to 6.2.0. The affected element is an unknown function of the file /checkout/confirm/ of the component Gift Voucher Handler. The manipulation leads to race condition. The attack may be initiated remotely. The attack's complexity is rated as high. The exploitability is described as difficult. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-22	3.1	CVE-2025-10778
nuz007--smsboom	A security vulnerability has been detected in nuz007 smsboom up to 01b2f35bbbc23f3e0f60f38ca0e3d1b286f8d674. Impacted is an unknown function of the file d.php. Such manipulation of the argument hm leads to cross site scripting. The attack may be launched remotely. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases.	2025-09-25	3.5	CVE-2025-10945
nuz007--smsboom	A vulnerability was detected in nuz007 smsboom up to 01b2f35bbbc23f3e0f60f38ca0e3d1b286f8d674. The affected element is an unknown function of the file dy.php. Performing manipulation of the argument hm results in cross site scripting. Remote exploitation of the attack is possible. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided.	2025-09-25	3.5	CVE-2025-10946
NVIDIA--NVIDIA CUDA Toolkit	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in the nvdisasm binary where a user may cause an out-of-bounds read by passing a malformed ELF file to nvdisasm. A successful exploit of this vulnerability may lead to a partial denial of service.	2025-09-24	3.3	CVE-2025-23248
NVIDIA--NVIDIA CUDA Toolkit	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in the cuobjdump binary where a user may cause an out-of-bounds read by passing a malformed ELF file to cuobjdump. A successful exploit of this vulnerability may lead to a partial denial of service.	2025-09-24	3.3	CVE-2025-23255
NVIDIA--NVIDIA CUDA Toolkit	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in the nvdisasm binary where a user may cause an out-of-bounds read by passing a malformed ELF file to nvdisasm. A successful exploit of this vulnerability may lead to a partial denial of service.	2025-09-24	3.3	CVE-2025-23271

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
NVIDIA--NVIDIA CUDA Toolkit	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in nvdisasm where an attacker may cause a heap-based buffer overflow by getting the user to run nvdisasm on a malicious ELF file. A successful exploit of this vulnerability may lead to arbitrary code execution at the privilege level of the user running nvdisasm.	2025-09-24	3.3	CVE-2025-23308
NVIDIA--NVIDIA CUDA Toolkit	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in nvdisasm where a user may cause an out-of-bounds write by running nvdisasm on a malicious ELF file. A successful exploit of this vulnerability may lead to denial of service.	2025-09-24	3.3	CVE-2025-23338
NVIDIA--NVIDIA CUDA Toolkit	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in cuobjdump where an attacker may cause a stack-based buffer overflow by getting the user to run cuobjdump on a malicious ELF file. A successful exploit of this vulnerability may lead to arbitrary code execution at the privilege level of the user running cuobjdump.	2025-09-24	3.3	CVE-2025-23339
NVIDIA--NVIDIA CUDA Toolkit	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in the nvdisasm binary where a user may cause an out-of-bounds read by passing a malformed ELF file to nvdisasm. A successful exploit of this vulnerability may lead to a partial denial of service.	2025-09-24	3.3	CVE-2025-23340
NVIDIA--NVIDIA CUDA Toolkit	NVIDIA CUDA Toolkit contains a vulnerability in cuobjdump, where an unprivileged user can cause a NULL pointer dereference. A successful exploit of this vulnerability may lead to a limited denial of service.	2025-09-24	3.3	CVE-2025-23346
NVIDIA--NVIDIA CUDA Toolkit	NVIDIA CUDA Toolkit for all platforms contains a vulnerability in nvJPEG where a local authenticated user may cause a divide by zero error by submitting a specially crafted JPEG file. A successful exploit of this vulnerability may lead to denial of service.	2025-09-24	2.5	CVE-2025-23273
OGRECave--Ogre	A vulnerability was detected in OGRECave Ogre up to 14.4.1. The impacted element is the function Ogre::LogManager::stream of the file /ogre/OgreMain/src/OgreLogManager.cpp. Performing manipulation of the argument mDefaultLog results in null pointer dereference. The attack must be initiated from a local position. The exploit is now public and may be used.	2025-09-26	3.3	CVE-2025-11017
Projectworlds--Visitor Management System	A vulnerability has been found in Projectworlds Visitor Management System 1.0. Affected is an unknown function of the file /myform.php of the component Add Visitor Page. The manipulation of the argument Name leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	2025-09-27	2.4	CVE-2025-11067
