BULLETIN (SB24-092)

VULNERABILITY SUMMARY FOR THE MONTH OF

MARCH 2024

Bulletin (SB24-092)
Vulnerability Summary for the Month of March 2024

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
acowebs -- pdf_invoices_and_packing_slips_for_woocommerce	Deserialization of Untrusted Data vulnerability in Acowebs PDF Invoices and Packing Slips For WooCommerce.This issue affects PDF Invoices and Packing Slips For WooCommerce: from n/a through 1.3.7.	2024-03-28	8.2	CVE-2024-30230
active_websight -- seo_backlink_monitor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Active Websight SEO Backlink Monitor allows Reflected XSS.This issue affects SEO Backlink Monitor: from n/a through 1.5.0.	2024-03-27	7.1	CVE-2024-29907
adtribes.io -- product_feed_pro_for_woocommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AdTribes.Io Product Feed PRO for WooCommerce allows Reflected XSS.This issue affects Product Feed PRO for WooCommerce: from n/a through 13.2.5.	2024-03-27	7.1	CVE-2024-24800
andy_moyle -- church_admin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Andy Moyle Church Admin.This issue affects Church Admin: from n/a through 4.0.27.	2024-03-28	8.5	CVE-2024-30244
ansys -- pyansys-geometry	PyAnsys Geometry is a Python client library for the Ansys Geometry service and other CAD Ansys products. On file src/ansys/geometry/core/connection/product_instance.py, upon calling this method _start_program directly, users could exploit its usage to perform malicious operations on the current machine where the script is ran. This vulnerability is fixed in 0.3.3 and 0.4.12.	2024-03-26	7.4	CVE-2024-29189
apache_software_foundation -- apache_fineract	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Fineract.This issue affects Apache Fineract: <1.8.5. Users are recommended to upgrade to version 1.8.5 or 1.9.0, which fix the issue.	2024-03-29	9.9	CVE-2024-23538
apache_software_foundation -- apache_fineract	Improper Privilege Management vulnerability in Apache Fineract.This issue affects Apache Fineract: <1.8.5. Users are recommended to upgrade to version 1.9.0, which fixes the issue.	2024-03-29	8.4	CVE-2024-23537
apache_software_foundation -- apache_fineract	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Fineract.This issue affects Apache Fineract: <1.8.5. Users are recommended to upgrade to version 1.8.5 or 1.9.0, which fix the issue.	2024-03-29	8.3	CVE-2024-23539
appscreo -- easy_social_share_buttons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Appscreo Easy Social Share Buttons allows Reflected XSS.This issue affects Easy Social Share Buttons: from n/a through 9.4.	2024-03-27	7.1	CVE-2024-30196
archetyped -- cornerstone	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Archetyped Cornerstone allows Reflected XSS.This issue affects Cornerstone: from n/a through 0.8.0.	2024-03-28	7.1	CVE-2024-28002
archetyped -- favicon_rotator	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Archetyped Favicon Rotator allows Reflected XSS.This issue affects Favicon Rotator: from n/a through 1.2.10.	2024-03-28	7.1	CVE-2024-28001
artbees -- jupiterx_core	Unrestricted Upload of File with Dangerous Type vulnerability in Artbees JupiterX Core.This issue affects JupiterX Core: from n/a through 3.3.5.	2024-03-26	9	CVE-2023-38388
automationdirect -- c-more_ea9_hmi_ea9-t6cl	There is a function in AutomationDirect C-MORE EA9 HMI that allows an attacker to send a relative path in the URL without proper sanitizing of the content.	2024-03-26	7.5	CVE-2024-25136
bdthemes -- element_pack_elementor_addons	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BdThemes Element Pack Elementor Addons.This issue affects Element Pack Elementor Addons: from n/a through 5.5.3.	2024-03-29	8.5	CVE-2024-30496
benjamin_rojas -- wp_editor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Benjamin Rojas WP Editor allows Reflected XSS.This issue affects WP Editor: from n/a through 1.2.8.	2024-03-27	7.1	CVE-2024-24700
bestwebsoft -- limit_attempts_by_bestwebsoft	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BestWebSoft Limit Attempts by BestWebSoft allows Reflected XSS.This issue affects Limit Attempts by BestWebSoft: from n/a through 1.2.9.	2024-03-29	7.1	CVE-2024-30439

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bizswoop_a_cpf_concepts,_llc_brand -- bizprint	Cross-Site Request Forgery (CSRF) vulnerability in BizSwoop a CPF Concepts, LLC Brand BizPrint allows Cross-Site Scripting (XSS).This issue affects BizPrint: from n/a through 4.5.5.	2024-03-27	7.1	CVE-2024-29773
booking_activities_team -- booking_activities	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Booking Activities Team Booking Activities allows Reflected XSS.This issue affects Booking Activities: from n/a through 1.15.19.	2024-03-29	7.1	CVE-2024-30449
bosch -- network_synchronizer_enterprise	Command Injection in the diagnostics interface of the Bosch Network Synchronizer allows unauthorized users full access to the device.	2024-03-25	8.8	CVE-2024-25002 psirt@bosch.com
brainstorm_force -- spectra	Server-Side Request Forgery (SSRF) vulnerability in Brainstorm Force Spectra.This issue affects Spectra: from n/a through 2.6.6.	2024-03-28	7.1	CVE-2023-36679
brainstorm_force -- starter_templates_-_elementor_wordpress_&_beaver_builder_templates	Server-Side Request Forgery (SSRF) vulnerability in Brainstorm Force Starter Templates - Elementor, WordPress & Beaver Builder Templates, Brainstorm Force Premium Starter Templates.This issue affects Starter Templates - Elementor, WordPress & Beaver Builder Templates: from n/a through 3.2.4; Premium Starter Templates: from n/a through 3.2.4.	2024-03-28	7.1	CVE-2023-34370
bulletin -- wordpress_announcement_&_notification_banner_plugin_-_bulletin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Bulletin WordPress Announcement & Notification Banner Plugin - Bulletin.This issue affects WordPress Announcement & Notification Banner Plugin - Bulletin: from n/a through 3.8.5.	2024-03-29	7.6	CVE-2024-30478
campcodes-house-rental-management-system	A vulnerability was found in Campcodes House Rental Management System 1.0. It has been classified as critical. Affected is an unknown function of the file ajax.php. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257982 is the identifier assigned to this vulnerability.	2024-03-26	7.3	CVE-2024-2916
castos -- seriously_simple_podcasting	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Castos Seriously Simple Podcasting allows Reflected XSS.This issue affects Seriously Simple Podcasting: from n/a through 3.0.2.	2024-03-28	7.1	CVE-2024-25599
checkemail -- check_&_log_email	The Check & Log Email plugin for WordPress is vulnerable to Unauthenticated Hook Injection in all versions up to, and including, 1.0.9 via the check_nonce function. This makes it possible for unauthenticated attackers to execute actions with hooks in WordPress under certain circumstances. The action the attacker wishes to execute needs to have a nonce check, and the nonce needs to be known to the attacker. Furthermore, the absence of a capability check is a requirement.	2024-03-26	8.1	CVE-2024-0866
cilium -- cilium	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Users of IPsec transparent encryption in Cilium may be vulnerable to cryptographic attacks that render the transparent encryption ineffective. In particular, Cilium is vulnerable to chosen plaintext, key recovery, replay attacks by a man-in-the-middle attacker. These attacks are possible due to an ESP sequence number collision when multiple nodes are configured with the same key. Fixed versions of Cilium use unique keys for each IPsec tunnel established between nodes, resolving all of the above attacks. This vulnerability is fixed in 1.13.13, 1.14.9, and 1.15.3.	2024-03-27	8	CVE-2024-28860
cisco -- cisco_aironet_access_point_software	A vulnerability in the IP packet processing of Cisco Access Point (AP) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of certain IPv4 packets. An attacker could exploit this vulnerability by sending a crafted IPv4 packet either to or through an affected device. A successful exploit could allow the attacker to cause an affected device to reload unexpectedly, resulting in a DoS condition. To successfully exploit this vulnerability, the attacker does not need to be associated with the affected AP. This vulnerability cannot be exploited by sending IPv6 packets.	2024-03-27	8.6	CVE-2024-20271

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- cisco_ios_xe_software	A vulnerability in the DHCP snooping feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to a crafted IPv4 DHCP request packet being mishandled when endpoint analytics are enabled. An attacker could exploit this vulnerability by sending a crafted DHCP request through an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: The attack vector is listed as network because a DHCP relay anywhere on the network could allow exploits from networks other than the adjacent one.	2024-03-27	8.6	CVE-2024-20259
cisco -- cisco_ios_xe_software	A vulnerability in the IPv4 Software-Defined Access (SD-Access) fabric edge node feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause high CPU utilization and stop all traffic processing, resulting in a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of certain IPv4 packets. An attacker could exploit this vulnerability by sending certain IPv4 packets to an affected device. A successful exploit could allow the attacker to cause the device to exhaust CPU resources and stop processing traffic, resulting in a DoS condition.	2024-03-27	8.6	CVE-2024-20314
cisco -- cisco_ios_xe_software	A vulnerability in the multicast DNS (mDNS) gateway feature of Cisco IOS XE Software for Wireless LAN Controllers (WLCs) could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper management of mDNS client entries. An attacker could exploit this vulnerability by connecting to the wireless network and sending a continuous stream of specific mDNS packets. A successful exploit could allow the attacker to cause the wireless controller to have high CPU utilization, which could lead to access points (APs) losing their connection to the controller and result in a DoS condition.	2024-03-27	7.4	CVE-2024-20303
cisco -- ios	A vulnerability in the IKEv1 fragmentation code of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a heap underflow, resulting in an affected device reloading. This vulnerability exists because crafted, fragmented IKEv1 packets are not properly reassembled. An attacker could exploit this vulnerability by sending crafted UDP packets to an affected system. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. Note: Only traffic that is directed to the affected system can be used to exploit this vulnerability. This vulnerability can be triggered by IPv4 and IPv6 traffic..	2024-03-27	8.6	CVE-2024-20308
cisco -- ios	A vulnerability in the Locator ID Separation Protocol (LISP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. This vulnerability is due to the incorrect handling of LISP packets. An attacker could exploit this vulnerability by sending a crafted LISP packet to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition. Note: This vulnerability could be exploited over either IPv4 or IPv6 transport.	2024-03-27	8.6	CVE-2024-20311
cisco -- ios	A vulnerability in Cisco IOS Software for Cisco Catalyst 6000 Series Switches could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly. This vulnerability is due to improper handling of process-switched traffic. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition.	2024-03-27	7.4	CVE-2024-20276
cisco -- ios	A vulnerability in the Intermediate System-to-Intermediate System (IS-IS) protocol of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation when parsing an ingress IS-IS packet. An attacker could exploit this vulnerability by sending a crafted IS-IS packet to an affected device after forming an adjacency. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. Note: The IS-IS protocol is a routing protocol. To exploit this vulnerability, an attacker must be Layer 2-adjacent to the affected device and have formed an adjacency.	2024-03-27	7.4	CVE-2024-20312
code-projects -- mobile_shop	A vulnerability was found in code-projects Mobile Shop 1.0. It has been classified as critical. Affected is an unknown function of the file Details.php of the component Login Page. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258000.	2024-03-26	7.3	CVE-2024-2927

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects -- online_book_system	A vulnerability classified as critical was found in code-projects Online Book System 1.0. This vulnerability affects unknown code of the file /index.php. The manipulation of the argument username/password/login_username/login_password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-258202 is the identifier assigned to this vulnerability.	2024-03-27	7.3	CVE-2024-3000
codeigniter4 -- codeigniter4	CodeIgniter is a PHP full-stack web framework A vulnerability was found in the Language class that allowed DoS attacks. This vulnerability can be exploited by an attacker to consume a large amount of memory on the server. Upgrade to v4.4.7 or later.	2024-03-29	7.5	CVE-2024-29904
codepeople -- calculated_fields_form	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodePeople Calculated Fields Form allows Reflected XSS.This issue affects Calculated Fields Form: from n/a through 1.2.54.	2024-03-27	7.1	CVE-2024-29759
contact_form_with_captcha -- contact_form_with_captcha	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Contact Form With Captcha allows Reflected XSS.This issue affects Contact Form With Captcha: from n/a through 1.6.8.	2024-03-26	7.1	CVE-2023-45771
contest_gallery -- contest_gallery	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Contest Gallery.This issue affects Contest Gallery: from n/a through 21.3.4.	2024-03-28	8.5	CVE-2024-30236
contest_gallery -- contest_gallery	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Contest Gallery.This issue affects Contest Gallery: from n/a through 21.3.2.	2024-03-27	8.5	CVE-2024-30238
contest_gallery -- contest_gallery	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Contest Gallery allows Reflected XSS.This issue affects Contest Gallery: from n/a through 21.3.5.	2024-03-29	7.1	CVE-2024-30428
conversios -- conversios.io	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Conversios Conversios.Io allows Reflected XSS.This issue affects Conversios.Io: from n/a through 6.9.1.	2024-03-27	7.1	CVE-2024-29794
creative_solutions -- creative_image_slider_-_responsive_slider_plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Creative Solutions Creative Image Slider - Responsive Slider Plugin allows Reflected XSS.This issue affects Creative Image Slider - Responsive Slider Plugin: from n/a through 2.1.3.	2024-03-29	7.1	CVE-2024-30447
crm_perks -- crm_perks_forms	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CRM Perks CRM Perks Forms.This issue affects CRM Perks Forms: from n/a through 1.1.4.	2024-03-29	9.3	CVE-2024-30498
crm_perks -- crm_perks_forms	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CRM Perks CRM Perks Forms.This issue affects CRM Perks Forms: from n/a through 1.1.4.	2024-03-29	8.5	CVE-2024-30499
cubewp -- cubewp_-_all-in-one_dynamic_content_framework	Unrestricted Upload of File with Dangerous Type vulnerability in CubeWP CubeWP - All-in-One Dynamic Content Framework.This issue affects CubeWP - All-in-One Dynamic Content Framework: from n/a through 1.1.12.	2024-03-29	9.9	CVE-2024-30500
cyberchimps -- responsive	The Responsive theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_footer_text_callback function in all versions up to, and including, 5.0.2. This makes it possible for unauthenticated attackers to inject arbitrary HTML content into the site's footer.	2024-03-29	7.5	CVE-2024-2848
datalens-tech -- datalens	DataLens is a business intelligence and data visualization system. A specifically crafted request allowed the creation of a special chart type with the ability to pass custom javascript code that would later be executed in an unprotected sandbox on subsequent requests to that chart. The problem was fixed in the datalens-ui version `0.1449.0`. Restricting access to the API for creating or modifying charts (`/charts/api/charts/v1/`) would mitigate the issue.	2024-03-29	8.8	CVE-2024-29890
decalog -- decalog	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in DecaLog.This issue affects DecaLog: from n/a through 3.9.0.	2024-03-28	7.6	CVE-2024-30245
dell -- insightiq	Dell InsightIQ, version 5.0, contains an improper access control vulnerability. A remote low privileged attacker could potentially exploit this vulnerability, leading to unauthorized access to monitoring data.	2024-03-27	8.3	CVE-2024-25962

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- powerscale_onefs	Dell PowerScale OneFS versions 9.4.0.x through 9.7.0.x contains an insertion of sensitive information into log file vulnerability. A low privileged local attacker could potentially exploit this vulnerability, leading to sensitive information disclosure, escalation of privileges.	2024-03-28	7.9	CVE-2024-25959
dell -- powerscale_onefs	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.x contains a cleartext transmission of sensitive information vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to escalation of privileges.	2024-03-28	7.3	CVE-2024-25960
dell -- virtual_appliance_(vapp)_manager	Dell vApp Manager, versions prior to 9.2.4.9 contain a Command Injection Vulnerability. An authorized attacker could potentially exploit this vulnerability leading to an execution of an inserted command. Dell recommends customers to upgrade at the earliest opportunity.	2024-03-28	7.2	CVE-2024-25946
dell -- virtual_appliance_(vapp)_manager	Dell vApp Manager, versions prior to 9.2.4.9 contain a Command Injection Vulnerability. An authorized attacker could potentially exploit this vulnerability leading to an execution of an inserted command. Dell recommends customers to upgrade at the earliest opportunity.	2024-03-28	7.2	CVE-2024-25955
digamber_pradhan -- preview_e-mails_for_woocommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Digamber Pradhan Preview E-mails for WooCommerce allows Reflected XSS.This issue affects Preview E-mails for WooCommerce: from n/a through 2.2.1.	2024-03-28	7.1	CVE-2024-27999
echo_plugins -- knowledge_base_for_documentation_faqs_with_ai_assistance	Deserialization of Untrusted Data vulnerability in Echo Plugins Knowledge Base for Documentation, FAQs with AI Assistance.This issue affects Knowledge Base for Documentation, FAQs with AI Assistance: from n/a through 11.30.2.	2024-03-27	8.7	CVE-2024-24842
eclipse_foundation -- threadx	In Eclipse ThreadX before 6.4.0, xQueueCreate() and xQueueCreateSet() functions from the FreeRTOS compatibility API (utility/rtos_compatibility_layers/FreeRTOS/tx_freertos.c) were missing parameter checks. This could lead to integer wraparound, under-allocations and heap buffer overflows.	2024-03-26	7.3	CVE-2024-2212
eclipse_foundation -- threadx	In Eclipse ThreadX before version 6.4.0, the _Mtxinit() function in the Xtensa port was missing an array size check causing a memory overwrite. The affected file was ports/xtensa/xcc/src/tx_clib_lock.c	2024-03-26	7	CVE-2024-2214
eclipse_foundation -- threadx	In Eclipse ThreadX NetX Duo before 6.4.0, if an attacker can control parameters of __portable_aligned_alloc() could cause an integer wrap-around and an allocation smaller than expected. This could cause subsequent heap buffer overflows.	2024-03-26	7	CVE-2024-2452
egehan_security -- webpdks	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Egehan Security WebPDKS allows SQL Injection.This issue affects WebPDKS: through 20240329. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-29	9.8	CVE-2023-6191
electron -- packager	Electron Packager bundles Electron-based application source code with a renamed Electron executable and supporting files into folders ready for distribution. A random segment of ~1-10kb of Node.js heap memory allocated either side of a known buffer will be leaked into the final executable. This memory _could_ contain sensitive information such as environment variables, secrets files, etc. This issue is patched in 18.3.1.	2024-03-29	7.5	CVE-2024-29900
elementor.com -- elementor_website_builder	Unrestricted Upload of File with Dangerous Type vulnerability in Elementor.Com Elementor Website Builder.This issue affects Elementor Website Builder: from 3.3.0 through 3.18.1.	2024-03-26	9.9	CVE-2023-48777
etoile_web_design -- front_end_users	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Etoile Web Design Front End Users allows Reflected XSS.This issue affects Front End Users: from n/a before 3.2.25.	2024-03-26	7.1	CVE-2023-33322
everpress -- mailster	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in EverPress Mailster allows Reflected XSS.This issue affects Mailster: from n/a through 4.0.6.	2024-03-29	7.1	CVE-2024-30503
expresstech -- quiz_and_survey_master	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ExpressTech Quiz And Survey Master.This issue affects Quiz And Survey Master: from n/a through 8.1.4.	2024-03-26	9.3	CVE-2023-28787
faboba -- falang_multilanguage	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Faboba Falang multilanguage.This issue affects Falang multilanguage: from n/a through 1.3.47.	2024-03-29	7.6	CVE-2024-30495

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foliovision:_making_the_web_work_for_you -- fv_flowplayer_video_player	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Foliovision: Making the web work for you FV Flowplayer Video Player allows Reflected XSS.This issue affects FV Flowplayer Video Player: from n/a through 7.5.41.7212.	2024-03-27	7.1	CVE-2024-22299
forgerock -- access_management	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ForgeRock Access Management allows Authorization Bypass. This issue affects access management: before 7.3.0, before 7.2.1, before 7.1.4, through 7.0.2.	2024-03-27	8.1	CVE-2023-0582
fortra -- robot_schedule_enterprise_agent	Fortra's Robot Schedule Enterprise Agent for Windows prior to version 3.04 is susceptible to privilege escalation. A low-privileged user can overwrite the service executable. When the service is restarted, the replaced binary runs with local system privileges, allowing a low-privileged user to gain elevated privileges.	2024-03-28	7.3	CVE-2024-0259
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions before 16.8.5, all versions starting from 16.9 before 16.9.3, all versions starting from 16.10 before 16.10.1. A wiki page with a crafted payload may lead to a Stored XSS, allowing attackers to perform arbitrary actions on behalf of victims.	2024-03-28	8.7	CVE-2023-6371
givewp -- givewp	Deserialization of Untrusted Data vulnerability in GiveWP.This issue affects GiveWP: from n/a through 3.4.2.	2024-03-28	8	CVE-2024-30229
gsheetconnector -- cf7_google_sheets_connector	Insertion of Sensitive Information into Log File vulnerability in GSheetConnector CF7 Google Sheets Connector.This issue affects CF7 Google Sheets Connector: from n/a through 5.0.5.	2024-03-26	7.5	CVE-2023-44989
hercules_design -- hercules_core_	Deserialization of Untrusted Data vulnerability in Hercules Design Hercules Core.This issue affects Hercules Core : from n/a through 6.4.	2024-03-28	9.9	CVE-2024-30228
hitachi -- hitachi_virtual_storage_platform	Insertion of Sensitive Information into Log File vulnerability in Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500, Hitachi Virtual Storage Platform G1000, G1500, Hitachi Virtual Storage Platform F1500, Hitachi Virtual Storage Platform 5100, 5500, 5100H, 5500H, Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H, Hitachi Unified Storage VM, Hitachi Virtual Storage Platform G100, G200, G400, G600, G800, Hitachi Virtual Storage Platform F400, F600, F800, Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900, Hitachi Virtual Storage Platform F350, F370, F700, F900, Hitachi Virtual Storage Platform E390, E590, E790, E990, E1090, E390H, E590H, E790H, E1090H allows local users to gain sensitive information.This issue affects Hitachi Virtual Storage Platform: before DKCMAIN Ver. 70-06-74-00/00, SVP Ver. 70-06-58/00; Hitachi Virtual Storage Platform VP9500: before DKCMAIN Ver. 70-06-74-00/00, SVP Ver. 70-06-58/00; Hitachi Virtual Storage Platform G1000, G1500: before DKCMAIN Ver. 80-06-92-00/00, SVP Ver. 80-06-87/00; Hitachi Virtual Storage Platform F1500: before DKCMAIN Ver. 80-06-92-00/00, SVP Ver. 80-06-87/00; Hitachi Virtual Storage Platform 5100, 5500,5100H, 5500H: before DKCMAIN Ver. 90-08-81-00/00, SVP Ver. 90-08-81/00, before DKCMAIN Ver. 90-08-62-00/00, SVP Ver. 90-08-62/00, before DKCMAIN Ver. 90-08-43-00/00, SVP Ver. 90-08-43/00; Hitachi Virtual Storage Platform 5200, 5600,5200H, 5600H: before DKCMAIN Ver. 90-08-81-00/00, SVP Ver. 90-08-81/00, before DKCMAIN Ver. 90-08-62-00/00, SVP Ver. 90-08-62/00, before DKCMAIN Ver. 90-08-43-00/00, SVP Ver. 90-08-43/00; Hitachi Unified Storage VM: before DKCMAIN Ver. 73-03-75-X0/00, SVP Ver. 73-03-74/00, before DKCMAIN Ver. 73(75)-03-75-X0/00, SVP Ver. 73(75)-03-74/00; Hitachi Virtual Storage Platform G100, G200, G400, G600, G800: before DKCMAIN Ver. 83-06-19-X0/00, SVP Ver. 83-06-20-X0/00, before DKCMAIN Ver. 83-05-47-X0/00, SVP Ver. 83-05-51-X0/00; Hitachi Virtual Storage Platform F400, F600, F800: before DKCMAIN Ver. 83-06-19-X0/00, SVP Ver. 83-06-20-X0/00, before DKCMAIN Ver. 83-05-47-X0/00, SVP Ver. 83-05-51-X0/00; Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900: before DKCMAIN Ver. 88-08-09-XX/00, SVP Ver. 88-08-11-X0/02; Hitachi Virtual Storage Platform F350, F370, F700, F900: before DKCMAIN Ver. 88-08-09-XX/00, SVP Ver. 88-08-11-X0/02; Hitachi Virtual Storage Platform E390, E590, E790, E990, E1090, E390H, E590H, E790H, E1090H: before DKCMAIN Ver. 93-06-81-X0/00, SVP Ver. 93-06-81-X0/00, before DKCMAIN Ver. 93-06-62-X0/00, SVP Ver. 93-06-62-X0/00, before DKCMAIN Ver. 93-06-43-X0/00, SVP Ver. 93-06-43-X0/00.	2024-03-25	9.9	CVE-2022-36407
hitachi_energy -- mach_scm	SCM Software is a client and server application. An Authenticated System manager client can execute LINQ query in the SCM server, for customized filtering. An Authenticated malicious client can send a specially crafted code to skip the	2024-03-27	7.5	CVE-2024-0400

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	validation and execute arbitrary code (RCE) on the SCM Server remotely. Malicious clients can execute any command by using this RCE vulnerability.			
hitachi_energy -- mach_scm	Authenticated List control client can execute the LINQ query in SCM Server to present event as list for operator. An authenticated malicious client can send special LINQ query to execute arbitrary code remotely (RCE) on the SCM Server that an attacker otherwise does not have authorization to do.	2024-03-27	7.5	CVE-2024-2097
hitachi_energy -- rtu500_series_cmu_firmware	A vulnerability exists in the stb-language file handling that affects the RTU500 series product versions listed below. A malicious actor could print random memory content in the RTU500 system log, if an authorized user uploads a specially crafted stb-language file.	2024-03-27	8.2	CVE-2024-1531
hometory -- mang_board_wp	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hometory Mang Board WP allows Reflected XSS.This issue affects Mang Board WP: from n/a through 1.8.0.	2024-03-29	7.1	CVE-2024-30431
i_thirteen_web_solution -- wp_responsive_tabs_horizontal_vertical_and_accordion_tabs	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in I Thirteen Web Solution WP Responsive Tabs horizontal vertical and accordion Tabs.This issue affects WP Responsive Tabs horizontal vertical and accordion Tabs: from n/a through 1.1.17.	2024-03-29	8.5	CVE-2024-30497
ibm -- common_cryptographic_architecture	IBM Common Cryptographic Architecture (CCA) 7.0.0 through 7.5.36 could allow a remote user to cause a denial of service due to incorrect data handling for certain types of AES operations. IBM X-Force ID: 270602.	2024-03-26	7.5	CVE-2023-47150
icegram -- email_subscribers_&_newsletters	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Icegram Email Subscribers & Newsletters allows Reflected XSS.This issue affects Email Subscribers & Newsletters: from n/a through 5.7.11.	2024-03-27	7.1	CVE-2024-22300
indianic -- widgets_controller	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in IndiaNIC Widgets Controller allows Reflected XSS.This issue affects Widgets Controller: from n/a through 1.1.	2024-03-27	7.1	CVE-2024-25926
infinitum_form -- geo_controller	Deserialization of Untrusted Data vulnerability in INFINITUM FORM Geo Controller.This issue affects Geo Controller: from n/a through 8.6.4.	2024-03-28	9	CVE-2024-30227
it_path_solutions -- contact_form_to_any_api	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in IT Path Solutions Contact Form to Any API.This issue affects Contact Form to Any API: from n/a through 1.1.8.	2024-03-28	8.5	CVE-2024-30242
jetbrains -- teamcity	In JetBrains TeamCity before 2024.03 2FA could be bypassed by providing a special URL parameter	2024-03-28	7.4	CVE-2024-31136
johnbillion -- wp-crontrol	WP Crontrol controls the cron events on WordPress websites. WP Crontrol includes a feature that allows administrative users to create events in the WP-Cron system that store and execute PHP code subject to the restrictive security permissions documented here. While there is no known vulnerability in this feature on its own, there exists potential for this feature to be vulnerable to RCE if it were specifically targeted via vulnerability chaining that exploited a separate SQLi (or similar) vulnerability. This is exploitable on a site if one of the below preconditions are met, the site is vulnerable to a writeable SQLi vulnerability in any plugin, theme, or WordPress core, the site's database is compromised at the hosting level, the site is vulnerable to a method of updating arbitrary options in the wp_options table, or the site is vulnerable to a method of triggering an arbitrary action, filter, or function with control of the parameters. As a hardening measure, WP Crontrol version 1.16.2 ships with a new feature that prevents tampering of the code stored in a PHP cron event.	2024-03-25	8.1	CVE-2024-28850
jonathankissam -- action_network	The Action Network plugin for WordPress is vulnerable to SQL Injection via the 'bulk-action' parameter in version 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.	2024-03-27	7.2	CVE-2024-2954

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jordy_meow -- ai_engine:_chatgpt_chatbot	Unrestricted Upload of File with Dangerous Type vulnerability in Jordy Meow AI Engine: ChatGPT Chatbot.This issue affects AI Engine: ChatGPT Chatbot: from n/a through 2.1.4.	2024-03-28	9.1	CVE-2024-29100
julien_crego -- manager_for_icomoon	Unrestricted Upload of File with Dangerous Type vulnerability in Julien Crego Manager for Icomoon.This issue affects Manager for Icomoon: from n/a through 2.0.	2024-03-26	9.1	CVE-2023-29386
jumpserver -- jumpserver	JumpServer is an open source bastion host and an operation and maintenance security audit system. Attackers can bypass the input validation mechanism in JumpServer's Ansible to execute arbitrary code within the Celery container. Since the Celery container runs with root privileges and has database access, attackers could steal sensitive information from all hosts or manipulate the database. This vulnerability is fixed in v3.10.7.	2024-03-29	9.9	CVE-2024-29201
jumpserver -- jumpserver	JumpServer is an open source bastion host and an operation and maintenance security audit system. Attackers can exploit a Jinja2 template injection vulnerability in JumpServer's Ansible to execute arbitrary code within the Celery container. Since the Celery container runs with root privileges and has database access, attackers could steal sensitive information from all hosts or manipulate the database. This vulnerability is fixed in v3.10.7.	2024-03-29	9.9	CVE-2024-29202
jupyterhub -- jupyterhub	JupyterHub is an open source multi-user server for Jupyter notebooks. By tricking a user into visiting a malicious subdomain, the attacker can achieve an XSS directly affecting the former's session. More precisely, in the context of JupyterHub, this XSS could achieve full access to JupyterHub API and user's single-user server. The affected configurations are single-origin JupyterHub deployments and JupyterHub deployments with user-controlled applications running on subdomains or peer subdomains of either the Hub or a single-user server. This vulnerability is fixed in 4.1.0.	2024-03-27	8.1	CVE-2024-28233
kadence_wp -- gutenberg_blocks_by_kadence_blocks	Server-Side Request Forgery (SSRF) vulnerability in Kadence WP Gutenberg Blocks by Kadence Blocks.This issue affects Gutenberg Blocks by Kadence Blocks: from n/a through 3.2.19.	2024-03-28	7.7	CVE-2024-23500
kainelabs -- youzify_-_buddypress_moderation	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KaineLabs Youzify - Buddypress Moderation.This issue affects Youzify - Buddypress Moderation: from n/a through 1.2.5.	2024-03-25	7.3	CVE-2024-2864
katie_seaborn -- zotpress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Katie Seaborn Zotpress.This issue affects Zotpress: from n/a through 7.3.7.	2024-03-29	8.5	CVE-2024-30488
kienso -- co-marquage_service-public.fr	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kienso Co-marquage service-public.Fr allows Reflected XSS.This issue affects Co-marquage service-public.Fr: from n/a through 0.5.72.	2024-03-27	7.1	CVE-2024-29758
kindspells -- astro-shield	Astro-Shield is a library to compute the subresource integrity hashes for your JS scripts and CSS stylesheets. When automated CSP headers generation for SSR content is enabled and the web application serves content that can be partially controlled by external users, then it is possible that the CSP headers generation feature might be "allow-listing" malicious injected resources like inlined JS, or references to external malicious scripts. The fix is available in version 1.3.0.	2024-03-28	7.5	CVE-2024-29896
klbtheme -- cosmetsy_theme_(core_plugin)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KlbTheme Cosmetsy theme (core plugin), KlbTheme Partdo theme (core plugin), KlbTheme Bacola theme (core plugin), KlbTheme Medibazar theme (core plugin), KlbTheme Furnob theme (core plugin), KlbTheme Clotya theme (core plugin) allows Reflected XSS.This issue affects Cosmetsy theme (core plugin): from n/a through 1.3.0; Partdo theme (core plugin): from n/a through 1.0.9; Bacola theme (core plugin): from n/a through 1.3.3; Medibazar theme (core plugin): from n/a through 1.2.3; Furnob theme (core plugin): from n/a through 1.1.7; Clotya theme (core plugin): from n/a through 1.1.5.	2024-03-26	7.1	CVE-2023-49839
kylephillips -- favorites	The Favorites plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'user_favorites' shortcode in all versions up to, and including, 2.3.3 due to insufficient input sanitization and output escaping on user supplied attributes such as 'no_favorites'. This makes it possible for authenticated attackers, with	2024-03-30	7.2	CVE-2024-2948

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
lg_electronics -- lg_led_assistant	This vulnerability allows remote attackers to reset the password of anonymous users without authorization on the affected LG LED Assistant.	2024-03-25	9.1	CVE-2024-2862 product.security@lge.com
mad_fish_digital -- bulk_noindex_&_nofollow_toolkit	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mad Fish Digital Bulk NoIndex & NoFollow Toolkit allows Reflected XSS.This issue affects Bulk NoIndex & NoFollow Toolkit: from n/a through 2.01.	2024-03-27	7.1	CVE-2024-29791
mainwp -- mainwp_file_uploader_extension	Unrestricted Upload of File with Dangerous Type vulnerability in MainWP MainWP File Uploader Extension.This issue affects MainWP File Uploader Extension: from n/a through 4.1.	2024-03-26	10	CVE-2023-23656
mainwp -- mainwp_links_manager_extension	Deserialization of Untrusted Data vulnerability in MainWP MainWP Links Manager Extension.This issue affects MainWP Links Manager Extension: from n/a through 2.1.	2024-03-28	8.1	CVE-2023-23649
max_foundry -- media_library_folders	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Max Foundry Media Library Folders.This issue affects Media Library Folders: from n/a through 8.1.7.	2024-03-29	8.5	CVE-2024-30486
mergen_software -- quality_management_system	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mergen Software Quality Management System allows SQL Injection.This issue affects Quality Management System: through 25032024.	2024-03-25	9.8	CVE-2024-2865
metagauss -- profilegrid_	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Metagauss ProfileGrid.This issue affects ProfileGrid : from n/a through 5.7.8.	2024-03-29	9.3	CVE-2024-30490
metagauss -- profilegrid_	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Metagauss ProfileGrid.This issue affects ProfileGrid : from n/a through 5.7.1.	2024-03-28	8.5	CVE-2024-30241
metagauss -- profilegrid_	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Metagauss ProfileGrid.This issue affects ProfileGrid : from n/a through 5.7.8.	2024-03-29	8.5	CVE-2024-30491
mndpsingh287 -- theme_editor	Unrestricted Upload of File with Dangerous Type vulnerability in mndpsingh287 Theme Editor.This issue affects Theme Editor: from n/a through 2.7.1.	2024-03-26	7.2	CVE-2023-6091
n/a -- cockpit	A flaw was found in Cockpit. Deleting a sosreport with a crafted name via the Cockpit web interface can lead to a command injection vulnerability, resulting in privilege escalation. This issue affects Cockpit versions 270 and newer.	2024-03-28	7.3	CVE-2024-2947
n/a -- oss_aliyun	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ?? OSS Aliyun.This issue affects OSS Aliyun: from n/a through 1.4.10.	2024-03-29	7.6	CVE-2024-30494
n/a -- pcp	A flaw was found in PCP. The default pmproxy configuration exposes the Redis server backend to the local network, allowing remote command execution with the privileges of the Redis user. This issue can only be exploited when pmproxy is running. By default, pmproxy is not running and needs to be started manually. The pmproxy service is usually started from the 'Metrics settings' page of the Cockpit web interface. This flaw affects PCP versions 4.3.4 and newer.	2024-03-28	8.8	CVE-2024-3019
n/a -- web3-utils	Versions of the package web3-utils before 4.2.1 are vulnerable to Prototype Pollution via the utility functions format and mergeDeep, due to insecure recursive merge. An attacker can manipulate an object's prototype, potentially leading to the alteration of the behavior of all objects inheriting from the affected prototype by passing specially crafted input to these functions.	2024-03-25	7.5	CVE-2024-21505
n/a -- xz	Malicious code was discovered in the upstream tarballs of xz, starting with version 5.6.0. Through a series of complex obfuscations, the liblzma build process extracts a prebuilt object file from a disguised test file existing in the source code, which is then used to modify specific functions in the liblzma code. This results in a modified liblzma library that can be used by any software linked against this library, intercepting and modifying the data interaction with this library.	2024-03-29	10	CVE-2024-3094

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n_squared -- simply_schedule_appointments	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in N Squared Simply Schedule Appointments allows Reflected XSS.This issue affects Simply Schedule Appointments: from n/a through 1.6.6.20.	2024-03-27	7.1	CVE-2024-22311
netweblogic -- meta_tag_manager	The Meta Tag Manager plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.0.2 via deserialization of untrusted input in the get_post_data function. This makes it possible for authenticated attackers, with contributor access or higher, to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-03-28	8.8	CVE-2024-1770
nextcloud -- nextcloudpi	NextcloudPi is a ready to use image for Virtual Machines, Raspberry Pi, Odroid HC1, Rock64 and other boards. A command injection vulnerability in NextCloudPi allows command execution as the root user via the NextCloudPi web-panel. Due to a security misconfiguration this can be used by anyone with access to NextCloudPi web-panel, no authentication is required. It is recommended that the NextCloudPi is upgraded to 1.53.1.	2024-03-29	10	CVE-2024-30247
nvidia -- gpu_display_driver,_vgpu_driver_cloud_gaming_driver	NVIDIA GPU Display Driver for Linux contains a vulnerability where an attacker may access a memory location after the end of the buffer. A successful exploit of this vulnerability may lead to denial of service and data tampering.	2024-03-27	7.1	CVE-2024-0074
nvidia -- gpu_display_driver_vgpu_driver,_cloud_gaming_driver	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can cause an out-of-bounds write. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2024-03-27	7.8	CVE-2024-0071
nvidia -- gpu_display_driver_vgpu_driver_cloud_gaming_driver	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer when the driver is performing an operation at a privilege level that is higher than the minimum level required. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2024-03-27	7.8	CVE-2024-0073
nvidia -- vgpu_driver_cloud_gaming_driver	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, where it allows a guest OS to allocate resources for which the guest OS is not authorized. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	2024-03-27	7.8	CVE-2024-0077
oliver_seidel_bastian_germann -- cformsii	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Oliver Seidel, Bastian Germann CformsII allows Stored XSS.This issue affects CformsII: from n/a through 15.0.5.	2024-03-27	7.1	CVE-2024-22149

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
onthegosystems -- types	Unrestricted Upload of File with Dangerous Type vulnerability in OnTheGoSystems Types.This issue affects Types: from n/a through 3.4.17.	2024-03-26	7.2	CVE-2023-27440
openeuler -- a-tune-collector	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in openEuler A-Tune-Collector on Linux allows Command Injection. This vulnerability is associated with program files https://gitee.Com/openeuler/A-Tune-Collector/blob/master/atune_collector/plugin/monitor/process/sched.Py. This issue affects A-Tune-Collector: from 1.1.0-3 through 1.3.0.	2024-03-25	8.1	CVE-2024-24897
openeuler -- aops-zeus	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in openEuler aops-zeus on Linux allows Command Injection. This vulnerability is associated with program files https://gitee.Com/openeuler/aops-zeus/blob/master/zeus/conf/constant.Py. This issue affects aops-zeus: from 1.2.0 through 1.4.0.	2024-03-25	7.2	CVE-2024-24899
openeuler -- gala-gopher	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in openEuler gala-gopher on Linux allows Command Injection. This vulnerability is associated with program files https://gitee.Com/openeuler/gala-gopher/blob/master/src/probes/extends/ebpf.Probe/src/ioprobe/ioprobe.C. This issue affects gala-gopher: through 1.0.2.	2024-03-25	7.8	CVE-2024-24890
openeuler -- isulad	Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in openEuler iSulad on Linux allows Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions. This vulnerability is associated with program files https://gitee.Com/openeuler/iSulad/blob/master/src/cmd/isulad/main.C. This issue affects iSulad: 2.0.18-13, from 2.1.4-1 through 2.1.4-2.	2024-03-25	7	CVE-2021-33632
openeuler -- migration-tools	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Privilege Management vulnerability in openEuler migration-tools on Linux allows Command Injection, Restful Privilege Elevation. This vulnerability is associated with program files https://gitee.Com/openeuler/migration-tools/blob/master/index.Py. This issue affects migration-tools: from 1.0.0 through 1.0.1.	2024-03-25	8.1	CVE-2024-24892
opentext -- secure_content_manager	By leveraging the vulnerability, lower-privileged users of Content Manager can manipulate Content Manager clients to elevate privileges and perform unauthorized operations.	2024-03-25	8.5	CVE-2024-1973
opentextÃƒÂ¢- -- zenworks_configuration_management_(zcm)	Incorrect Authorization vulnerability in OpenTextÃ¢â€žÂ¢ ZENworks Configuration Management (ZCM) allows Unauthorized Use of Device Resources.This issue affects ZENworks Configuration Management (ZCM) versions: 2020 update 3, 23.3, and 23.4.	2024-03-27	7.4	CVE-2023-6400
ossrs -- srs	SRS is a simple, high-efficiency, real-time video server. SRS's `/api/v1/vhosts/vid-<id>?callback=<payload>` endpoint didn't filter the callback function name which led to injecting malicious javascript payloads and executing XSS (Cross-Site Scripting). This vulnerability is fixed in 5.0.210 and 6.0.121.	2024-03-28	7.2	CVE-2024-29882
perfectwpthemes -- glaze_blog_lite	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in perfectwpthemes Glaze Blog Lite, themebeez Fascinate, themebeez Cream Blog, themebeez Cream Magazine allows Reflected XSS.This issue affects Glaze Blog Lite: from n/a through <= 1.1.4; Fascinate: from n/a through 1.0.8; Cream Blog: from n/a through 2.1.3; Cream Magazine: from n/a through 2.1.4.	2024-03-26	7.1	CVE-2023-28687
photo_gallery_team -- photo_gallery_by_ays	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Photo Gallery Team Photo Gallery by Ays allows Reflected XSS.This issue affects Photo Gallery by Ays: from n/a through 5.5.2.	2024-03-27	7.1	CVE-2024-29919
phpgurukul -- emergency_ambulance_hiring_portal	A vulnerability classified as critical has been found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. Affected is an unknown function of the file /admin/login.php of the component Admin Login Page. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-258678 is the identifier assigned to this vulnerability.	2024-03-30	7.3	CVE-2024-3085