Rapid7--Appspider Pro	Rapid7 Appspider Pro versions below 7.5.021, suffer from a broken access control vulnerability in the application's configuration file loading mechanism, whereby an attacker can place files in directories belonging to other users or projects. Affected versions allow standard users to add custom configuration files. These files, which are loaded in alphabetical order, can override or change the settings of the original configuration files, creating a security vulnerability. This issue stems from improper directory access management. This vulnerability was remediated in version 7.5.021 of the product.	2025-09-25	3.3	CVE-2025-36857
roxnor--ShopEngine Elementor WooCommerce Builder Addon All in One WooCommerce Solution	The ShopEngine Elementor WooCommerce Builder Addon - All in One WooCommerce Solution plugin for WordPress is vulnerable to unauthorized access due to an incorrect capability check on the post_save() function in all versions up to, and including, 4.8.3. This makes it possible for authenticated attackers, with Editor-level access and above, to update the plugin's settings.	2025-09-26	2.7	CVE-2025-10173
Total.js--CMS	A vulnerability was found in Total.js CMS 1.0.0. Affected by this vulnerability is the function layouts_save of the file /admin/ of the component Layout Page. Performing manipulation of the argument HTML results in cross site scripting. It is	2025-09-25	2.4	CVE-2025-10940

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	possible to initiate the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.			
Total.js--CMS	A vulnerability has been found in Total.js CMS up to 19.9.0. This impacts an unknown function of the component Files Menu. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-09-26	2.4	CVE-2025-11019
westboy--CicadasCMS	A vulnerability was found in westboy CicadasCMS 1.0. Affected by this vulnerability is an unknown functionality of the file /system/cms/category/save. The manipulation of the argument categoryName results in cross site scripting. The attack can be executed remotely. The exploit has been made public and could be used.	2025-09-27	2.4	CVE-2025-11068
westboy--CicadasCMS	A vulnerability was determined in westboy CicadasCMS 1.0. Affected by this issue is some unknown functionality of the file /system/org/save of the component Add Department Handler. This manipulation of the argument Name causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	2025-09-27	2.4	CVE-2025-11069
WSO2--WSO2 Identity Server	A username enumeration vulnerability exists in multiple WSO2 products when Multi-Attribute Login is enabled. In this configuration, the system returns a distinct "User does not exist" error message to the login form, regardless of the validate_username setting. This behavior allows malicious actors to determine which usernames exist in the system based on observable discrepancies in the application's responses. Exploitation of this vulnerability could aid in brute-force attacks, targeted phishing campaigns, or other social engineering techniques by confirming the validity of user identifiers within the system.	2025-09-26	3.7	CVE-2025-1396
WSO2--WSO2 Identity Server as Key Manager	An authentication bypass vulnerability exists in multiple WSO2 products when FIDO authentication is enabled. When a user account is deleted, the system does not automatically remove associated FIDO registration data. If a new user account is later created using the same username, the system may associate the new account with the previously registered FIDO device. This flaw may allow a previously deleted user to authenticate using their FIDO credentials and impersonate the newly created user, resulting in unauthorized access. The vulnerability applies only to deployments that utilize FIDO-based authentication.	2025-09-23	3.3	CVE-2025-0672
yi-ge--get-header-ip	A weakness has been identified in yi-ge get-header-ip up to 589b23d0eb0043c310a6a13ce4bbe2505d0d0b15. This issue affects the function ip of the file ip.php. This manipulation of the argument callback causes cross site scripting. The attack may be initiated remotely. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-25	3.5	CVE-2025-10944
Zohocorp--Endpoint Central	ZohoCorp ManageEngine Endpoint Central was impacted by an improper privilege management issue in the agent setup. This issue affects Endpoint Central: through 11.4.2500.25, through 11.4.2508.13.	2025-09-25	3.9	CVE-2025-5494