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phpgurukul -- emergency_ambulance_hiring_portal	A vulnerability, which was classified as critical, has been found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. Affected by this issue is some unknown functionality of the file ambulance-tracking.php of the component Ambulance Tracking Page. The manipulation of the argument searchdata leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258680.	2024-03-30	7.3	CVE-2024-3087
phpgurukul -- emergency_ambulance_hiring_portal	A vulnerability, which was classified as critical, was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. This affects an unknown part of the file /admin/forgot-password.php of the component Forgot Password Page. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258681 was assigned to this vulnerability.	2024-03-30	7.3	CVE-2024-3088
pi-hole -- pi-hole	The Pi-hole is a DNS sinkhole that protects your devices from unwanted content without installing any client-side software. A vulnerability has been discovered in Pihole that allows an authenticated user on the platform to read internal server files arbitrarily, and because the application runs from behind, reading files is done as a privileged user.If the URL that is in the list of "Adslists" begins with "file*" it is understood that it is updating from a local file, on the other hand if it does not begin with "file*" depending on the state of the response it does one thing or another. The problem resides in the update through local files. When updating from a file which contains non-domain lines, 5 of the non-domain lines are printed on the screen, so if you provide it with any file on the server which contains non-domain lines it will print them on the screen. This vulnerability is fixed by 5.18.	2024-03-27	7.6	CVE-2024-28247
pi-hole -- pi-hole	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Supsystic Slider by Supsystic.This issue affects Slider by Supsystic: from n/a through 1.8.10.	2024-03-28	7.6	CVE-2024-30237
pickplugins -- post_grid	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PickPlugins Post Grid allows Reflected XSS.This issue affects Post Grid: from n/a through 2.2.74.	2024-03-29	7.1	CVE-2024-30441
pluggabl_llc -- booster_for_woocommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pluggabl LLC Booster for WooCommerce allows Reflected XSS.This issue affects Booster for WooCommerce: from n/a through 7.1.7.	2024-03-27	7.1	CVE-2024-29760
podlove -- podlove_podcast_publisher	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Podlove Podlove Podcast Publisher allows Reflected XSS.This issue affects Podlove Podcast Publisher: from n/a through 4.0.9.	2024-03-27	7.1	CVE-2024-29915
posimyth -- the_plus_blocks_for_block_editor_|_gutenberg	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in POSIMYTH The Plus Blocks for Block Editor | Gutenberg allows Reflected XSS.This issue affects The Plus Blocks for Block Editor | Gutenberg: from n/a through 3.2.5.	2024-03-29	7.1	CVE-2024-30435
pretty_links -- shortlinks_by_pretty_links	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pretty Links Shortlinks by Pretty Links allows Reflected XSS.This issue affects Shortlinks by Pretty Links: from n/a through 3.6.2.	2024-03-27	7.1	CVE-2024-29770
princeahmed -- integrate_google_drive_-_browse_upload_download_embed,_play_share_gallery_and_manage_your_google_drive_files_into_your_wordpress_site	The Integrate Google Drive - Browse, Upload, Download, Embed, Play, Share, Gallery, and Manage Your Google Drive Files Into Your WordPress Site plugin for WordPress is vulnerable to unauthorized access of data, modification of data, and loss of data due to a missing capability check on multiple AJAX in all versions up to, and including, 1.3.8. This makes it possible for authenticated attackers to modify plugin settings as well as allowing full read/write/delete access to the Google Drive associated with the plugin.	2024-03-30	10	CVE-2024-2086
propertyhive -- propertyhive	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PropertyHive allows Reflected XSS.This issue affects PropertyHive: from n/a through 2.0.8.	2024-03-27	7.1	CVE-2024-29923
realmag777 -- bear	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in realmag777 BEAR allows Reflected XSS.This issue affects BEAR: from n/a through 1.1.4.2.	2024-03-28	7.1	CVE-2024-30200
realmag777 -- husky_-	The HUSKY - Products Filter Professional for WooCommerce plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.3.5.2 via	2024-03-29	7.2	CVE-2024-3061

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_products_filter_professional_for_woocommerce	the 'type' parameter. This makes it possible for authenticated attackers, with administrator-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.			
realmag777 -- wordpress_meta_data_and_taxonomies_filter_(mdtf)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in realmag777 WordPress Meta Data and Taxonomies Filter (MDTF) allows Reflected XSS.This issue affects WordPress Meta Data and Taxonomies Filter (MDTF): from n/a through 1.3.3.	2024-03-27	7.1	CVE-2024-29763
repute_infosystems -- armember	Deserialization of Untrusted Data vulnerability in Repute Infosystems ARMember.This issue affects ARMember: from n/a through 4.0.26.	2024-03-28	9	CVE-2024-30223
repute_infosystems -- armember	Deserialization of Untrusted Data vulnerability in Repute Infosystems ARMember.This issue affects ARMember: from n/a through 4.0.26.	2024-03-28	8.5	CVE-2024-30222
reservation_diary -- redi_restaurant_reservation	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Reservation Diary ReDi Restaurant Reservation allows Reflected XSS.This issue affects ReDi Restaurant Reservation: from n/a through 24.0128.	2024-03-27	7.1	CVE-2024-29806
rockwell_automation -- arena_simulation	An arbitrary code execution vulnerability in Rockwell Automation Arena Simulation could let a malicious user insert unauthorized code into the software. This is done by writing beyond the designated memory area, which causes an access violation. Once inside, the threat actor can run harmful code on the system. This affects the confidentiality, integrity, and availability of the product. To trigger this, the user would unwittingly need to open a malicious file shared by the threat actor.	2024-03-26	7.8	CVE-2024-21912
rockwell_automation -- arena_simulation	A heap-based memory buffer overflow vulnerability in Rockwell Automation Arena Simulation software could potentially allow a malicious user to insert unauthorized code into the software by overstepping the memory boundaries, which triggers an access violation. Once inside, the threat actor can run harmful code on the system. This affects the confidentiality, integrity, and availability of the product. To trigger this, the user would unwittingly need to open a malicious file shared by the threat actor.	2024-03-26	7.8	CVE-2024-21913
rockwell_automation -- arena_simulation	A memory buffer vulnerability in Rockwell Automation Arena Simulation software could potentially allow a malicious user to insert unauthorized code to the software by corrupting the memory and triggering an access violation. Once inside, the threat actor can run harmful code on the system. This affects the confidentiality, integrity, and availability of the product. To trigger this, the user would unwittingly need to open a malicious file shared by the threat actor.	2024-03-26	7.8	CVE-2024-21918
rockwell_automation -- arena_simulation	An uninitialized pointer in Rockwell Automation Arena Simulation software could potentially allow a malicious user to insert unauthorized code to the software by leveraging the pointer after it is properly. Once inside, the threat actor can run harmful code on the system. This affects the confidentiality, integrity, and availability of the product. To trigger this, the user would unwittingly need to open a malicious file shared by the threat actor.	2024-03-26	7.8	CVE-2024-21919
rockwell_automation -- arena_simulation	A memory corruption vulnerability in Rockwell Automation Arena Simulation software could potentially allow a malicious user to insert unauthorized code to the software by corrupting the memory triggering an access violation. Once inside, the threat actor can run harmful code on the system. This affects the confidentiality, integrity, and availability of the product. To trigger this, the user would unwittingly need to open a malicious file shared by the threat actor.	2024-03-26	7.8	CVE-2024-2929
rockwell_automation_ -- powerflex_527	A denial-of-service vulnerability exists in the Rockwell Automation PowerFlexÃ‚Â® 527 due to improper input validation in the device. If exploited, the web server will crash and need a manual restart to recover it.	2024-03-25	7.5	CVE-2024-2425
rockwell_automation_ -- powerflex_527	A denial-of-service vulnerability exists in the Rockwell Automation PowerFlexÃ‚Â® 527 due to improper input validation in the device. If exploited, a disruption in the CIP communication will occur and a manual restart will be required by the user to recover it.	2024-03-25	7.5	CVE-2024-2426
rockwell_automation_ -- powerflex_527	A denial-of-service vulnerability exists in the Rockwell Automation PowerFlexÃ‚Â® 527 due to improper traffic throttling in the device. If multiple data packets are sent to the device repeatedly the device will crash and require a manual restart to recover.	2024-03-25	7.5	CVE-2024-2427

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ruijie -- rg-eg350	A vulnerability classified as critical was found in Ruijie RG-EG350 up to 20240318. Affected by this vulnerability is the function setAction of the file /itbox_pi/networksafe.php?a=set of the component HTTP POST Request Handler. The manipulation of the argument bandwidth leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257977 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	8.8	CVE-2024-2909
salon_booking_system -- salon_booking_system	Unrestricted Upload of File with Dangerous Type vulnerability in Salon Booking System Salon booking system.This issue affects Salon booking system: from n/a through 9.5.	2024-03-29	10	CVE-2024-30510
semenov -- new_royalslider	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Semenov New RoyalSlider allows Reflected XSS.This issue affects New RoyalSlider: from n/a through 3.4.2.	2024-03-27	7.1	CVE-2024-30195
serverpod -- serverpod	Serverpod is an app and web server, built for the Flutter and Dart ecosystem. This bug bypassed the validation of TSL certificates on all none web HTTP clients in the `serverpod_client` package. Making them susceptible to a man in the middle attack against encrypted traffic between the client device and the server. An attacker would need to be able to intercept the traffic and highjack the connection to the server for this vulnerability to be used. Upgrading to version `1.2.6` resolves this issue.	2024-03-27	7.4	CVE-2024-29887
shopup -- shipping_with_venipak_for_woocommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShopUp Shipping with Venipak for WooCommerce allows Reflected XSS.This issue affects Shipping with Venipak for WooCommerce: from n/a through 1.19.5.	2024-03-27	7.1	CVE-2024-29805
sonaar_music -- mp3_audio_player_for_music_radio_&_podcast_by_sonaar	Missing Authorization vulnerability in Sonaar Music MP3 Audio Player for Music, Radio & Podcast by Sonaar.This issue affects MP3 Audio Player for Music, Radio & Podcast by Sonaar: from n/a through 5.1.	2024-03-29	7.6	CVE-2024-30487
sourcecodester -- music_gallery_site	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file classes/Master.php?f=save_music. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258001 was assigned to this vulnerability.	2024-03-27	7.3	CVE-2024-2930
spiffy_plugins -- spiffy_calendar	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Spiffy Plugins Spiffy Calendar allows Reflected XSS.This issue affects Spiffy Calendar: from n/a through 4.9.7.	2024-03-29	7.1	CVE-2024-30427
splunk -- splunk_enterprise	In Splunk Enterprise versions below 9.2.1, 9.1.4, and 9.0.9, the Dashboard Examples Hub in the Splunk Dashboard Studio app lacks protections for risky SPL commands. This could let attackers bypass SPL safeguards for risky commands in the Hub. The vulnerability would require the attacker to phish the victim by tricking them into initiating a request within their browser.	2024-03-27	8.1	CVE-2024-29946
splunk -- splunk_enterprise	In Splunk Enterprise versions below 9.2.1, 9.1.4, and 9.0.9, the software potentially exposes authentication tokens during the token validation process. This exposure happens when either Splunk Enterprise runs in debug mode or the JsonWebToken component has been configured to log its activity at the DEBUG logging level.	2024-03-27	7.2	CVE-2024-29945
squirrly -- seo_plugin_by_squirrly_seo	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Squirrly SEO Plugin by Squirrly SEO allows Reflected XSS.This issue affects SEO Plugin by Squirrly SEO: from n/a through 12.3.16.	2024-03-27	7.1	CVE-2024-29790
stylemix -- masterstudy_lms_wordpress_plugin_-_for_online_courses_and_education	The MasterStudy LMS plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.3.1. This is due to insufficient validation checks within the _register_user() function called by the 'wp_ajax_nopriv_stm_lms_register' AJAX action. This makes it possible for unauthenticated attackers to register a user with administrator-level privileges when MasterStudy LMS Pro is installed and the LMS Forms Editor add-on is enabled.	2024-03-29	9.8	CVE-2024-2409
stylemix -- masterstudy_lms_	The MasterStudy LMS plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.3.0 via the 'modal' parameter. This makes it	2024-03-29	9.8	CVE-2024-2411

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress_plugin_-_for_online_courses_and_education	possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.			
survey_maker_team -- survey_maker	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Survey Maker team Survey Maker allows Reflected XSS.This issue affects Survey Maker: from n/a through 4.0.6.	2024-03-27	7.1	CVE-2024-29918
synology -- surveillance_station	Missing authorization vulnerability in System webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to bypass security constraints via unspecified vectors.	2024-03-28	9.9	CVE-2024-29241
synology -- surveillance_station	Missing authorization vulnerability in GetStmUrlPath webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to obtain sensitive information via unspecified vectors.	2024-03-28	7.7	CVE-2024-29228
synology -- surveillance_station	Missing authorization vulnerability in GetLiveViewPath webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to obtain sensitive information via unspecified vectors.	2024-03-28	7.7	CVE-2024-29229
sysaid -- sysaid	SysAid before version 23.2.14 b18 - CWE-918: Server-Side Request Forgery (SSRF) may allow exposing the local OS user's NTLMv2 hash	2024-03-28	7.2	CVE-2024-27775
teamviewer -- remote_client	Insecure UNIX Symbolic Link (Symlink) Following in TeamViewer Remote Client prior Version 15.52 for macOS allows an attacker with unprivileged access, to potentially elevate privileges or conduct a denial-of-service-attack by overwriting the symlink.	2024-03-26	7.1	CVE-2024-1933 psirt@teamviewer.com
tenda -- ac10_firmware	A vulnerability, which was classified as critical, has been found in Tenda AC10 16.03.10.13/16.03.10.20. Affected by this issue is the function fromSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument timeZone leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257780. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-24	9.8	CVE-2024-2856
tenda -- ac10u_firmware	A vulnerability was found in Tenda AC10U 15.03.06.48/15.03.06.49. It has been rated as critical. This issue affects the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257777 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-24	9.8	CVE-2024-2853
tenda -- ac15_firmware	A vulnerability was found in Tenda AC15 15.03.05.18 and classified as critical. Affected by this issue is the function saveParentControlInfo of the file /goform/saveParentControlInfo. The manipulation of the argument urls leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257774 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-24	9.8	CVE-2024-2850
tenda -- ac15_firmware	A vulnerability was found in Tenda AC15 15.03.05.18/15.03.20_multi. It has been classified as critical. This affects the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257775. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-24	9.8	CVE-2024-2851
tenda -- ac15_firmware	A vulnerability was found in Tenda AC15 15.03.20_multi. It has been declared as critical. This vulnerability affects the function saveParentControlInfo of the file /goform/saveParentControlInfo. The manipulation of the argument urls leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257776. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-24	9.8	CVE-2024-2852
tenda -- ac15_firmware	A vulnerability classified as critical was found in Tenda AC15 15.03.05.18/15.03.05.19/15.03.20. Affected by this vulnerability is the function fromSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument time leads to stack-based buffer overflow. The attack can be launched	2024-03-24	9.8	CVE-2024-2855

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257779. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
tenda -- ac18_firmware	A vulnerability classified as critical has been found in Tenda AC18 15.03.05.05. Affected is the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257778 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-24	9.8	CVE-2024-2854
tenda -- ac7	A vulnerability, which was classified as critical, was found in Tenda AC7 15.03.06.44. Affected is the function formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257934 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	8.8	CVE-2024-2891
tenda -- ac7	A vulnerability has been found in Tenda AC7 15.03.06.44 and classified as critical. Affected by this vulnerability is the function formSetCfm of the file /goform/setcfm. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257935. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	8.8	CVE-2024-2892
tenda -- ac7	A vulnerability was found in Tenda AC7 15.03.06.44 and classified as critical. Affected by this issue is the function formSetDeviceName of the file /goform/SetOnlineDevName. The manipulation of the argument devName leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257936. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	8.8	CVE-2024-2893
tenda -- ac7	A vulnerability was found in Tenda AC7 15.03.06.44. It has been classified as critical. This affects the function formSetQosBand of the file /goform/SetNetControlList. The manipulation of the argument list leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257937 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	8.8	CVE-2024-2894
tenda -- ac7	A vulnerability was found in Tenda AC7 15.03.06.44. It has been declared as critical. This vulnerability affects the function formWifiWpsOOB of the file /goform/WifiWpsOOB. The manipulation of the argument index leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257938 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	8.8	CVE-2024-2895
tenda -- ac7	A vulnerability was found in Tenda AC7 15.03.06.44. It has been rated as critical. This issue affects the function formWifiWpsStart of the file /goform/WifiWpsStart. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257939. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	8.8	CVE-2024-2896
tenda -- ac7	A vulnerability classified as critical was found in Tenda AC7 15.03.06.44. Affected by this vulnerability is the function fromSetRouteStatic of the file /goform/SetStaticRouteCfg. The manipulation of the argument list leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257941 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	8.8	CVE-2024-2898
tenda -- ac7	A vulnerability, which was classified as critical, has been found in Tenda AC7 15.03.06.44. Affected by this issue is the function fromSetWirelessRepeat of the file /goform/WifiExtraSet. The manipulation of the argument wpapsk_crypto leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257942 is the identifier	2024-03-26	8.8	CVE-2024-2899

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
tenda -- ac7	A vulnerability, which was classified as critical, was found in Tenda AC7 15.03.06.44. This affects the function saveParentControlInfo of the file /goform/saveParentControlInfo. The manipulation of the argument deviceId/time/urls leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257943. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	8.8	CVE-2024-2900
tenda -- ac7	A vulnerability has been found in Tenda AC7 15.03.06.44 and classified as critical. This vulnerability affects the function setSchedWifi of the file /goform/openSchedWifi. The manipulation of the argument schedEndTime leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257944. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	8.8	CVE-2024-2901
tenda -- ac7	A vulnerability was found in Tenda AC7 15.03.06.44 and classified as critical. This issue affects the function fromSetWifiGusetBasic of the file /goform/WifiGuestSet. The manipulation of the argument shareSpeed leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257945 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	8.8	CVE-2024-2902
tenda -- ac7	A vulnerability was found in Tenda AC7 15.03.06.44. It has been classified as critical. Affected is the function GetParentControlInfo of the file /goform/GetParentControlInfo. The manipulation of the argument mac leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257946 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	8.8	CVE-2024-2903
tenda -- f1203	A vulnerability was found in Tenda F1203 2.0.1.6. It has been declared as critical. Affected by this vulnerability is the function R7WebsSecurityHandler of the file /goform/execCommand. The manipulation of the argument password leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258145 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2976
tenda -- f1203	A vulnerability was found in Tenda F1203 2.0.1.6. It has been rated as critical. Affected by this issue is the function formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-258146 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2977
tenda -- f1203	A vulnerability classified as critical has been found in Tenda F1203 2.0.1.6. This affects the function formSetCfm of the file /goform/setcfm. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258147. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2978
tenda -- f1203	A vulnerability classified as critical was found in Tenda F1203 2.0.1.6. This vulnerability affects the function setSchedWifi of the file /goform/openSchedWifi. The manipulation of the argument schedStartTime/schedEndTime leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258148. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2979
tenda -- fh1202	A vulnerability, which was classified as critical, has been found in Tenda FH1202 1.2.0.14(408). This issue affects the function formexeCommand of the file /goform/execCommand. The manipulation of the argument cmdinput leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258149 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2980

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenda -- fh1202	A vulnerability, which was classified as critical, was found in Tenda FH1202 1.2.0.14(408). Affected is the function form_fast_setting_wifi_set of the file /goform/fast_setting_wifi_set. The manipulation of the argument ssid leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-258150 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2981
tenda -- fh1202	A vulnerability was found in Tenda FH1202 1.2.0.14(408) and classified as critical. Affected by this issue is the function formSetClientState of the file /goform/SetClientState. The manipulation of the argument deviceId/limitSpeed/limitSpeedUp leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258152. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2983
tenda -- fh1202	A vulnerability was found in Tenda FH1202 1.2.0.14(408). It has been classified as critical. This affects the function formSetCfm of the file /goform/setcfm. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258153 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2984
tenda -- fh1202	A vulnerability was found in Tenda FH1202 1.2.0.14(408). It has been declared as critical. This vulnerability affects the function formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-258154 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2985
tenda -- fh1202	A vulnerability was found in Tenda FH1202 1.2.0.14(408). It has been rated as critical. This issue affects the function formSetSpeedWan of the file /goform/SetSpeedWan. The manipulation of the argument speed_dir leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258155. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2986
tenda -- fh1202	A vulnerability classified as critical has been found in Tenda FH1202 1.2.0.14(408). Affected is the function GetParentControlInfo of the file /goform/GetParentControlInfo. The manipulation of the argument mac leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258156. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2987
tenda -- fh1202	A vulnerability classified as critical was found in Tenda FH1203 2.0.1.6. Affected by this vulnerability is the function fromSetRouteStatic of the file /goform/fromRouteStatic. The manipulation of the argument entrys leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258157 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2988
tenda -- fh1202	A vulnerability, which was classified as critical, has been found in Tenda FH1203 2.0.1.6. Affected by this issue is the function fromNatStaticSetting of the file /goform/NatStaticSetting. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-258158 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2989
tenda -- fh1203	A vulnerability, which was classified as critical, was found in Tenda FH1203 2.0.1.6. This affects the function formexeCommand of the file /goform/execCommand. The manipulation of the argument cmdinput leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258159. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2990
tenda -- fh1203	A vulnerability was found in Tenda FH1203 2.0.1.6 and classified as critical. This issue affects the function formSetCfm of the file /goform/setcfm. The manipulation	2024-03-27	8.8	CVE-2024-2992

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of the argument funcpara1 leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258161 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
tenda -- fh1203	A vulnerability was found in Tenda FH1203 2.0.1.6. It has been classified as critical. Affected is the function formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-258162 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2993
tenda -- fh1203	A vulnerability was found in Tenda FH1203 2.0.1.6. It has been declared as critical. Affected by this vulnerability is the function GetParentControlInfo of the file /goform/GetParentControlInfo. The manipulation of the argument mac leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258163. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-2994
tenda -- fh1205	A vulnerability classified as critical was found in Tenda FH1205 2.0.0.7(775). This vulnerability affects the function fromSetRouteStatic of the file /goform/fromRouteStatic. The manipulation of the argument entrys leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258292. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-3006
tenda -- fh1205	A vulnerability, which was classified as critical, has been found in Tenda FH1205 2.0.0.7(775). This issue affects the function fromNatStaticSetting of the file /goform/NatStaticSetting. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258293 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-3007
tenda -- fh1205	A vulnerability, which was classified as critical, was found in Tenda FH1205 2.0.0.7(775). Affected is the function formexeCommand of the file /goform/execCommand. The manipulation of the argument cmdinput leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-258294 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	8.8	CVE-2024-3008
tenda -- fh1205	A vulnerability was found in Tenda FH1205 2.0.0.7(775) and classified as critical. Affected by this issue is the function formSetCfm of the file /goform/setcfm. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258296. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-28	8.8	CVE-2024-3010
tenda -- fh1205	A vulnerability was found in Tenda FH1205 2.0.0.7(775). It has been classified as critical. This affects the function formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258297 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-28	8.8	CVE-2024-3011
tenda -- fh1205	A vulnerability was found in Tenda FH1205 2.0.0.7(775). It has been declared as critical. This vulnerability affects the function GetParentControlInfo of the file /goform/GetParentControlInfo. The manipulation of the argument mac leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-258298 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-28	8.8	CVE-2024-3012
teosoft_software -- teobase	Authentication Bypass by Primary Weakness vulnerability in TeoSOFT Software TeoBASE allows Authentication Bypass.This issue affects TeoBASE: through 20240327. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	9.8	CVE-2023-6153

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
teosoft_software -- teobase	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TeoSOFT Software TeoBASE allows SQL Injection.This issue affects TeoBASE: through 27032024. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	9.8	CVE-2023-6173
terry_lin -- wp_githuber_md	Unrestricted Upload of File with Dangerous Type vulnerability in Terry Lin WP Githuber MD.This issue affects WP Githuber MD: from n/a through 1.16.2.	2024-03-26	9.1	CVE-2023-47846
themefusion -- avada	Unrestricted Upload of File with Dangerous Type vulnerability in ThemeFusion Avada.This issue affects Avada: from n/a through 7.11.1.	2024-03-26	8.5	CVE-2023-39307
themefusion -- avada	Server-Side Request Forgery (SSRF) vulnerability in ThemeFusion Avada.This issue affects Avada: from n/a through 7.11.1.	2024-03-28	7.7	CVE-2023-39313
themefusion -- fusion_builder	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ThemeFusion Fusion Builder.This issue affects Fusion Builder: from n/a through 3.11.1.	2024-03-28	8.5	CVE-2023-39309
themefusion -- fusion_builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeFusion Fusion Builder allows Reflected XSS.This issue affects Fusion Builder: from n/a through 3.11.1.	2024-03-27	7.1	CVE-2023-39306
themefusion -- fusion_builder	Cross-Site Request Forgery (CSRF) vulnerability in ThemeFusion Fusion Builder.This issue affects Fusion Builder: from n/a through 3.11.1.	2024-03-27	7.1	CVE-2023-39311
thorsten -- phpmyfaq	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. A SQL injection vulnerability has been discovered in the the "Add News" functionality due to improper escaping of the email address. This allows any authenticated user with the rights to add/edit FAQ news to exploit this vulnerability to exfiltrate data, take over accounts and in some cases, even achieve RCE. The vulnerable field lies in the `authorEmail` field which uses PHP's `FILTER_VALIDATE_EMAIL` filter. This filter is insufficient in protecting against SQL injection attacks and should still be properly escaped. However, in this version of phpMyFAQ (3.2.5), this field is not escaped properly can be used together with other fields to fully exploit the SQL injection vulnerability. This vulnerability is fixed in 3.2.6.	2024-03-25	8.8	CVE-2024-27299
thorsten -- phpmyfaq	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. A SQL injection vulnerability has been discovered in the `insertentry` & `saveentry` when modifying records due to improper escaping of the email address. This allows any authenticated user with the rights to add/edit FAQ news to exploit this vulnerability to exfiltrate data, take over accounts and in some cases, even achieve RCE. This vulnerability is fixed in 3.2.6.	2024-03-25	8.8	CVE-2024-28107
thorsten -- phpmyfaq	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. The category image upload function in phpmyfaq is vulnerable to manipulation of the `Content-type` and `lang` parameters, allowing attackers to upload malicious files with a .php extension, potentially leading to remote code execution (RCE) on the system. This vulnerability is fixed in 3.2.6.	2024-03-25	7.2	CVE-2024-28105
tomas -- wordpress_tooltips	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Tomas WordPress Tooltips.This issue affects WordPress Tooltips: from n/a before 9.4.5.	2024-03-28	8.5	CVE-2024-30243
tp-link -- tp-link_ex20v_ax1800_tp-link_archer_c5v_ac1200_tp-link_td-w9970_tp-link_td-w9970v3_tp-link_vx220-g2u_tp-link_vn020-g2u_	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in TP-Link TP-Link EX20v AX1800, Tp-Link Archer C5v AC1200, Tp-Link TD-W9970, Tp-Link TD-W9970v3, TP-Link VX220-G2u, TP-Link VN020-G2u allows authenticated OS Command Injection.This issue affects TP-Link EX20v AX1800, Tp-Link Archer C5v AC1200, Tp-Link TD-W9970, Tp-Link TD-W9970v3 : through 20240328. Also the vulnerability continues in the TP-Link VX220-G2u and TP-Link VN020-G2u models due to the products not being produced and supported.	2024-03-28	9.8	CVE-2023-6437
trustindex.io -- widgets_for_google_reviews	Unrestricted Upload of File with Dangerous Type vulnerability in Trustindex.Io Widgets for Google Reviews.This issue affects Widgets for Google Reviews: from n/a through 11.0.2.	2024-03-26	8	CVE-2023-48275
trustindex.io -- wp_testimonials	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Trustindex.Io WP Testimonials.This issue affects WP Testimonials: from n/a through 1.4.3.	2024-03-28	7.6	CVE-2024-25924

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tumult_inc. -- tumult_hype_animations	Unrestricted Upload of File with Dangerous Type vulnerability in Tumult Inc. Tumult Hype Animations.This issue affects Tumult Hype Animations: from n/a through 1.9.12.	2024-03-28	9.1	CVE-2024-2890
typps -- calendarista	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Typps Calendarista.This issue affects Calendarista: from n/a through 15.5.7.	2024-03-28	8.5	CVE-2024-30240
unlimited_elements -- unlimited_elements_for_elementor_(free_widgets_addons,_templates)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) allows Reflected XSS.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 1.5.93.	2024-03-27	7.1	CVE-2024-29792
venalean -- tuleap	Tuleap is an Open Source Suite to improve management of software developments and collaboration. A malicious user could exploit this issue on purpose to delete information on the instance or possibly gain access to restricted artifacts. It is however not possible to control exactly which information is deleted. Information from theDate, File, Float, Int, List, OpenList, Text, and Permissions on artifact (this one can lead to the disclosure of restricted information) fields can be impacted. This vulnerability is fixed in Tuleap Community Edition version 15.7.99.6 and Tuleap Enterprise Edition 15.7-2, 15.6-5, 15.5-6, 15.4-8, 15.3-6, 15.2-5, 15.1-9, 15.0-9, and 14.12-6.	2024-03-29	7.6	CVE-2024-30246
verapdf -- verapdf-library	veraPDF-library is a PDF/A validation library. Executing policy checks using custom schematron files invokes an XSL transformation that could lead to a remote code execution (RCE) vulnerability. This vulnerability is fixed in 1.24.2.	2024-03-28	8.1	CVE-2024-28109
vsourz_digital -- all_in_one_redirection	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vsourz Digital All In One Redirection allows Stored XSS.This issue affects All In One Redirection: from n/a through 2.2.0.	2024-03-29	7.1	CVE-2024-30506
w3_eden_inc. -- premium_packages	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in W3 Eden, Inc. Premium Packages allows Reflected XSS.This issue affects Premium Packages: from n/a through 5.8.2.	2024-03-27	7.1	CVE-2024-29924
wapppress_team -- wapppress	Unrestricted Upload of File with Dangerous Type vulnerability in WappPress Team WappPress.This issue affects WappPress: from n/a through 5.0.3.	2024-03-27	10	CVE-2023-49815
webdzier -- button	The Button plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.1.28 via deserialization of untrusted input in the button_shortcode function. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-03-29	8.8	CVE-2024-1872
webtoffee -- product_import_export_for_woocommerce	Unrestricted Upload of File with Dangerous Type vulnerability in WebToffee Product Import Export for WooCommerce.This issue affects Product Import Export for WooCommerce: from n/a through 2.4.1.	2024-03-26	9.1	CVE-2024-30231
webtoffee -- woocommerce_pdf_invoices,_packing_slips,_delivery_notes_and_shipping_labels	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebToffee WooCommerce PDF Invoices, Packing Slips, Delivery Notes and Shipping Labels allows Reflected XSS.This issue affects WooCommerce PDF Invoices, Packing Slips, Delivery Notes and Shipping Labels: from n/a through 4.4.0.	2024-03-27	7.1	CVE-2024-22288
wedevs -- wp_erp_|_complete_hr_solution_with_recruitment_&_job_listings_|_woocommerce_crm_&	The WP ERP | Complete HR solution with recruitment & job listings | WooCommerce CRM & Accounting plugin for WordPress is vulnerable to union-based SQL Injection via the 'email' parameter in all versions up to, and including, 1.12.9 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 subscriber-level access and above, to append	2024-03-29	8.8	CVE-2024-0608

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_accounting	additional SQL queries into already existing queries that can be used to extract sensitive information from the database.			
wedevs -- wp_erp_|_complete_hr_solution_with_recruitment_&_job_listings_|_woocommerce_crm_&_accounting	The WP ERP | Complete HR solution with recruitment & job listings | WooCommerce CRM & Accounting plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'api_key' parameter in all versions up to, and including, 1.12.9 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.	2024-03-29	7.2	CVE-2024-0609
wedevs -- wp_erp_|_complete_hr_solution_with_recruitment_&_job_listings_|_woocommerce_crm_&_accounting	The WP ERP | Complete HR solution with recruitment & job listings | WooCommerce CRM & Accounting plugin for WordPress is vulnerable to time-based SQL Injection via the erp/v1/accounting/v1/transactions/sales REST API endpoint in all versions up to, and including, 1.12.9 due to insufficient escaping on the user supplied status and customer_id parameters and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with accounting manager or admin privileges and higher to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-03-29	7.2	CVE-2024-0913
wedevs -- wp_erp_|_complete_hr_solution_with_recruitment_&_job_listings_|_woocommerce_crm_&_accounting	The WP ERP | Complete HR solution with recruitment & job listings | WooCommerce CRM & Accounting plugin for WordPress is vulnerable to time-based SQL Injection via the id parameter via the erp/v1/accounting/v1/vendors/1/products/ REST route in all versions up to, and including, 1.12.9 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 admin or accounting manager privileges, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-03-29	7.2	CVE-2024-0956
wen_solutions -- wp_child_theme_generator	Unrestricted Upload of File with Dangerous Type vulnerability in WEN Solutions WP Child Theme Generator.This issue affects WP Child Theme Generator: from n/a through 1.0.9.	2024-03-26	9.1	CVE-2023-47873
wholesale_team -- wholesalex	Deserialization of Untrusted Data vulnerability in Wholesale Team WholesaleX.This issue affects WholesaleX: from n/a through 1.3.2.	2024-03-28	10	CVE-2024-30224
wireshark_foundation -- wireshark	NetScreen file parser crash in Wireshark 4.0.0 to 4.0.10 and 3.6.0 to 3.6.18 allows denial of service via crafted capture file	2024-03-26	7.8	CVE-2023-6175
wireshark_foundation -- wireshark	T.38 dissector crash in Wireshark 4.2.0 to 4.0.3 and 4.0.0 to 4.0.13 allows denial of service via packet injection or crafted capture file	2024-03-26	7.8	CVE-2024-2955
wixtoolset -- issues	WiX toolset lets developers create installers for Windows Installer, the Windows installation engine. When a bundle runs as SYSTEM user, Burn uses GetTempPathW which points to an insecure directory C:\Windows\Temp to drop and load multiple binaries. Standard users can hijack the binary before it's loaded in the application resulting in elevation of privileges. This vulnerability is fixed in 3.14.1 and 4.0.5.	2024-03-24	7.3	CVE-2024-29187
wixtoolset -- issues	WiX toolset lets developers create installers for Windows Installer, the Windows installation engine. The custom action behind WiX's `RemoveFolderEx` functionality could allow a standard user to delete protected directories. `RemoveFolderEx` deletes an entire directory tree during installation or uninstallation. It does so by recursing every subdirectory starting at a specified directory and adding each subdirectory to the list of directories Windows Installer should delete. If the setup author instructed `RemoveFolderEx` to delete a per-user folder from a per-machine installer, an attacker could create a directory junction in that per-user folder pointing to a per-machine, protected directory. Windows Installer, when executing the per-machine installer after approval by an administrator, would delete the target of the directory junction. This vulnerability is fixed in 3.14.1 and 4.0.5.	2024-03-24	7.9	CVE-2024-29188
wobbie.nl -- doneren_met_mollie	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wobbie.Nl Doneren met Mollie allows Reflected XSS.This issue affects Doneren met Mollie: from n/a through 2.10.2.	2024-03-27	7.1	CVE-2024-29767

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wolfssl -- wolfssl	Remotely executed SEGV and out of bounds read allows malicious packet sender to crash or cause an out of bounds read via sending a malformed packet with the correct length.	2024-03-25	7.5	CVE-2024-0901
wolfssl_inc. -- wolfssh	A vulnerability was found in wolfSSH's server-side state machine before versions 1.4.17. A malicious client could create channels without first performing user authentication, resulting in unauthorized access.	2024-03-25	9.1	CVE-2024-2873
wp_codeus -- advanced_sermons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Codeus Advanced Sermons allows Reflected XSS.This issue affects Advanced Sermons: from n/a through 3.1.	2024-03-27	7.1	CVE-2024-29928
wp_go_maps_(formerly_wp_google_maps) -- wp_google_maps	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Go Maps (formerly WP Google Maps) WP Google Maps allows Reflected XSS.This issue affects WP Google Maps: from n/a through 9.0.29.	2024-03-27	7.1	CVE-2024-29931
wp_lab -- wp-lister_lite_for_amazon	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Lab WP-Lister Lite for Amazon allows Reflected XSS.This issue affects WP-Lister Lite for Amazon: from n/a through 2.6.8.	2024-03-27	7.1	CVE-2024-30199
wp_sunshine -- sunshine_photo_cart	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Sunshine Sunshine Photo Cart allows Reflected XSS.This issue affects Sunshine Photo Cart: from n/a through 3.1.1.	2024-03-27	7.1	CVE-2024-30194
wp_travel_engine -- wp_travel_engine	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP Travel Engine.This issue affects WP Travel Engine: from n/a through 5.7.9.	2024-03-29	9.3	CVE-2024-30502
wp_travel_engine -- wp_travel_engine	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP Travel Engine.This issue affects WP Travel Engine: from n/a through 5.7.9.	2024-03-29	7.6	CVE-2024-30504
wpchill -- download_monitor	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPChill Download Monitor.This issue affects Download Monitor: from n/a through 4.9.4.	2024-03-29	7.6	CVE-2024-30501
wpdevelop_/_oplugins -- booking_calendar	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPdevelop / Oplugins Booking Calendar allows SQL Injection.This issue affects Booking Calendar: from n/a through 9.4.3.	2024-03-26	7.6	CVE-2023-23991
wpdeveloper -- betterdocs	Deserialization of Untrusted Data vulnerability in WPDeveloper BetterDocs.This issue affects BetterDocs: from n/a through 3.3.3.	2024-03-28	9	CVE-2024-30226
wpdevteam -- essential_addons_for_elementor_-_best_elementor_templates,_widgets_kits_&_woocommerce_builders	The Essential Addons for Elementor plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 5.9.13 via deserialization of untrusted input from the 'error_resetpassword' attribute of the "Login | Register Form" widget (disabled by default). This makes it possible for authenticated attackers, with author-level access and above, to inject a PHP Object. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-03-30	8.8	CVE-2024-3018
wpdirectorykit -- wp_directory_kit	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WpDirectoryKit WP Directory Kit allows Reflected XSS.This issue affects WP Directory Kit: from n/a through 1.2.9.	2024-03-27	7.1	CVE-2024-29774
wpengine,_inc. -- wp_migrate	Deserialization of Untrusted Data vulnerability in WPENGINE, INC. WP Migrate.This issue affects WP Migrate: from n/a through 2.6.10.	2024-03-28	10	CVE-2024-30225
wpeverest -- user_registration	Deserialization of Untrusted Data vulnerability in WPEverest User Registration.This issue affects User Registration: from n/a through 2.3.2.1.	2024-03-26	7.4	CVE-2023-27459
wpjobboard -- jobeleon_theme	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPJobBoard Jobeleon Theme allows Reflected XSS.This issue affects Jobeleon Theme: from n/a through 1.9.1.	2024-03-29	7.1	CVE-2022-47153
wpmu_dev -- forminator	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPMU DEV Forminator allows Reflected XSS.This issue affects Forminator: from n/a through 1.29.0.	2024-03-27	7.1	CVE-2024-29777
xpeedstudio -- elementskit_eleme	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.0.6 via the render_raw function. This makes it possible for authenticated attackers, with contributor-level access and	2024-03-30	8.8	CVE-2024-2047

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ntor_addons	above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.			
xylus_themes -- wordpress_importer	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xylus Themes WordPress Importer allows Reflected XSS.This issue affects WordPress Importer: from n/a through 1.0.4.	2024-03-27	7.1	CVE-2024-30201
zachary_segal -- catablog	Unrestricted Upload of File with Dangerous Type vulnerability in Zachary Segal CataBlog.This issue affects CataBlog: from n/a through 1.7.0.	2024-03-26	9.1	CVE-2023-47842
zitadel -- zitadel	ZITADEL users can upload their own avatar image and various image types are allowed. Due to a missing check, an attacker could upload HTML and pretend it is an image to gain access to the victim's account in certain scenarios. A possible victim would need to directly open the supposed image in the browser, where a session in ZITADEL needs to be active for this exploit to work. The exploit could only be reproduced if the victim was using Firefox. Chrome, Safari as well as Edge did not execute the code. This vulnerability is fixed in 2.48.3, 2.47.8, 2.46.5, 2.45.5, 2.44.7, 2.43.11, and 2.42.17.	2024-03-27	8.7	CVE-2024-29891
zoho_campaigns -- zoho_campaigns	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Zoho Campaigns.This issue affects Zoho Campaigns: from n/a through 2.0.6.	2024-03-28	8.5	CVE-2024-30239
zscaler -- client_connector	An arbitrary file deletion in ZSATrayManager where it protects the temporary encrypted ZApp issue reporting file from the unprivileged end user access and modification. Fixed version: Win ZApp 4.3.0 and later.	2024-03-26	7.3	CVE-2023-41969
zscaler -- client_connector	In some rare cases, there is a password type validation missing in Revert Password check and for some features it could be disabled. Fixed Version: Win ZApp 4.3.0.121 and later.	2024-03-26	7.3	CVE-2023-41972
zscaler -- client_connector	ZSATray passes the previousInstallerName as a config parameter to TrayManager, and TrayManager constructs the path and appends previousInstallerName to get the full path of the exe. Fixed Version: Win ZApp 4.3.0.121 and later.	2024-03-26	7.3	CVE-2023-41973
zscaler -- client_connector	The ZScaler service is susceptible to a local privilege escalation vulnerability found in the ZScalerService process. Fixed Version: Mac ZApp 4.2.0.241 and later.	2024-03-26	7	CVE-2024-23482
N/A -- N/A	Directory Traversal vulnerability in Devan-Kerman ARRP v.0.8.1 and before allows a remote attacker to execute arbitrary code via the dumpDirect in RuntimeResourcePackImpl component.	2024-03-19	8.8	CVE-2024-24042
N/A -- N/A	danielmiessler fabric through 1.3.0 allows installer/client/gui/static/js/index.js XSS because of innerHTML mishandling, such as in htmlToPlainText.	2024-03-18	7.4	CVE-2024-29154
aam -- advanced_access_manager	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AAM Advanced Access Manager allows Reflected XSS.This issue affects Advanced Access Manager: from n/a through 6.9.20.	2024-03-19	7.1	CVE-2024-29127
abast -- scan_visio_edocument_suite_web_viewer	A SQL Injection has been found on SCAN_VISIO eDocument Suite Web Viewer of Abast. This vulnerability allows an unauthenticated user to retrieve, update and delete all the information of database. This vulnerability was found on login page via "user" parameter.	2024-03-21	9.8	CVE-2024-29732 cve-
acryldata -- datahub-helm	datahub-helm provides the Kubernetes Helm charts for deploying Datahub and its dependencies on a Kubernetes cluster. Starting in version 0.1.143 and prior to version 0.2.182, due to configuration issues in the helm chart, if there was a successful initial deployment during a limited window of time, personal access tokens were possibly created with a default secret key. Since the secret key is a static, publicly available value, someone could inspect the algorithm used to generate personal access tokens and generate their own for an instance. Deploying with Metadata Service Authentication enabled would have been difficult during window of releases. If someone circumvented the helm settings and manually set Metadata Service Authentication to be enabled using environment variables directly, this would skip over the autogeneration logic for the Kubernetes Secrets and DataHub GMS would default to the signing key specified statically in the application.yml. Most deployments probably did not attempt to circumvent the helm settings to enable Metadata Service Authentication during this time, so impact is most likely limited. Any deployments with Metadata Service Authentication enabled should ensure that their secret values are properly randomized. Version 0.2.182 contains a patch for this issue. As a workaround, one	2024-03-20	9.1	CVE-2024-29037

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	may reset the token signing key to be a random value, which will invalidate active personal access tokens.			
adobe -- animate	Animate versions 24.0, 23.0.3 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.	2024-03-18	7.8	CVE-2024-20761
adobe -- bridge	Bridge versions 13.0.5, 14.0.1 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.	2024-03-18	7.8	CVE-2024-20752
adobe -- bridge	Bridge versions 13.0.5, 14.0.1 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.	2024-03-18	7.8	CVE-2024-20755
adobe -- bridge	Bridge versions 13.0.5, 14.0.1 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.	2024-03-18	7.8	CVE-2024-20756
adobe -- coldfusion	ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Access Control vulnerability that could lead to arbitrary file system read. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized access to sensitive files and perform arbitrary file system write. Exploitation of this issue does not require user interaction.	2024-03-18	8.2	CVE-2024-20767
adobe -- lightroom_desktop	Lightroom Desktop versions 7.1.2 and earlier are affected by an Untrusted Search Path vulnerability that could result in arbitrary code execution in the context of the current user. If the application uses a search path to locate critical resources such as programs, then an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-03-18	7.5	CVE-2024-20754
adobe -- premiere_pro	Premiere Pro versions 24.1, 23.6.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-03-18	7.8	CVE-2024-20745
adobe -- premiere_pro	Premiere Pro versions 24.1, 23.6.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-03-18	7.8	CVE-2024-20746
amssplus -- amss++	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/book/main/select_send.php, in the 'sd_index' parameter. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	2024-03-18	8.2	CVE-2024-2584 cve-
amssplus -- amss++	File upload restriction evasion vulnerability in AMSS++ version 4.31. This vulnerability could allow an authenticated user to potentially obtain RCE through webshell, compromising the entire infrastructure.	2024-03-18	9.9	CVE-2024-2599 cve-
amssplus -- amss++	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/book/main/select_send_2.php, in the 'sd_index' parameter. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	2024-03-18	8.2	CVE-2024-2585 cve-
amssplus -- amss++	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/index.php, in the 'username' parameter. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	2024-03-18	8.2	CVE-2024-2586 cve-
amssplus -- amss++	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/book/main/bookdetail_khet_person.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	2024-03-18	8.2	CVE-2024-2587 cve-
amssplus -- amss++	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/admin/index.php, in the 'id' parameter. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	2024-03-18	8.2	CVE-2024-2588 cve-
amssplus -- amss++	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/book/main/bookdetail_school_person.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	2024-03-18	8.2	CVE-2024-2589 cve-

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
amssplus -- amss++	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/mail/main/select_send.php, in the 'sd_index' parameter. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	2024-03-18	8.2	CVE-2024-2590 cve-
amssplus -- amss++	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/book/main/bookdetail_group.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	2024-03-18	8.2	CVE-2024-2591 cve-
amssplus -- amss++	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/person/pic_show.php, in the 'person_id' parameter. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	2024-03-18	8.2	CVE-2024-2592 cve-
amssplus -- amss++	Vulnerability in AMSS++ version 4.31, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /amssplus/modules/book/main/bookdetail_group.php, in the 'b_id' parameter. This vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-03-18	7.1	CVE-2024-2593 cve-
amssplus -- amss++	Vulnerability in AMSS++ version 4.31, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /amssplus/admin/index.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-03-18	7.1	CVE-2024-2594 cve-
amssplus -- amss++	Vulnerability in AMSS++ version 4.31, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /amssplus/modules/book/main/bookdetail_khet_person.php, in the 'b_id' parameter. This vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-03-18	7.1	CVE-2024-2595 cve-
amssplus -- amss++	Vulnerability in AMSS++ version 4.31, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /amssplus/modules/mail/main/select_send.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-03-18	7.1	CVE-2024-2596 cve-
amssplus -- amss++	Vulnerability in AMSS++ version 4.31, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /amssplus/modules/book/main/bookdetail_school_person.php, in the 'b_id' parameter. This vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-03-18	7.1	CVE-2024-2597 cve-
amssplus -- amss++	Vulnerability in AMSS++ version 4.31, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /amssplus/modules/book/main/select_send_2.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	2024-03-18	7.1	CVE-2024-2598 cve-
apollographql -- router	The Apollo Router is a graph router written in Rust to run a federated supergraph that uses Apollo Federation. Versions 0.9.5 until 1.40.2 are subject to a Denial-of-Service (DoS) type vulnerability. When receiving compressed HTTP payloads, affected versions of the Router evaluate the `limits.http_max_request_bytes` configuration option after the entirety of the compressed payload is decompressed. If affected versions of the Router receive highly compressed payloads, this could result in significant memory consumption while the compressed payload is expanded. Router version 1.40.2 has a fix for the vulnerability. Those who are unable to upgrade may be able to implement mitigations at proxies or load balancers positioned in front of their Router fleet (e.g. Nginx, HAProxy, or cloud-native WAF services) by creating limits on HTTP body upload size.	2024-03-21	7.5	CVE-2024-28101
argoproj -- argo_cd	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Prior to versions 2.8.13, 2.9.9, and 2.10.4, an attacker can exploit a chain of vulnerabilities, including a Denial of Service (DoS) flaw and in-memory data storage weakness, to effectively bypass the application's brute force login protection. This is a critical security vulnerability that allows attackers to bypass the brute force login protection mechanism. Not only can they crash the service affecting all users, but they can also make unlimited login attempts, increasing the risk of account compromise. Versions 2.8.13, 2.9.9, and 2.10.4 contain a patch for this issue.	2024-03-18	9.8	CVE-2024-21652
argoproj -- argo_cd	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Prior to versions 2.8.13, 2.9.9, and 2.10.4, an attacker can exploit a critical flaw in the application to initiate a Denial of Service (DoS) attack, rendering the application	2024-03-18	7.5	CVE-2024-21661

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	inoperable and affecting all users. The issue arises from unsafe manipulation of an array in a multi-threaded environment. The vulnerability is rooted in the application's code, where an array is being modified while it is being iterated over. This is a classic programming error but becomes critically unsafe when executed in a multi-threaded environment. When two threads interact with the same array simultaneously, the application crashes. This is a Denial of Service (DoS) vulnerability. Any attacker can crash the application continuously, making it impossible for legitimate users to access the service. The issue is exacerbated because it does not require authentication, widening the pool of potential attackers. Versions 2.8.13, 2.9.9, and 2.10.4 contain a patch for this issue.			
argoproj -- argo_cd	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Prior to versions 2.8.13, 2.9.9, and 2.10.4, an attacker can effectively bypass the rate limit and brute force protections by exploiting the application's weak cache-based mechanism. This loophole in security can be combined with other vulnerabilities to attack the default admin account. This flaw undermines a patch for CVE-2020-8827 intended to protect against brute-force attacks. The application's brute force protection relies on a cache mechanism that tracks login attempts for each user. This cache is limited to a `defaultMaxCacheSize` of 1000 entries. An attacker can overflow this cache by bombarding it with login attempts for different users, thereby pushing out the admin account's failed attempts and effectively resetting the rate limit for that account. This is a severe vulnerability that enables attackers to perform brute force attacks at an accelerated rate, especially targeting the default admin account. Users should upgrade to version 2.8.13, 2.9.9, or 2.10.4 to receive a patch.	2024-03-18	7.5	CVE-2024-21662
astropy -- astropy	Astropy is a project for astronomy in Python that fosters interoperability between Python astronomy packages. Version 5.3.2 of the Astropy core package is vulnerable to remote code execution due to improper input validation in the `TranformGraph().to_dot_graph` function. A malicious user can provide a command or a script file as a value to the `savelayout` argument, which will be placed as the first value in a list of arguments passed to `subprocess.Popen`. Although an error will be raised, the command or script will be executed successfully. Version 5.3.3 fixes this issue.	2024-03-18	8.4	CVE-2023-41334
cegid -- meta4_hr	An Unrestricted Upload of File vulnerability has been found on Cegid Meta4 HR, that allows an attacker to upload malicios files to the server via '/config/espanol/update_password.jsp' file. Modifying the 'M4_NEW_PASSWORD' parameter, an attacker could store a malicious JSP file inside the file directory, to be executed the the file is loaded in the application.	2024-03-19	9	CVE-2024-2636 cve-
cegid -- meta4_hr	A Information Exposure Vulnerability has been found on Meta4 HR. This vulnerability allows an attacker to obtain a lot of information about the application such as the variables set in the process, the Tomcat versions, library versions and underlying operation system via HTTP GET '/sitetest/english/dumpenv.jsp'.	2024-03-19	7.5	CVE-2024-2632 cve-
cegid -- meta4_hr	The configuration pages available are not intended to be placed on an Internet facing web server, as they expose file paths to the client, who can be an attacker. Instead of rewriting these pages to avoid this vulnerability, they will be dismissed from future releases of Cegid Meta4 HR, as they do not offer product functionality	2024-03-19	7.3	CVE-2024-2635 cve-
checkmk_gmbh -- checkmk	Least privilege violation in the Checkmk agent plugins mk_oracle, mk_oracle.ps1, and mk_oracle_crs before Checkmk 2.3.0b4 (beta), 2.2.0p24, 2.1.0p41 and 2.0.0 (EOL) allows local users to escalate privileges.	2024-03-22	8.2	CVE-2024-0638
checkmk_gmbh -- checkmk	Least privilege violation and reliance on untrusted inputs in the mk_informix Checkmk agent plugin before Checkmk 2.3.0b4 (beta), 2.2.0p24, 2.1.0p41 and 2.0.0 (EOL) allows local users to escalate privileges.	2024-03-22	8.8	CVE-2024-28824
chirp_systems -- chirp_access	Chirp Access improperly stores credentials within its source code, potentially exposing sensitive information to unauthorized access.	2024-03-20	9.1	CVE-2024-2197
ciges -- cigesv2	SQL injection vulnerability in the CIGESv2 system, through /ajaxConfigTotem.php, in the 'id' parameter. The exploitation of this vulnerability could allow a remote user to retrieve all data stored in the database by sending a specially crafted SQL query.	2024-03-22	9.8	CVE-2024-2722 cve-
ciges -- cigesv2	SQL injection vulnerability in the CIGESv2 system, through /ajaxSubServicios.php, in the 'idServicio' parameter. The exploitation of this vulnerability could allow a remote user to retrieve all data stored in the database by sending a specially crafted SQL query.	2024-03-22	9.8	CVE-2024-2723 cve-
ciges -- cigesv2	SQL injection vulnerability in the CIGESv2 system, through /ajaxServiciosAtencion.php, in the 'idServicio' parameter. The exploitation	2024-03-22	9.8	CVE-2024-2724 cve-

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of this vulnerability could allow a remote user to retrieve all data stored in the database by sending a specially crafted SQL query.			
ciges -- cigesv2	Information exposure vulnerability in the CIGESv2 system. A remote attacker might be able to access /vendor/composer/installed.json and retrieve all installed packages used by the application.	2024-03-22	7.5	CVE-2024-2725 cve-
cilium -- cilium	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Starting in version 1.13.9 and prior to versions 1.13.13, 1.14.8, and 1.15.2, Cilium's HTTP policies are not consistently applied to all traffic in the scope of the policies, leading to HTTP traffic being incorrectly and intermittently forwarded when it should be dropped. This issue has been patched in Cilium 1.15.2, 1.14.8, and 1.13.13. There are no known workarounds for this issue.	2024-03-18	7.2	CVE-2024-28248
cimatti_consulting -- contact_forms_by_cimatti	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cimatti Consulting Contact Forms by Cimatti allows Stored XSS.This issue affects Contact Forms by Cimatti: from n/a through 1.7.0.	2024-03-19	7.1	CVE-2024-29117
codekraft -- antispam_for_contact_form_7	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Codekraft AntiSpam for Contact Form 7 allows Reflected XSS.This issue affects AntiSpam for Contact Form 7: from n/a through 0.6.0.	2024-03-17	7.1	CVE-2024-27961
coder -- coder	Coder allows oragnizations to provision remote development environments via Terraform. Prior to versions 2.6.1, 2.7.3, and 2.8.4, a vulnerability in Coder's OIDC authentication could allow an attacker to bypass the `CODER_OIDC_EMAIL_DOMAIN` verification and create an account with an email not in the allowlist. Deployments are only affected if the OIDC provider allows users to create accounts on the provider. During OIDC registration, the user's email was improperly validated against the allowed `CODER_OIDC_EMAIL_DOMAIN`s. This could allow a user with a domain that only partially matched an allowed domain to successfully login or register. An attacker could register a domain name that exploited this vulnerability and register on a Coder instance with a public OIDC provider. Coder instances with OIDC enabled and protected by the `CODER_OIDC_EMAIL_DOMAIN` configuration are affected. Coder instances using a private OIDC provider are not affected, as arbitrary users cannot register through a private OIDC provider without first having an account on the provider. Public OIDC providers are impacted. GitHub authentication and external authentication are not impacted. This vulnerability is remedied in versions 2.8.4, 2.7.3, and 2.6.1 All versions prior to these patches are affected by the vulnerability.*It is recommended that customers upgrade their deployments as soon as possible if they are utilizing OIDC authentication with the `CODER_OIDC_EMAIL_DOMAIN` setting.	2024-03-21	8.2	CVE-2024-27918
dassault_syst-mes -- solidworks_desktop	Heap-based Buffer Overflow, Memory Corruption, Out-Of-Bounds Read, Out-Of-Bounds Write, Stack-based Buffer Overflow, Type Confusion, Uninitialized Variable, Use-After-Free vulnerabilities exist in the file reading procedure in SOLIDWORKS Desktop on Release SOLIDWORKS 2024. These vulnerabilities could allow an attacker to execute arbitrary code while opening a specially crafted CATPART, DWG, DXF, IPT, JT, SAT, SLDDRW, SLDPRT, STL, STP, X_B or X_T file.	2024-03-22	7.8	CVE-2024-1848 3DS.Information-Security@3ds.com
dell -- poweredge_platform	Dell PowerEdge Server BIOS contains a heap-based buffer overflow vulnerability. A local high privileged attacker could potentially exploit this vulnerability to write to otherwise unauthorized memory.	2024-03-19	7.2	CVE-2024-22453
delta_electronics -- diaenergie	SQL injection vulnerability exists in GetDIAE_unListParameters.	2024-03-21	8.8	CVE-2024-23494
delta_electronics -- diaenergie	SQL injection vulnerability exists in GetDIAE_slogListParameters.	2024-03-21	8.8	CVE-2024-23975
delta_electronics -- diaenergie	Path traversal attack is possible and write outside of the intended directory and may access sensitive information. If a file name is specified that already exists on the file system, then the original file will be overwritten.	2024-03-21	8.1	CVE-2024-25567
delta_electronics -- diaenergie	SQL injection vulnerability exists in the script DIAE_tagHandler.ashx.	2024-03-21	8.8	CVE-2024-25937
delta_electronics -- diaenergie	Privileges are not fully verified server-side, which can be abused by a user with limited privileges to bypass authorization and access privileged functionality.	2024-03-21	8.8	CVE-2024-28029

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
delta_electronics -- diaenergie	SQL injection vulnerability exists in GetDIAE_astListParameters.	2024-03-21	8.8	CVE-2024-28040
delta_electronics -- diaenergie	It is possible to perform a path traversal attack and write outside of the intended directory. If a file name is specified that already exists on the file system, then the original file will be overwritten.	2024-03-21	8.1	CVE-2024-28171
delta_electronics -- diaenergie	SQL injection vulnerability exists in the script Handler_CFG.ashx.	2024-03-21	8.8	CVE-2024-28891
denoland -- deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. In version 1.39.0, use of raw file descriptors in `op_node_ipc_pipe()` leads to premature close of arbitrary file descriptors, allowing standard input to be re-opened as a different resource resulting in permission prompt bypass. Node child_process IPC relies on the JS side to pass the raw IPC file descriptor to `op_node_ipc_pipe()`, which returns a `IpcJsonStreamResource` ID associated with the file descriptor. On closing the resource, the raw file descriptor is closed together. Use of raw file descriptors in `op_node_ipc_pipe()` leads to premature close of arbitrary file descriptors. This allow standard input (fd 0) to be closed and re-opened for a different resource, which allows a silent permission prompt bypass. This is exploitable by an attacker controlling the code executed inside a Deno runtime to obtain arbitrary code execution on the host machine regardless of permissions. This bug is known to be exploitable. There is a working exploit that achieves arbitrary code execution by bypassing prompts from zero permissions, additionally abusing the fact that Cache API lacks filesystem permission checks. The attack can be conducted silently as stderr can also be closed, suppressing all prompt outputs. Version 1.39.1 fixes the bug.	2024-03-21	8.2	CVE-2024-27933
denoland -- deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Starting in version 1.36.2 and prior to version 1.40.3, use of inherently unsafe `*const c_void` and `ExternalPointer` leads to use-after-free access of the underlying structure, resulting in arbitrary code execution. Use of inherently unsafe `*const c_void` and `ExternalPointer` leads to use-after-free access of the underlying structure, which is exploitable by an attacker controlling the code executed inside a Deno runtime to obtain arbitrary code execution on the host machine regardless of permissions. This bug is known to be exploitable for both `*const c_void` and `ExternalPointer` implementations. Version 1.40.3 fixes this issue.	2024-03-21	8.4	CVE-2024-27934
denoland -- deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime with secure defaults. Starting in version 1.32.1 and prior to version 1.41 of the deno_runtime library, maliciously crafted permission request can show the spoofed permission prompt by inserting a broken ANSI escape sequence into the request contents. Deno is stripping any ANSI escape sequences from the permission prompt, but permissions given to the program are based on the contents that contain the ANSI escape sequences. Any Deno program can spoof the content of the interactive permission prompt by inserting a broken ANSI code, which allows a malicious Deno program to display the wrong file path or program name to the user. Version 1.41 of the deno_runtime library contains a patch for the issue.	2024-03-21	8.8	CVE-2024-27936
denoland -- deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Starting in version 1.35.1 and prior to version 1.36.3, a vulnerability in Deno's Node.js compatibility runtime allows for cross-session data contamination during simultaneous asynchronous reads from Node.js streams sourced from sockets or files. The issue arises from the re-use of a global buffer (BUF) in stream_wrap.ts used as a performance optimization to limit allocations during these asynchronous read operations. This can lead to data intended for one session being received by another session, potentially resulting in data corruption and unexpected behavior. This affects all users of Deno that use the node.js compatibility layer for network communication or other streams, including packages that may require node.js libraries indirectly. Version 1.36.3 contains a patch for this issue.	2024-03-21	7.2	CVE-2024-27935
dev_institute -- restrict_user_access_-_membership_plugin_with_force	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DEV Institute Restrict User Access - Membership Plugin with Force allows Reflected XSS.This issue affects Restrict User Access - Membership Plugin with Force: from n/a through 2.5.	2024-03-19	7.1	CVE-2024-29138
django-wiki -- django-wiki	django-wiki is a wiki system for Django. Installations of django-wiki prior to version 0.10.1 are vulnerable to maliciously crafted article content that can cause severe	2024-03-18	7.5	CVE-2024-28865

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	use of server CPU through a regular expression loop. Version 0.10.1 fixes this issue. As a workaround, close off access to create and edit articles by anonymous users.			
dnesscarkey -- wp_armour_-_honeypot_anti_spam	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dnesscarkey WP Armour - Honeypot Anti Spam allows Reflected XSS.This issue affects WP Armour - Honeypot Anti Spam: from n/a through 2.1.13.	2024-03-19	7.1	CVE-2024-29091
elliot_sowersby,_relywp -- coupon_affiliates	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Elliot Sowersby, RelyWP Coupon Affiliates allows Reflected XSS.This issue affects Coupon Affiliates: from n/a through 5.12.7.	2024-03-19	7.1	CVE-2024-29125
eprosima -- fast_dds	eprosima Fast DDS is a C++ implementation of the Data Distribution Service standard of the Object Management Group. Prior to versions 2.14.0, 2.13.4, 2.12.3, 2.10.4, and 2.6.8, manipulated DATA Submessage can cause a heap overflow error in the Fast-DDS process, causing the process to be terminated remotely. Additionally, the payload_size in the DATA Submessage packet is declared as uint32_t. When a negative number, such as -1, is input into this variable, it results in an Integer Overflow (for example, -1 gets converted to 0xFFFFFFFF). This eventually leads to a heap-buffer-overflow, causing the program to terminate. Versions 2.14.0, 2.13.4, 2.12.3, 2.10.4, and 2.6.8 contain a fix for this issue.	2024-03-20	9.6	CVE-2024-28231
evergreen_content_poster -- evergreen_content_poster	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Evergreen Content Poster allows Reflected XSS.This issue affects Evergreen Content Poster: from n/a through 1.4.1.	2024-03-19	7.1	CVE-2024-29099
firassaidi -- woocommerce_license_manager	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Firassaidi WooCommerce License Manager allows Reflected XSS.This issue affects WooCommerce License Manager: from n/a through 5.3.1.	2024-03-19	7.1	CVE-2024-29121
firebirdsql -- firebird	Firebird is a relational database. Versions 4.0.0 through 4.0.3 and version 5.0 beta1 are vulnerable to a server crash when a user uses a specific form of SET BIND statement. Any non-privileged user with minimum access to a server may type a statement with a long `CHAR` length, which causes the server to crash due to stack corruption. Versions 4.0.4.2981 and 5.0.0.117 contain fixes for this issue. No known workarounds are available.	2024-03-20	7.5	CVE-2023-41038
florian_'fkrauthan'_krauthan -- wp_mpdf	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Florian 'fkrauthan' Krauthan allows Reflected XSS.This issue affects wp-mpdf: from n/a through 3.7.1.	2024-03-21	7.1	CVE-2024-27962
franklin_fueling_system -- evo_550	Franklin Fueling System EVO 550 and EVO 5000 are vulnerable to a Path Traversal vulnerability that could allow an attacker to access sensitive files on the system.	2024-03-19	7.5	CVE-2024-2442
frappe -- frappe	Frappe is a full-stack web application framework. Prior to versions 14.66.3 and 15.16.0, file permission can be bypassed using certain endpoints, granting less privileged users permission to delete or clone a file. Versions 14.66.3 and 15.16.0 contain a patch for this issue. No known workarounds are available.	2024-03-21	8.1	CVE-2024-27105
frappe -- frappe	Frappe is a full-stack web application framework. Prior to versions 14.64.0 and 15.0.0, SQL injection from a particular whitelisted method can result in access to data which the user doesn't have permission to access. Versions 14.64.0 and 15.0.0 contain a patch for this issue. No known workarounds are available.	2024-03-21	7.5	CVE-2024-24813
freescout-helpdesk -- freescout	FreeScout is a self-hosted help desk and shared mailbox. Versions prior to 1.8.128 are vulnerable to OS Command Injection in the /public/tools.php source file. The value of the php_path parameter is being executed as an OS command by the shell_exec function, without validating it. This allows an adversary to execute malicious OS commands on the server. A practical demonstration of the successful command injection attack extracted the /etc/passwd file of the server. This represented the complete compromise of the server hosting the FreeScout application. This attack requires an attacker to know the `App_Key` of the application. This limitation makes the Attack Complexity to be High. If an attacker gets hold of the `App_Key`, the attacker can compromise the Complete server on which the application is deployed. Version 1.8.128 contains a patch for this issue.	2024-03-22	9	CVE-2024-29185
freescout-helpdesk -- freescout	FreeScout is a self-hosted help desk and shared mailbox. A Stored Cross-Site Scripting (XSS) vulnerability has been identified within the Signature Input Field of the FreeScout Application prior to version 1.8.128. Stored XSS occurs when user input is not properly sanitized and is stored on the server, allowing an attacker to	2024-03-22	8	CVE-2024-29184

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	inject malicious scripts that will be executed when other users access the affected page. In this case, the Support Agent User can inject malicious scripts into their signature, which will then be executed when viewed by the Administrator. The application protects users against XSS attacks by enforcing a CSP policy, the CSP Policy is: `script-src 'self' 'nonce-abcd' `. The CSP policy only allows the inclusion of JS files that are present on the application server and doesn't allow any inline script or script other than nonce-abcd. The CSP policy was bypassed by uploading a JS file to the server by a POST request to /conversation/upload endpoint. After this, a working XSS payload was crafted by including the uploaded JS file link as the src of the script. This bypassed the CSP policy and XSS attacks became possible. The impact of this vulnerability is severe as it allows an attacker to compromise the FreeScout Application. By exploiting this vulnerability, the attacker can perform various malicious actions such as forcing the Administrator to execute actions without their knowledge or consent. For instance, the attacker can force the Administrator to add a new administrator controlled by the attacker, thereby giving the attacker full control over the application. Alternatively, the attacker can elevate the privileges of a low-privileged user to Administrator, further compromising the security of the application. Attackers can steal sensitive information such as login credentials, session tokens, personal identifiable information (PII), and financial data. The vulnerability can also lead to defacement of the Application. Version 1.8.128 contains a patch for this issue.			
friendsofsymfony1 -- symfony1	Symfony 1 is a community-driven fork of the 1.x branch of Symfony, a PHP framework for web projects. Starting in version 1.1.0 and prior to version 1.5.19, Symfony 1 has a gadget chain due to dangerous deserialization in `sfNamespacedParameterHolder` class that would enable an attacker to get remote code execution if a developer deserializes user input in their project. Version 1.5.19 contains a patch for the issue.	2024-03-22	9.8	CVE-2024-28861
fujian_kelixin_communication -- command_and_dispatch_platform	A vulnerability was found in Fujian Kelixin Communication Command and Dispatch Platform up to 20240313. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file api/client/get_extension_yl.php. The manipulation of the argument imei leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257065 was assigned to this vulnerability.	2024-03-17	7.3	CVE-2024-2566
geoserver -- geoserver	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A path traversal vulnerability in versions 2.23.4 and prior requires GeoServer Administrator with access to the admin console to misconfigure the Global Settings for log file location to an arbitrary location. The admin console GeoServer Logs page provides a preview of these contents. As this issue requires GeoServer administrators access, often representing a trusted party, the vulnerability has not received a patch as of time of publication. As a workaround, a system administrator responsible for running GeoServer can use the `GEOSERVER_LOG_FILE` setting to override any configuration option provided by the Global Settings page. The `GEOSERVER_LOG_LOCATION` parameter can be set as system property, environment variables, or servlet context parameters.	2024-03-20	7.2	CVE-2023-41877
geoserver -- geoserver	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. An arbitrary file upload vulnerability exists in versions prior to 2.23.4 and 2.24.1 that enables an authenticated administrator with permissions to modify coverage stores through the REST Coverage Store API to upload arbitrary file contents to arbitrary file locations which can lead to remote code execution. Coverage stores that are configured using relative paths use a GeoServer Resource implementation that has validation to prevent path traversal but coverage stores that are configured using absolute paths use a different Resource implementation that does not prevent path traversal. This vulnerability can lead to executing arbitrary code. An administrator with limited privileges could also potentially exploit this to overwrite GeoServer security files and obtain full administrator privileges. Versions 2.23.4 and 2.24.1 contain a fix for this issue.	2024-03-20	7.2	CVE-2023-51444
gesundheit_beweg t_gmbh -- zippy	Unrestricted Upload of File with Dangerous Type vulnerability in Gesundheit Bewegt GmbH Zippy.This issue affects Zippy: from n/a through 1.6.9.	2024-03-21	8.8	CVE-2024-27964
getgrav -- grav	Grav is an open-source, flat-file content management system. A file upload path traversal vulnerability has been identified in the application prior to version 1.7.45, enabling attackers to replace or create files with extensions like .json, .zip, .css, .gif, etc. This critical security flaw poses severe risks, that can allow attackers to inject arbitrary code on the server, undermine integrity of backup files by overwriting	2024-03-21	8.8	CVE-2024-27921

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	existing files or creating new ones, and exfiltrate sensitive data using CSS exfiltration techniques. Upgrading to patched version 1.7.45 can mitigate the issue.			
getgrav -- grav	Grav is a content management system (CMS). Prior to version 1.7.43, users who may write a page may use the `frontmatter` feature due to insufficient permission validation and inadequate file name validation. This may lead to remote code execution. Version 1.7.43 fixes this issue.	2024-03-21	8.8	CVE-2024-27923
getgrav -- grav	Grav is an open-source, flat-file content management system. Grav CMS prior to version 1.7.45 is vulnerable to a Server-Side Template Injection (SSTI), which allows any authenticated user (editor permissions are sufficient) to execute arbitrary code on the remote server bypassing the existing security sandbox. Version 1.7.45 contains a patch for this issue.	2024-03-21	8.8	CVE-2024-28116
getgrav -- grav	Grav is an open-source, flat-file content management system. Prior to version 1.7.45, Grav validates accessible functions through the Utils::isDangerousFunction function, but does not impose restrictions on twig functions like twig_array_map, allowing attackers to bypass the validation and execute arbitrary commands. Twig processing of static pages can be enabled in the front matter by any administrative user allowed to create or edit pages. As the Twig processor runs unsandboxed, this behavior can be used to gain arbitrary code execution and elevate privileges on the instance. Upgrading to patched version 1.7.45 can mitigate this issue.	2024-03-21	8.8	CVE-2024-28117
getgrav -- grav	Grav is an open-source, flat-file content management system. Prior to version 1.7.45, due to the unrestricted access to twig extension class from Grav context, an attacker can redefine config variable. As a result, attacker can bypass a previous SSTI mitigation. Twig processing of static pages can be enabled in the front matter by any administrative user allowed to create or edit pages. As the Twig processor runs unsandboxed, this behavior can be used to gain arbitrary code execution and elevate privileges on the instance. Version 1.7.45 contains a fix for this issue.	2024-03-21	8.8	CVE-2024-28118
getgrav -- grav	Grav is an open-source, flat-file content management system. Prior to version 1.7.45, due to the unrestricted access to twig extension class from grav context, an attacker can redefine the escape function and execute arbitrary commands. Twig processing of static pages can be enabled in the front matter by any administrative user allowed to create or edit pages. As the Twig processor runs unsandboxed, this behavior can be used to gain arbitrary code execution and elevate privileges on the instance. Version 1.7.45 contains a patch for this issue.	2024-03-21	8.8	CVE-2024-28119
github -- enterprise_server	An attacker with an Administrator role in GitHub Enterprise Server could gain SSH root access via remote code execution. This vulnerability affected GitHub Enterprise Server version 3.8.0 and above and was fixed in version 3.8.17, 3.9.12, 3.10.9, 3.11.7 and 3.12.1. This vulnerability was reported via the GitHub Bug Bounty program.	2024-03-20	8	CVE-2024-2469
github -- github_enterprise_server	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance when configuring GeoJSON settings. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.13 and was fixed in versions 3.8.17, 3.9.12, 3.10.9, 3.11.7, and 3.12.1. This vulnerability was reported via the GitHub Bug Bounty program.	2024-03-20	9.1	CVE-2024-2443
glpi-project -- glpi	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. An authenticated user can exploit a SQL injection vulnerability in the search engine to extract data from the database. This issue has been patched in version 10.0.13.	2024-03-18	7.7	CVE-2024-27096
hasthemes -- extensions_for_cf7	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasThemes Extensions For CF7 allows Stored XSS.This issue affects Extensions For CF7: from n/a through 3.0.6.	2024-03-19	7.1	CVE-2024-29102
hasthemes -- ht_easy_ga4_(_google_analytics_4_)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasThemes HT Easy GA4 (Google Analytics 4) allows Stored XSS.This issue affects HT Easy GA4 (Google Analytics 4): from n/a through 1.1.7.	2024-03-19	7.1	CVE-2024-29094
i_thirteen_web_solution -- email_subscription_popup	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in I Thirteen Web Solution Email Subscription Popup allows Stored XSS.This issue affects Email Subscription Popup: from n/a through 1.2.20.	2024-03-17	7.1	CVE-2024-27960
ibm -- cloud_pak_for_aut	IBM Cloud Pak for Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is potentially vulnerable to	2024-03-21	7	CVE-2023-35899

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
omation	CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 259354.			
iconicwp -- woothumbs_for_woocommerce_by_iconic	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in IconicWP WooThumbs for WooCommerce by Iconic allows Reflected XSS.This issue affects WooThumbs for WooCommerce by Iconic: from n/a through 5.5.3.	2024-03-19	7.1	CVE-2024-29116
israelb1 -- management_app_for_woocommerce_-_order_notifications,_order_management,_lead_management,_uptime_monitoring	The Management App for WooCommerce - Order notifications, Order management, Lead management, Uptime Monitoring plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the nouvello_upload_csv_file function in all versions up to, and including, 1.2.0. 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.	2024-03-20	8.8	CVE-2024-1205
jens-maus -- raspberrymatic	RaspberryMatic is an open-source operating system for HomeMatic internet-of-things devices. RaspberryMatic / OCCU prior to version 3.75.6.20240316 contains a unauthenticated remote code execution (RCE) vulnerability, caused by multiple issues within the Java based `HMIPServer.jar` component. RaspberryMatric includes a Java based `HMIPServer`, that can be accessed through URLs starting with `/pages/jpages`. The `FirmwareController` class does however not perform any session id checks, thus this feature can be accessed without a valid session. Due to this issue, attackers can gain remote code execution as root user, allowing a full system compromise. Version 3.75.6.20240316 contains a patch.	2024-03-18	10	CVE-2024-24578
jhpyle -- docassemble	Docassemble is an expert system for guided interviews and document assembly. The vulnerability allows attackers to gain unauthorized access to information on the system through URL manipulation. It affects versions 1.4.53 to 1.4.96. The vulnerability has been patched in version 1.4.97 of the master branch.	2024-03-21	7.5	CVE-2024-27292
jose_mortellaro -- specific_content_for_mobile_-_customize_the_mobile_version_without_redirections	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jose Mortellaro Specific Content For Mobile - Customize the mobile version without redirections allows Reflected XSS.This issue affects Specific Content For Mobile - Customize the mobile version without redirections: from n/a through 0.1.9.5.	2024-03-19	7.1	CVE-2024-29126
jupyterhub -- jupyter-server-proxy	Jupyter Server Proxy allows users to run arbitrary external processes alongside their Jupyter notebook servers and provides authenticated web access. Prior to versions 3.2.3 and 4.1.1, Jupyter Server Proxy did not check user authentication appropriately when proxying websockets, allowing unauthenticated access to anyone who had network access to the Jupyter server endpoint. This vulnerability can allow unauthenticated remote access to any websocket endpoint set up to be accessible via Jupyter Server Proxy. In many cases, this leads to remote unauthenticated arbitrary code execution, due to how affected instances use websockets. The websocket endpoints exposed by `jupyter_server` itself is not affected. Projects that do not rely on websockets are also not affected. Versions 3.2.3 and 4.1.1 contain a fix for this issue.	2024-03-20	9	CVE-2024-28179
jupyterhub -- oauthenticator	OAuthenticator provides plugins for JupyterHub to use common OAuth providers, as well as base classes for writing one's own Authenticators with any OAuth 2.0 provider. `GoogleOAuthenticator.hosted_domain` is used to restrict what Google accounts can be authorized access to a JupyterHub. The restriction is intented to be to Google accounts part of one or more Google organization verified to control specified domain(s). Prior to version 16.3.0, the actual restriction has been to Google accounts with emails ending with the domain. Such accounts could have been created by anyone which at one time was able to read an email associated with the domain. This was described by Dylan Ayrey (@dxa4481) in this [blog post] from 15th December 2023). OAuthenticator 16.3.0 contains a patch for this issue. As a workaround, restrict who can login another way, such as `allowed_users` or `allowed_google_groups`.	2024-03-20	7.5	CVE-2024-29033
kiloview -- ndi	Use of Hard-coded Credentials in Kiloview NDI allows un-authenticated users to bypass authenticationThis issue affects Kiloview NDI N3, N3-s, N4, N20, N30, N40 and was fixed in Firmware version 2.02.0227 .	2024-03-21	9.8	CVE-2024-2161

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kiloview -- ndi	An OS Command Injection vulnerability in Kiloview NDI allows a low-privileged user to execute arbitrary code remotely on the device with high privileges. This issue affects Kiloview NDI N3, N3-s, N4, N20, N30, N40 and was fixed in Firmware version 2.02.0227 .	2024-03-21	8.8	CVE-2024-2162
ldapaccountmanager -- lam	LDAP Account Manager (LAM) is a webfrontend for managing entries stored in an LDAP directory. LAM's log configuration allows to specify arbitrary paths for log files. Prior to version 8.7, an attacker could exploit this by creating a PHP file and cause LAM to log some PHP code to this file. When the file is then accessed via web the code would be executed. The issue is mitigated by the following: An attacker needs to know LAM's master configuration password to be able to change the main settings; and the webserver needs write access to a directory that is accessible via web. LAM itself does not provide any such directories. The issue has been fixed in 8.7. As a workaround, limit access to LAM configuration pages to authorized users.	2024-03-18	7.9	CVE-2024-23333
maciej_bis -- permalink_manager_lite	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Maciej Bis Permalink Manager Lite allows Reflected XSS.This issue affects Permalink Manager Lite: from n/a through 2.4.3.	2024-03-19	7.1	CVE-2024-29092
mark_tilly -- mycurator_content_curation	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mark Tilly MyCurator Content Curation allows Reflected XSS.This issue affects MyCurator Content Curation: from n/a through 3.76.	2024-03-19	7.1	CVE-2024-29139
mediavine -- create_by_mediavine	The Create by Mediavine plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 1.9.4 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.	2024-03-20	9.8	CVE-2024-1711
meshery -- meshery	Meshery is an open source, cloud native manager that enables the design and management of Kubernetes-based infrastructure and applications. A SQL injection vulnerability in Meshery prior to version 0.7.17 allows a remote attacker to obtain sensitive information via the `order` parameter of `GetMeshSyncResources`. Version 0.7.17 contains a patch for this issue.	2024-03-21	7.5	CVE-2024-29031
metagauss -- eventprime	Missing Authorization vulnerability in Metagauss EventPrime.This issue affects EventPrime: from n/a through 3.3.9.	2024-03-23	8.2	CVE-2024-24832
metagauss -- registrationmagic	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Metagauss RegistrationMagic allows Reflected XSS.This issue affects RegistrationMagic: from n/a through 5.2.5.9.	2024-03-19	7.1	CVE-2024-29113
microsoft -- microsoft_.net_framework_4.8	.NET Framework Information Disclosure Vulnerability	2024-03-23	7.5	CVE-2024-29059
microsoft -- xbox_gaming_services	Xbox Gaming Services Elevation of Privilege Vulnerability	2024-03-21	8.8	CVE-2024-28916
mndpsingh287 -- file_manager	The File Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 7.2.4. This is due to missing or incorrect nonce validation on the wp_file_manager page that includes files through the 'lang' parameter. This makes it possible for unauthenticated attackers to include local JavaScript files that can be leveraged to achieve RCE via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This issue was partially patched in version 7.2.4, and fully patched in 7.2.5.	2024-03-21	8.8	CVE-2024-1538
mobsf -- mobile-security-framework-mobsf	Mobile Security Framework (MobSF) is a pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis. In version 3.9.5 Beta and prior, MobSF does not perform any input validation when extracting the hostnames in `android:host`, so requests can also be sent to local hostnames. This can lead to server-side request forgery. An attacker can cause the server to make a connection to internal-only services within the organization's infrastructure. Commit 5a8eeee73c5f504a6c3abdf2a139a13804efdb77 has a hotfix for this issue.	2024-03-22	7.5	CVE-2024-29190

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a -- golang-fips/openssl	A memory leak flaw was found in Golang in the RSA encrypting/decrypting code, which might lead to a resource exhaustion vulnerability using attacker-controlled inputs. The memory leak happens in github.com/golang-fips/openssl/openssl/rsa.go#L113. The objects leaked are pkey and ctx. That function uses named return parameters to free pkey and ctx if there is an error initializing the context or setting the different properties. All return statements related to error cases follow the "return nil, nil, fail(...)" pattern, meaning that pkey and ctx will be nil inside the deferred function that should free them.	2024-03-21	7.5	CVE-2024-1394
n/a -- libdwarf	A double-free vulnerability was found in libdwarf. In a multiply-corrupted DWARF object, libdwarf may try to dealloc(free) an allocation twice, potentially causing unpredictable and various results.	2024-03-18	7.5	CVE-2024-2002
n/a -- podman	A flaw was found in Buildah (and subsequently Podman Build) which allows containers to mount arbitrary locations on the host filesystem into build containers. A malicious Containerfile can use a dummy image with a symbolic link to the root filesystem as a mount source and cause the mount operation to mount the host root filesystem inside the RUN step. The commands inside the RUN step will then have read-write access to the host filesystem, allowing for full container escape at build time.	2024-03-18	8.6	CVE-2024-1753
n/a -- spring_security	In Spring Security, versions 5.7.x prior to 5.7.12, 5.8.x prior to 5.8.11, versions 6.0.x prior to 6.0.9, versions 6.1.x prior to 6.1.8, versions 6.2.x prior to 6.2.3, an application is possible vulnerable to broken access control when it directly uses the AuthenticatedVoter#vote passing a null Authentication parameter.	2024-03-18	8.2	CVE-2024-22257
n/a -- tourfic	Unrestricted Upload of File with Dangerous Type vulnerability in Tourfic.This issue affects Tourfic: from n/a through 2.11.15.	2024-03-19	9.9	CVE-2024-29135
n/a -- unixodbc	An out-of-bounds stack write flaw was found in unixODBC on 64-bit architectures where the caller has 4 bytes and callee writes 8 bytes. This issue may go unnoticed on little-endian architectures, while big-endian architectures can be broken.	2024-03-18	7.1	CVE-2024-1013
n/a -- xnio	A flaw was found in XNIO. The XNIO NotifierState that can cause a Stack Overflow Exception when the chain of notifier states becomes problematically large can lead to uncontrolled resource management and a possible denial of service (DoS).	2024-03-22	7.5	CVE-2023-5685
netentsec -- ns-asg_application_security_gateway	A vulnerability, which was classified as critical, has been found in Netentsec NS-ASG Application Security Gateway 6.3. This issue affects some unknown processing of the file /admin/singlelogin.php. The manipulation of the argument loginId leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257285 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-19	7.3	CVE-2024-2647
ninjateam -- database_for_contact_form_7	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NinjaTeam Database for Contact Form 7 allows Stored XSS.This issue affects Database for Contact Form 7: from n/a through 3.0.6.	2024-03-19	7.1	CVE-2024-29103
olive_themes -- olive_one_click_demo_import	Missing Authorization vulnerability in Olive Themes Olive One Click Demo Import allows importing settings and data, ultimately leading to XSS.This issue affects Olive One Click Demo Import: from n/a through 1.1.1.	2024-03-20	8.2	CVE-2024-2702
openeuler -- aops_ceres	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in openEuler aops-ceres on Linux allows Command Injection. This vulnerability is associated with program files ceres/function/util.Py. This issue affects aops-ceres: from 1.3.0 through 1.4.1.	2024-03-23	7.3	CVE-2021-33633
opentext -- arcsight_platform	A potential vulnerability has been identified in OpenText ArcSight Platform. The vulnerability could be remotely exploited.	2024-03-20	9.8	CVE-2024-1811
opentext -- pvcs_version_manager	Weak access control in OpenText PVCS Version Manager allows potential bypassing of authentication and download of files.	2024-03-21	9.8	CVE-2024-1147
opentext -- pvcs_version_manager	Weak access control in OpenText PVCS Version Manager allows potential bypassing of authentication and uploading of files.	2024-03-21	9.8	CVE-2024-1148
optimole -- super_page_cache_for_cloudflare	Cross-Site Request Forgery (CSRF) vulnerability in Optimole Super Page Cache for Cloudflare allows Stored XSS.This issue affects Super Page Cache for Cloudflare: from n/a through 4.7.5.	2024-03-21	7.1	CVE-2024-27968

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
owncast -- owncast	Owncast is an open source, self-hosted, decentralized, single user live video streaming and chat server. In versions 0.1.2 and prior, a lenient CORS policy allows attackers to make a cross origin request, reading privileged information. This can be used to leak the admin password. Commit 9215d9ba0f29d62201d3feea9e77dcd274581624 fixes this issue.	2024-03-20	8.2	CVE-2024-29026
panabit -- panalog	A vulnerability classified as critical was found in Panabit Panalog 202103080942. This vulnerability affects unknown code of the file /Maintain/sprog_upstatus.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. The identifier of this vulnerability is VDB-255268. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-21	7.3	CVE-2024-2014
pandora_fms -- pandora_fms	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pandora FMS on all allows SQL Injection. This ulnerability allowed SQL injections to be made even if authentication failed.This issue affects Pandora FMS: from 700 through <776.	2024-03-19	7.5	CVE-2023-44091
pandora_fms -- pandora_fms	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Pandora FMS on all allows OS Command Injection. This vulnerability allowed to create a reverse shell and execute commands in the OS. This issue affects Pandora FMS: from 700 through <776.	2024-03-19	7.6	CVE-2023-44092
parse-community -- parse_server	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 6.5.5 and 7.0.0-alpha.29, calling an invalid Parse Server Cloud Function name or Cloud Job name crashes the server and may allow for code injection, internal store manipulation or remote code execution. The patch in versions 6.5.5 and 7.0.0-alpha.29 added string sanitation for Cloud Function name and Cloud Job name. As a workaround, sanitize the Cloud Function name and Cloud Job name before it reaches Parse Server.	2024-03-19	9	CVE-2024-29027
pauple -- table_&_contact_form_7_database_-_tablesome	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pauple Table & Contact Form 7 Database - Tablesome allows Reflected XSS.This issue affects Table & Contact Form 7 Database - Tablesome: from n/a through 1.0.27.	2024-03-19	7.1	CVE-2024-29110
pie_register -- pie_register	Unrestricted Upload of File with Dangerous Type vulnerability in Pie Register.This issue affects Pie Register: from n/a through 3.8.3.1.	2024-03-17	10	CVE-2024-27957
post_smtp -- post_smtp	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Post SMTP POST SMTP allows Reflected XSS.This issue affects POST SMTP: from n/a through 2.8.6.	2024-03-19	7.1	CVE-2024-29128
progress_software -- loadmaster	An OS command injection vulnerability has been identified in LoadMaster. An authenticated UI user with any permission settings may be able to inject commands into a UI component using a shell command resulting in OS command injection.	2024-03-22	8.4	CVE-2024-2448
progress_software -- loadmaster	A cross-site request forgery vulnerability has been identified in LoadMaster. It is possible for a malicious actor, who has prior knowledge of the IP or hostname of a specific LoadMaster, to direct an authenticated LoadMaster administrator to a third-party site. In such a scenario, the CSRF payload hosted on the malicious site would execute HTTP transactions on behalf of the LoadMaster administrator.	2024-03-22	7.5	CVE-2024-2449
progress_software_corporation -- telerik_report_server	In Progress® Telerik® Report Server versions prior to 2024 Q1 (10.0.24.130), a remote code execution attack is possible through an insecure deserialization vulnerability.	2024-03-20	9.9	CVE-2024-1800
progress_software_corporation -- telerik_reporting	In Progress® Telerik® Reporting versions prior to 2024 Q1 (18.0.24.130), a code execution attack is possible by a remote threat actor through an insecure deserialization vulnerability.	2024-03-20	8.5	CVE-2024-1856
progress_software_corporation -- telerik_reporting	In Progress® Telerik® Reporting versions prior to 2024 Q1 (18.0.24.130), a code execution attack is possible by a local threat actor through an insecure deserialization vulnerability.	2024-03-20	7.7	CVE-2024-1801
python_software_foundation -- cpython	An issue was found in the CPython `tempfile.TemporaryDirectory` class affecting versions 3.12.2, 3.11.8, 3.10.13, 3.9.18, and 3.8.18 and prior. The tempfile.TemporaryDirectory class would dereference symlinks during cleanup of permissions-related errors. This means users which can run privileged programs are potentially able to modify permissions of files referenced by symlinks in some circumstances.	2024-03-19	7.8	CVE-2023-6597

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rubengc -- gamipress_-_the_#1_gamification_plugin_to_reward_points_achievements_badges_&_ranks_in_wordpress	The GamiPress - The #1 gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to SQL Injection via the 'achievement_types' attribute of the gamipress_earnings shortcode in all versions up to, and including, 6.8.6 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.	2024-03-20	8.8	CVE-2024-1799
ruijie -- rg-nbs2009g-p	A vulnerability was found in Ruijie RG-NBS2009G-P up to 20240305. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /EXCU_SHELL. The manipulation of the argument Command1 leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257281 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-19	7.3	CVE-2024-2642
sailpoint -- identityiq	This vulnerability allows access to arbitrary files in the application server file system due to a path traversal vulnerability in JavaServer Faces (JSF) 2.2.20 documented in CVE-2020-6950. The remediation for this vulnerability contained in this security fix provides additional changes to the remediation announced in May 2021 tracked by ETN IIQSAW-3585 and January 2024 tracked by IIQFW-336. This vulnerability in IdentityIQ is assigned CVE-2024-2227.	2024-03-22	10	CVE-2024-2227
sailpoint -- identityiq	This vulnerability allows an authenticated user to perform a Lifecycle Manager flow or other QuickLink for a target user outside of the defined QuickLink Population.	2024-03-22	7.1	CVE-2024-2228
schneider_electric -- easergy_t200_(modbus)_models:_t200i_t200e_t200p_t200s_t200h	CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could cause account takeover and unauthorized access to the system when an attacker conducts brute-force attacks against the login form.	2024-03-18	9.8	CVE-2024-2051
schneider_electric -- easergy_t200_(modbus)_models:_t200i_t200e_t200p_t200s_t200h	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists when an attacker injects then executes arbitrary malicious JavaScript code within the context of the product.	2024-03-18	8.2	CVE-2024-2050
schneider_electric -- easergy_t200_(modbus)_models:_t200i_t200e_t200p_t200s_t200h	CWE-552: Files or Directories Accessible to External Parties vulnerability exists that could allow unauthenticated files and logs exfiltration and download of files when an attacker modifies the URL to download to a different location.	2024-03-18	7.5	CVE-2024-2052
schneider_electric -- ecostruxure_power_design_-_ecodial	CWE-502: Deserialization of Untrusted Data vulnerability exists that could cause remote code execution when a malicious project file is loaded into the application by a valid user.	2024-03-18	7.8	CVE-2024-2229
scott_paterson -- contact_form_7_-_paypal_&_stripe_add-on	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Scott Paterson Contact Form 7 - PayPal & Stripe Add-on allows Reflected XSS.This issue affects Contact Form 7 - PayPal & Stripe Add-on: from n/a through 2.0.	2024-03-19	7.1	CVE-2024-29130
sentrifugo -- sentrifugo	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/index/getdepartments/format/html, 'business_id' parameter./sentrifugo/index.php/index/getdepartments/format/html, 'business_id' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	2024-03-21	9.8	CVE-2024-29870 cve-

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sentrifugo -- sentrifugo	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/index/getdepartments/sentrifugo/index.php/index/updatecontactnumber, 'id' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	2024-03-21	9.8	CVE-2024-29871 cve-
sentrifugo -- sentrifugo	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/empscreening/add, 'agencyids' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	2024-03-21	9.8	CVE-2024-29872 cve-
sentrifugo -- sentrifugo	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/reports/businessunits/format/html, 'bunitname' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	2024-03-21	9.8	CVE-2024-29873 cve-
sentrifugo -- sentrifugo	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/default/reports/activeuserrptpdf, 'sort_name' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	2024-03-21	9.8	CVE-2024-29874 cve-
sentrifugo -- sentrifugo	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/default/reports/exportactiveuserrpt, 'sort_name' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	2024-03-21	9.8	CVE-2024-29875 cve-
sentrifugo -- sentrifugo	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/reports/activitylogreport, 'sortby' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	2024-03-21	9.8	CVE-2024-29876 cve-
sentrifugo -- sentrifugo	Cross-Site Scripting (XSS) vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/expenses/expensecategories/edit, 'expense_category_name' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted URL to the victim and steal their session data.	2024-03-21	7.1	CVE-2024-29877 cve-
sentrifugo -- sentrifugo	Cross-Site Scripting (XSS) vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/sitepreference/add, 'description' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted URL to the victim and steal their session data.	2024-03-21	7.1	CVE-2024-29878 cve-
sentrifugo -- sentrifugo	Cross-Site Scripting (XSS) vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/index/getdepartments/format/html, 'business_id' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted URL to the victim and steal their session data.	2024-03-21	7.1	CVE-2024-29879 cve-
social_media_share_buttons_by_sygnoos -- social_media_share_buttons	Deserialization of Untrusted Data vulnerability in Social Media Share Buttons By Sygnoos Social Media Share Buttons.This issue affects Social Media Share Buttons: from n/a through 2.1.0.	2024-03-20	8.2	CVE-2024-2721
sourcecodester -- employee_task_management_system	A vulnerability was found in SourceCodester Employee Task Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin-manage-user.php. The manipulation leads to execution after redirect. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257072.	2024-03-18	7.3	CVE-2024-2569
sourcecodester -- employee_task_management_system	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been classified as critical. This affects an unknown part of the file /edit-task.php. The manipulation leads to execution after redirect. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257073 was assigned to this vulnerability.	2024-03-18	7.3	CVE-2024-2570
sourcecodester -- employee_task_management_system	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /manage-admin.php. The manipulation leads to execution after redirect. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257074 is the identifier assigned to this vulnerability.	2024-03-18	7.3	CVE-2024-2571
sourcecodester -- employee_task_management_system	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /task-details.php. The manipulation leads to execution after redirect. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257075.	2024-03-18	7.3	CVE-2024-2572

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sourcecodester -- employee_task_management_system	A vulnerability classified as critical has been found in SourceCodester Employee Task Management System 1.0. Affected is an unknown function of the file /task-info.php. The manipulation leads to execution after redirect. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257076.	2024-03-18	7.3	CVE-2024-2573
sourcecodester -- employee_task_management_system	A vulnerability classified as critical was found in SourceCodester Employee Task Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /edit-task.php. The manipulation of the argument task_id leads to authorization bypass. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257077 was assigned to this vulnerability.	2024-03-18	7.3	CVE-2024-2574
sourcecodester -- employee_task_management_system	A vulnerability, which was classified as critical, has been found in SourceCodester Employee Task Management System 1.0. Affected by this issue is some unknown functionality of the file /task-details.php. The manipulation of the argument task_id leads to authorization bypass. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257078 is the identifier assigned to this vulnerability.	2024-03-18	7.3	CVE-2024-2575
sourcecodester -- employee_task_management_system	A vulnerability, which was classified as critical, was found in SourceCodester Employee Task Management System 1.0. This affects an unknown part of the file /update-admin.php. The manipulation of the argument admin_id leads to authorization bypass. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257079.	2024-03-18	7.3	CVE-2024-2576
sourcecodester -- employee_task_management_system	A vulnerability has been found in SourceCodester Employee Task Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /update-employee.php. The manipulation of the argument admin_id leads to authorization bypass. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257080.	2024-03-18	7.3	CVE-2024-2577
stacklok -- minder	Minder is a software supply chain security platform. Prior to version 0.0.33, a Minder user can use the endpoints `GetRepositoryByName`, `DeleteRepositoryByName`, and `GetArtifactByName` to access any repository in the database, irrespective of who owns the repo and any permissions present. The database query checks by repo owner, repo name and provider name (which is always `github`). These query values are not distinct for the particular user - as long as the user has valid credentials and a provider, they can set the repo owner/name to any value they want and the server will return information on this repo. Version 0.0.33 contains a patch for this issue.	2024-03-21	7.1	CVE-2024-27916
svenl77 -- buddypress_woocommerce_my_account_integration_create_woocommerce_member_pages	The "BuddyPress WooCommerce My Account Integration. Create WooCommerce Member Pages" plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.4.20 via deserialization of untrusted input in the get_simple_request function. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject a PHP Object. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-03-23	8.8	CVE-2024-2025
tenable -- nessus_agent	As a part of Tenable's vulnerability disclosure program, a vulnerability in a Nessus plugin was identified and reported. This vulnerability could allow a malicious actor with sufficient permissions on a scan target to place a binary in a specific filesystem location, and abuse the impacted plugin in order to escalate privileges.	2024-03-18	7.8	CVE-2024-2390
tenda -- ac10	A vulnerability was found in Tenda AC10 16.03.10.13 and classified as critical. This issue affects the function fromSetRouteStatic of the file /goform/SetStaticRouteCfg. The manipulation of the argument list leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257081 was assigned to this vulnerability.	2024-03-18	8.8	CVE-2024-2581
tenda -- ac10u	A vulnerability was found in Tenda AC10U 15.03.06.48. It has been rated as critical. Affected by this issue is the function addWifiMacFilter of the file /goform/addWifiMacFilter. The manipulation of the argument deviceMac leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257462 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-20	8.8	CVE-2024-2711
tenda -- ac10u	A vulnerability classified as critical has been found in Tenda AC10U 15.03.06.49. Affected is the function formSetDeviceName of the file /goform/SetOnlineDevName. The manipulation of the argument mac leads to	2024-03-20	8.8	CVE-2024-2703

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257454 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
tenda -- ac10u	A vulnerability classified as critical was found in Tenda AC10U 15.03.06.49. Affected by this vulnerability is the function formSetFirewallCfg of the file /goform/SetFirewallCfg. The manipulation of the argument firewallEn leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257455. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-20	8.8	CVE-2024-2704
tenda -- ac10u	A vulnerability, which was classified as critical, has been found in Tenda AC10U 1.0/15.03.06.49. Affected by this issue is the function formSetQosBand of the file /goform/SetNetControlList. The manipulation of the argument list leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257456. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-20	8.8	CVE-2024-2705
tenda -- ac10u	A vulnerability, which was classified as critical, was found in Tenda AC10U 15.03.06.49. This affects the function formWifiWpsStart of the file /goform/WifiWpsStart. The manipulation of the argument index leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257457 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-20	8.8	CVE-2024-2706
tenda -- ac10u	A vulnerability was found in Tenda AC10U 15.03.06.49 and classified as critical. This issue affects the function formexeCommand of the file /goform/execCommand. The manipulation of the argument cmdinput leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257459. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-20	8.8	CVE-2024-2708
tenda -- ac10u	A vulnerability was found in Tenda AC10U 15.03.06.49. It has been classified as critical. Affected is the function fromSetRouteStatic of the file /goform/SetStaticRouteCfg. The manipulation of the argument list leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257460. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-20	8.8	CVE-2024-2709
tenda -- ac10u	A vulnerability was found in Tenda AC10U 15.03.06.49. It has been declared as critical. Affected by this vulnerability is the function setSchedWifi of the file /goform/openSchedWifi. The manipulation of the argument schedStartTime leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257461 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-20	8.8	CVE-2024-2710
tenda -- ac10u	A vulnerability, which was classified as critical, has been found in Tenda AC10U 15.03.06.48. Affected by this issue is the function formSetCfm of the file goform/setcfm. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257600. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-21	8.8	CVE-2024-2763
tenda -- ac10u	A vulnerability, which was classified as critical, was found in Tenda AC10U 15.03.06.48. This affects the function formSetPPTPServer of the file /goform/SetPptpServerCfg. The manipulation of the argument endIP leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257601 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-21	8.8	CVE-2024-2764
tenda -- ac15	A vulnerability was found in Tenda AC15 15.03.20_multi. It has been declared as critical. This vulnerability affects the function form_fast_setting_wifi_set of the file /goform/fast_setting_wifi_set. The manipulation of the argument ssid leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is	2024-03-22	8.8	CVE-2024-2813

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	VDB-257668. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
tenda -- ac15	A vulnerability was found in Tenda AC15 15.03.20_multi. It has been rated as critical. This issue affects the function fromDhcpListClient of the file /goform/DhcpListClient. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257669 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	8.8	CVE-2024-2814
tenda -- ac15	A vulnerability classified as critical has been found in Tenda AC15 15.03.20_multi. Affected is the function R7WebsSecurityHandler of the file /goform/execCommand of the component Cookie Handler. The manipulation of the argument password leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257670 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	8.8	CVE-2024-2815
tenda -- ac15	A vulnerability was found in Tenda AC15 15.03.05.18/15.03.20_multi. It has been rated as critical. Affected by this issue is the function formSetSpeedWan of the file /goform/SetSpeedWan. The manipulation of the argument speed_dir leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257660. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	8.8	CVE-2024-2805
tenda -- ac15	A vulnerability classified as critical has been found in Tenda AC15 15.03.05.18/15.03.20_multi. This affects the function addWifiMacFilter of the file /goform/addWifiMacFilter. The manipulation of the argument deviceId/deviceMac leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257661 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	8.8	CVE-2024-2806
tenda -- ac15	A vulnerability classified as critical was found in Tenda AC15 15.03.05.18/15.03.20_multi. This vulnerability affects the function formExpandDlnaFile of the file /goform/expandDlnaFile. The manipulation of the argument filePath leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257662 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	8.8	CVE-2024-2807
tenda -- ac15	A vulnerability, which was classified as critical, has been found in Tenda AC15 15.03.05.18/15.03.20_multi. This issue affects the function formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257663. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	8.8	CVE-2024-2808
tenda -- ac15	A vulnerability, which was classified as critical, was found in Tenda AC15 15.03.05.18/15.03.20_multi. Affected is the function formSetFirewallCfg of the file /goform/SetFirewallCfg. The manipulation of the argument firewallEn leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257664. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	8.8	CVE-2024-2809
tenda -- ac15	A vulnerability has been found in Tenda AC15 15.03.05.18/15.03.20_multi and classified as critical. Affected by this vulnerability is the function formWifiWpsOOB of the file /goform/WifiWpsOOB. The manipulation of the argument index leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257665 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	8.8	CVE-2024-2810
tenda -- ac15	A vulnerability was found in Tenda AC15 15.03.20_multi and classified as critical. Affected by this issue is the function formWifiWpsStart of the file /goform/WifiWpsStart. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257666 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	8.8	CVE-2024-2811

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenda -- ac18	A vulnerability has been found in Tenda AC18 15.13.07.09 and classified as critical. Affected by this vulnerability is the function fromSetWirelessRepeat. The manipulation of the argument wpapsk_crypto5g leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256999. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-17	8.8	CVE-2024-2546
tenda -- ac18	A vulnerability was found in Tenda AC18 15.03.05.05 and classified as critical. Affected by this issue is the function R7WebsSecurityHandler. The manipulation of the argument password leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257000. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-17	8.8	CVE-2024-2547
tenda -- ac18	A vulnerability was found in Tenda AC18 15.03.05.05. It has been rated as critical. This issue affects the function formexeCommand of the file /goform/execCommand. The manipulation of the argument cmdinput leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257057 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-17	8.8	CVE-2024-2558
themefic -- tourfic	Deserialization of Untrusted Data vulnerability in Themefic Tourfic.This issue affects Tourfic: from n/a through 2.11.17.	2024-03-19	8.5	CVE-2024-29136
themefic -- tourfic	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themefic Tourfic allows Reflected XSS.This issue affects Tourfic: from n/a through 2.11.7.	2024-03-19	7.1	CVE-2024-29137
themeisle -- visualizer	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeisle Visualizer allows Reflected XSS.This issue affects Visualizer: from n/a through 3.10.5.	2024-03-17	7.1	CVE-2024-27958
tomphttp -- bare-server-node	TOMP Bare Server implements the TompHTTP bare server. A vulnerability in versions prior to 2.0.2 relates to insecure handling of HTTP requests by the @tomphttp/bare-server-node package. This flaw potentially exposes the users of the package to manipulation of their web traffic. The impact may vary depending on the specific usage of the package but it can potentially affect any system where this package is in use. The problem has been patched in version 2.0.2. As of time of publication, no specific workaround strategies have been disclosed.	2024-03-21	9.8	CVE-2024-27922
typps -- calendarista_basic_edition	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Typps Calendarista Basic Edition.This issue affects Calendarista Basic Edition: from n/a through 3.0.2.	2024-03-21	7.1	CVE-2024-27993
ukrsolution -- barcode_scanner_with_inventory_&_order_manager	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UkrSolution Barcode Scanner with Inventory & Order Manager allows Reflected XSS.This issue affects Barcode Scanner with Inventory & Order Manager: from n/a through 1.5.3.	2024-03-19	7.1	CVE-2024-27998
unitronics_ -- unistream_unilogic	CWE-287: Improper Authentication may allow Authentication Bypass	2024-03-18	10	CVE-2024-27767
unitronics_ -- unistream_unilogic	Unitronics Unistream Unilogic - Versions prior to 1.35.227 - CWE-22: 'Path Traversal' may allow RCE	2024-03-18	9.8	CVE-2024-27768
unitronics_ -- unistream_unilogic	Unitronics Unistream Unilogic - Versions prior to 1.35.227 - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor may allow Taking Ownership Over Devices	2024-03-18	8.8	CVE-2024-27769
unitronics_ -- unistream_unilogic	Unitronics Unistream Unilogic - Versions prior to 1.35.227 - CWE-23: Relative Path Traversal	2024-03-18	8.8	CVE-2024-27770
unitronics_ -- unistream_unilogic	Unitronics Unistream Unilogic - Versions prior to 1.35.227 - CWE-22: 'Path Traversal' may allow RCE	2024-03-18	8.8	CVE-2024-27771
unitronics_ -- unistream_unilogic	Unitronics Unistream Unilogic - Versions prior to 1.35.227 - CWE-78: 'OS Command Injection' may allow RCE	2024-03-18	8.8	CVE-2024-27772
unitronics_ -- unistream_unilogic	Unitronics Unistream Unilogic - Versions prior to 1.35.227 - CWE-348: Use of Less Trusted Source may allow RCE	2024-03-18	8.8	CVE-2024-27773

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
unitronics_ -- unistream_unilogic	Unitronics Unistream Unilogic - Versions prior to 1.35.227 - CWE-259: Use of Hard-coded Password may allow disclosing Sensitive Information Embedded inside Device's Firmware	2024-03-18	7.5	CVE-2024-27774
valvepress -- automatic	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ValvePress Automatic allows SQL Injection.This issue affects Automatic: from n/a through 3.92.0.	2024-03-21	9.9	CVE-2024-27956
wasmi-labs -- wasmi	Wasmi is an efficient and lightweight WebAssembly interpreter with a focus on constrained and embedded systems. In the WASMI Interpreter, an Out-of-bounds Buffer Write will arise if the host calls or resumes a Wasm function with more parameters than the default limit (128), as it will surpass the stack value. This doesn't affect calls from Wasm to Wasm, only from host to Wasm. This vulnerability was patched in version 0.31.1.	2024-03-21	7.3	CVE-2024-28123
webberzone -- better_search_-_relevant_search_results_for_wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebberZone Better Search - Relevant search results for WordPress allows Stored XSS.This issue affects Better Search - Relevant search results for WordPress: from n/a through 3.3.0.	2024-03-19	7.1	CVE-2024-29142
webpack -- webpack-dev-middleware	Prior to versions 7.1.0, 6.1.2, and 5.3.4, the webpack-dev-middleware development middleware for devpack does not validate the supplied URL address sufficiently before returning the local file. It is possible to access any file on the developer's machine. The middleware can either work with the physical filesystem when reading the files or it can use a virtualized in-memory `memfs` filesystem. If `writeToDisk` configuration option is set to `true`, the physical filesystem is used. The `getFilenameFromUrl` method is used to parse URL and build the local file path. The public path prefix is stripped from the URL, and the `unsecaped` path suffix is appended to the `outputPath`. As the URL is not unescaped and normalized automatically before calling the midlleware, it is possible to use `%2e` and `%2f` sequences to perform path traversal attack. Developers using `webpack-dev-server` or `webpack-dev-middleware` are affected by the issue. When the project is started, an attacker might access any file on the developer's machine and exfiltrate the content. If the development server is listening on a public IP address (or `0.0.0.0`), an attacker on the local network can access the local files without any interaction from the victim (direct connection to the port). If the server allows access from third-party domains, an attacker can send a malicious link to the victim. When visited, the client side script can connect to the local server and exfiltrate the local files. Starting with fixed versions 7.1.0, 6.1.2, and 5.3.4, the URL is unescaped and normalized before any further processing.	2024-03-21	7.4	CVE-2024-29180
wpexpertsio -- wc_shop_sync_-_integrate_square_and_woocommerce_for_seamless_shop_management	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wpexpertsio WC Shop Sync - Integrate Square and WooCommerce for Seamless Shop Management allows Reflected XSS.This issue affects WC Shop Sync - Integrate Square and WooCommerce for Seamless Shop Management: from n/a through 4.2.9.	2024-03-17	7.1	CVE-2024-27959
wplit_pty_ltd -- oxyextras	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPLIT Pty Ltd OxyExtras allows Reflected XSS.This issue affects OxyExtras: from n/a through 1.4.4.	2024-03-19	7.1	CVE-2024-29129
wpvncom -- ux_flat	The UX Flat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'button' shortcode 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 and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-20	7.4	CVE-2024-2459
xpodas -- octopod	Authentication Bypass by Primary Weakness vulnerability in XPodas Octopod allows Authentication Bypass.This issue affects Octopod: before v1. NOTE: The vendor was contacted and it was learned that the product is not supported.	2024-03-21	9.8	CVE-2024-1202
yannick_lefebvre -- link_library	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Yannick Lefebvre Link Library allows Reflected XSS.This issue affects Link Library: from n/a through 7.6.	2024-03-19	7.1	CVE-2024-29123
yith -- yith_woocommerce_product_add-ons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in YITH YITH WooCommerce Product Add-Ons allows Reflected XSS.This issue affects YITH WooCommerce Product Add-Ons: from n/a through 4.5.0.	2024-03-21	7.1	CVE-2024-27994

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zitadel -- zitadel	ZITADEL, open source authentication management software, uses Go templates to render the login UI. Due to a improper use of the `text/template` instead of the `html/template` package, the Login UI did not sanitize input parameters prior to versions 2.47.3, 2.46.1, 2.45.1, 2.44.3, 2.43.9, 2.42.15, and 2.41.15. An attacker could create a malicious link, where he injected code which would be rendered as part of the login screen. While it was possible to inject HTML including JavaScript, the execution of such scripts would be prevented by the Content Security Policy. Versions 2.47.3, 2.46.1, 2.45.1, 2.44.3, 2.43.9, 2.42.15, and 2.41.15 contain a patch for this issue. No known workarounds are available.	2024-03-18	8.1	CVE-2024-28855
academylms -- academy_lms_-_elearning_and_online_course_solution_for_wordpress	The Academy LMS - eLearning and online course solution for WordPress plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.9.19. This is due to plugin allowing arbitrary user meta updates through the saved_user_info() function. This makes it possible for authenticated attackers, with minimal permissions such as students, to elevate their user role to that of an administrator.	2024-03-13	8.8	CVE-2024-1505
andrei_ivasiuc -- fontific_|_google_fonts	Cross-Site Request Forgery (CSRF) vulnerability in Andrei Ivasiuc Fontific | Google Fonts allows Stored XSS.This issue affects Fontific | Google Fonts: from n/a through 0.1.6.	2024-03-16	7.1	CVE-2024-27194
apache_software_foundation -- apache_pulsar	Improper Authentication vulnerability in Apache Pulsar Proxy allows an attacker to connect to the /proxy-stats endpoint without authentication. The vulnerable endpoint exposes detailed statistics about live connections, along with the capability to modify the logging level of proxied connections without requiring proper authentication credentials. This issue affects Apache Pulsar versions from 2.6.0 to 2.10.5, from 2.11.0 to 2.11.2, from 3.0.0 to 3.0.1, and 3.1.0. The known risks include exposing sensitive information such as connected client IP and unauthorized logging level manipulation which could lead to a denial-of-service condition by significantly increasing the proxy's logging overhead. When deployed via the Apache Pulsar Helm chart within Kubernetes environments, the actual client IP might not be revealed through the load balancer's default behavior, which typically obscures the original source IP addresses when externalTrafficPolicy is being configured to "Cluster" by default. The /proxy-stats endpoint contains topic level statistics, however, in the default configuration, the topic level statistics aren't known to be exposed. 2.10 Pulsar Proxy users should upgrade to at least 2.10.6. 2.11 Pulsar Proxy users should upgrade to at least 2.11.3. 3.0 Pulsar Proxy users should upgrade to at least 3.0.2. 3.1 Pulsar Proxy users should upgrade to at least 3.1.1. Users operating versions prior to those listed above should upgrade to the aforementioned patched versions or newer versions. Additionally, it's imperative to recognize that the Apache Pulsar Proxy is not intended for direct exposure to the internet. The architectural design of Pulsar Proxy assumes that it will operate within a secured network environment, safeguarded by appropriate perimeter defenses.	2024-03-12	8.2	CVE-2022-34321
apache_software_foundation -- apache_pulsar	Improper input validation in the Pulsar Function Worker allows a malicious authenticated user to execute arbitrary Java code on the Pulsar Function worker, outside of the sandboxes designated for running user-provided functions. This vulnerability also applies to the Pulsar Broker when it is configured with "functionsWorkerEnabled=true". This issue affects Apache Pulsar versions from 2.4.0 to 2.10.5, from 2.11.0 to 2.11.3, from 3.0.0 to 3.0.2, from 3.1.0 to 3.1.2, and 3.2.0. 2.10 Pulsar Function Worker users should upgrade to at least 2.10.6. 2.11 Pulsar Function Worker users should upgrade to at least 2.11.4. 3.0 Pulsar Function Worker users should upgrade to at least 3.0.3. 3.1 Pulsar Function Worker users should upgrade to at least 3.1.3. 3.2 Pulsar Function Worker users should upgrade to at least 3.2.1. Users operating versions prior to those listed above should upgrade to the aforementioned patched versions or newer versions.	2024-03-12	8.5	CVE-2024-27135
apache_software_foundation -- apache_pulsar	In Pulsar Functions Worker, authenticated users can upload functions in jar or nar files. These files, essentially zip files, are extracted by the Functions Worker. However, if a malicious file is uploaded, it could exploit a directory traversal vulnerability. This occurs when the filenames in the zip files, which aren't properly validated, contain special elements like "..", altering the directory path. This could allow an attacker to create or modify files outside of the designated extraction directory, potentially influencing system behavior. This vulnerability also applies to the Pulsar Broker when it is configured with "functionsWorkerEnabled=true". This issue affects Apache Pulsar versions from 2.4.0 to 2.10.5, from 2.11.0 to 2.11.3, from 3.0.0 to 3.0.2, from 3.1.0 to 3.1.2, and 3.2.0. 2.10 Pulsar Function Worker users should upgrade to at least 2.10.6. 2.11 Pulsar Function Worker users should upgrade to at least 2.11.4. 3.0 Pulsar Function Worker users should upgrade to at	2024-03-12	8.4	CVE-2024-27317

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	least 3.0.3. 3.1 Pulsar Function Worker users should upgrade to at least 3.1.3. 3.2 Pulsar Function Worker users should upgrade to at least 3.2.1. Users operating versions prior to those listed above should upgrade to the aforementioned patched versions or newer versions.			
apache_software_foundation -- apache_pulsar	The Pulsar Functions Worker includes a capability that permits authenticated users to create functions where the function's implementation is referenced by a URL. The supported URL schemes include "file", "http", and "https". When a function is created using this method, the Functions Worker will retrieve the implementation from the URL provided by the user. However, this feature introduces a vulnerability that can be exploited by an attacker to gain unauthorized access to any file that the Pulsar Functions Worker process has permissions to read. This includes reading the process environment which potentially includes sensitive information, such as secrets. Furthermore, an attacker could leverage this vulnerability to use the Pulsar Functions Worker as a proxy to access the content of remote HTTP and HTTPS endpoint URLs. This could also be used to carry out denial of service attacks. This vulnerability also applies to the Pulsar Broker when it is configured with "functionsWorkerEnabled=true". This issue affects Apache Pulsar versions from 2.4.0 to 2.10.5, from 2.11.0 to 2.11.3, from 3.0.0 to 3.0.2, from 3.1.0 to 3.1.2, and 3.2.0. 2.10 Pulsar Function Worker users should upgrade to at least 2.10.6. 2.11 Pulsar Function Worker users should upgrade to at least 2.11.4. 3.0 Pulsar Function Worker users should upgrade to at least 3.0.3. 3.1 Pulsar Function Worker users should upgrade to at least 3.1.3. 3.2 Pulsar Function Worker users should upgrade to at least 3.2.1. Users operating versions prior to those listed above should upgrade to the aforementioned patched versions or newer versions. The updated versions of Pulsar Functions Worker will, by default, impose restrictions on the creation of functions using URLs. For users who rely on this functionality, the Function Worker configuration provides two configuration keys: "additionalEnabledConnectorUrlPatterns" and "additionalEnabledFunctionsUrlPatterns". These keys allow users to specify a set of URL patterns that are permitted, enabling the creation of functions using URLs that match the defined patterns. This approach ensures that the feature remains available to those who require it, while limiting the potential for unauthorized access and exploitation.	2024-03-12	8.5	CVE-2024-27894
arcserve -- unified_data_protection	An authentication bypass vulnerability exists in Arcserve Unified Data Protection 9.2 and 8.1 in the edge-app-base-webui.jar!com.ca.arcserve.edge.app.base.ui.server.EdgeLoginServiceImpl.doLogin() function within wizardLogin.	2024-03-13	9.8	CVE-2024-0799
arcserve -- unified_data_protection	A path traversal vulnerability exists in Arcserve Unified Data Protection 9.2 and 8.1 in edge-app-base-webui.jar!com.ca.arcserve.edge.app.base.ui.server.servlet.ImportNodeServlet.	2024-03-13	8.8	CVE-2024-0800
arcserve -- unified_data_protection	A denial of service vulnerability exists in Arcserve Unified Data Protection 9.2 and 8.1 in ASNative.dll.	2024-03-13	7.5	CVE-2024-0801
argoproj -- argo-cd	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Due to the improper URL protocols filtering of links specified in the `link.argocd.argoproj.io` annotations in the application summary component, an attacker can achieve cross-site scripting with elevated permissions. All unpatched versions of Argo CD starting with v1.0.0 are vulnerable to a cross-site scripting (XSS) bug allowing a malicious user to inject a javascript: link in the UI. When clicked by a victim user, the script will execute with the victim's permissions (up to and including admin). This vulnerability allows an attacker to perform arbitrary actions on behalf of the victim via the API, such as creating, modifying, and deleting Kubernetes resources. A patch for this vulnerability has been released in Argo CD versions v2.10.3 v2.9.8, and v2.8.12. There are no completely-safe workarounds besides upgrading. The safest alternative, if upgrading is not possible, would be to create a Kubernetes admission controller to reject any resources with an annotation starting with link.argocd.argoproj.io or reject the resource if the value use an improper URL protocol. This validation will need to be applied in all clusters managed by ArgoCD.	2024-03-13	9	CVE-2024-28175
autopolisbg -- bulgarisation_for_woocommerce	The Bulgarisation for WooCommerce plugin for WordPress is vulnerable to unauthorized access due to missing capability checks on several functions in all versions up to, and including, 3.0.14. This makes it possible for unauthenticated and authenticated attackers, with subscriber-level access and above, to generate and delete labels.	2024-03-13	7.3	CVE-2024-0683

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autopolisbg -- bulgarisation_for_woocommerce	The Bulgarisation for WooCommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.14. This is due to missing or incorrect nonce validation on several functions. This makes it possible for unauthenticated attackers to generate and delete labels via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-12	7.3	CVE-2024-2395
aweber -- aweber_-_free_sign_up_form_and_landing_page_builder_plugin_for_lead_generation_and_email_newsletter_growth	The AWeber - Free Sign Up Form and Landing Page Builder Plugin for Lead Generation and Email Newsletter Growth plugin for WordPress is vulnerable to SQL Injection via the 'post_id' parameter in all versions up to, and including, 7.3.14 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.	2024-03-13	7.2	CVE-2024-1793
badger_meter -- monitool	SQL injection vulnerability in Badger Meter Monitool affecting versions 4.6.3 and earlier. A remote attacker could send a specially crafted SQL query to the server via the j_username parameter and retrieve the information stored in the database.	2024-03-12	9.8	CVE-2024-1301 cve-
badger_meter -- monitool	Information exposure vulnerability in Badger Meter Monitool affecting versions up to 4.6.3 and earlier. A local attacker could change the application's file parameter to a log file obtaining all sensitive information such as database credentials.	2024-03-12	7.3	CVE-2024-1302 cve-
bee -- beepress	Cross-Site Request Forgery (CSRF) vulnerability in Bee BeePress allows Stored XSS.This issue affects BeePress: from n/a through 6.9.8.	2024-03-16	7.1	CVE-2024-27197
boldgrid -- weforms_-_easy_drag_&_drop_contact_form_builder_for_wordpress	The weForms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Referer' HTTP header in all versions up to, and including, 1.6.21 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.	2024-03-12	7.2	CVE-2024-0386
canon_inc. -- color_imageclass_mf740c_series	Buffer overflow in identifier field of WSD probe request process of Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code.*:Satera MF740C Series/Satera MF640C Series/Satera LBP660C Series/Satera LBP620C Series firmware v12.07 and earlier, and Satera MF750C Series/Satera LBP670C Series firmware v03.09 and earlier sold in Japan.Color imageCLASS MF740C Series/Color imageCLASS MF640C Series/Color imageCLASS X MF1127C/Color imageCLASS LBP664Cdw/Color imageCLASS LBP622Cdw/Color imageCLASS X LBP1127C firmware v12.07 and earlier, and Color imageCLASS MF750C Series/Color imageCLASS X MF1333C/Color imageCLASS LBP674Cdw/Color imageCLASS X LBP1333C firmware v03.09 and earlier sold in US.i-SENSYS MF740C Series/i-SENSYS MF640C Series/C1127i Series/i-SENSYS LBP660C Series/i-SENSYS LBP620C Series/C1127P firmware v12.07 and earlier, and i-SENSYS MF750C Series/C1333i Series/i-SENSYS LBP673Cdw/C1333P firmware v03.09 and earlier sold in Europe.			
chatgptnextweb -- nextchat	NextChat, also known as ChatGPT-Next-Web, is a cross-platform chat user interface for use with ChatGPT. Versions 2.11.2 and prior are vulnerable to server-side request forgery and cross-site scripting. This vulnerability enables read access to internal HTTP endpoints but also write access using HTTP POST, PUT, and other methods. Attackers can also use this vulnerability to mask their source IP by forwarding malicious traffic intended for other Internet targets through these open proxies. As of time of publication, no patch is available, but other mitigation strategies are available. Users may avoid exposing the application to the public internet or, if exposing the application to the internet, ensure it is an isolated network with no access to any other internal resources.	2024-03-12	9.1	CVE-2023-49785
cisco -- cisco_ios_xr_software	A vulnerability in the Layer 2 Ethernet services of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause the line card network processor to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of specific Ethernet frames that are received on line cards that have the Layer 2 services feature enabled. An attacker could exploit this vulnerability by sending specific Ethernet frames through an affected device. A successful exploit could allow the attacker to cause the ingress interface network processor to reset, resulting in a loss of traffic over the interfaces that are supported by the network processor. Multiple resets of the network processor would cause the line card to reset, resulting in a DoS condition.	2024-03-13	7.4	CVE-2024-20318

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- cisco_ios_xr_software	A vulnerability in the SSH client feature of Cisco IOS XR Software for Cisco 8000 Series Routers and Cisco Network Convergence System (NCS) 540 Series and 5700 Series Routers could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient validation of arguments that are included with the SSH client CLI command. An attacker with low-privileged access to an affected device could exploit this vulnerability by issuing a crafted SSH client command to the CLI. A successful exploit could allow the attacker to elevate privileges to root on the affected device.	2024-03-13	7.8	CVE-2024-20320
cisco -- cisco_ios_xr_software	A vulnerability in the PPP over Ethernet (PPPoE) termination feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers could allow an unauthenticated, adjacent attacker to crash the ppp_ma process, resulting in a denial of service (DoS) condition. This vulnerability is due to the improper handling of malformed PPPoE packets that are received on a router that is running Broadband Network Gateway (BNG) functionality with PPPoE termination on a Lightspeed-based or Lightspeed-Plus-based line card. An attacker could exploit this vulnerability by sending a crafted PPPoE packet to an affected line card interface that does not terminate PPPoE. A successful exploit could allow the attacker to crash the ppp_ma process, resulting in a DoS condition for PPPoE traffic across the router.	2024-03-13	7.4	CVE-2024-20327
cms_made_simple -- cms_made_simple	Unrestricted file upload vulnerability in CMS Made Simple, affecting version 2.2.14. This vulnerability allows an authenticated user to bypass the security measures of the upload functionality and potentially create a remote execution of commands via webshell.	2024-03-12	9.8	CVE-2024-1527 cve-
cms_made_simple -- cms_made_simple	CMS Made Simple version 2.2.14, does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /admin/moduleinterface.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted JavaScript payload to an authenticated user and partially hijack their browser session.	2024-03-12	7.4	CVE-2024-1528 cve-
cms_made_simple -- cms_made_simple	Vulnerability in CMS Made Simple 2.2.14, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /admin/adduser.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted JavaScript payload to an authenticated user and partially take over their browser session.	2024-03-12	7.4	CVE-2024-1529 cve-
codepeople -- calculated_fields_form	The Calculated Fields Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form page href parameter in all versions up to, and including, 5.1.56 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. Exploitation requires the professional version or higher.	2024-03-13	7.2	CVE-2024-2020
concerted_action -- action_network	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Concerted Action Action Network allows Reflected XSS.This issue affects Action Network: from n/a through 1.4.2.	2024-03-15	7.1	CVE-2024-25921
corewcf -- corewcf	CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. If you have a NetFraming based CoreWCF service, extra system resources could be consumed by connections being left established instead of closing or aborting them. There are two scenarios when this can happen. When a client established a connection to the service and sends no data, the service will wait indefinitely for the client to initiate the NetFraming session handshake. Additionally, once a client has established a session, if the client doesn't send any requests for the period of time configured in the binding ReceiveTimeout, the connection is not properly closed as part of the session being aborted. The bindings affected by this behavior are NetTcpBinding, NetNamedPipeBinding, and UnixDomainSocketBinding. Only NetTcpBinding has the ability to accept non local connections. The currently supported versions of CoreWCF are v1.4.x and v1.5.x. The fix can be found in v1.4.2 and v1.5.3 of the CoreWCF packages. Users are advised to upgrade. There are no workarounds for this issue.	2024-03-15	7.5	CVE-2024-28252
cyberlord92 -- web_application_firewall_-_website_security	The Malware Scanner plugin and the Web Application Firewall plugin for WordPress (both by MiniOrange) are vulnerable to privilege escalation due to a missing capability check on the mo_wpns_init() function in all versions up to, and including, 4.7.2 (for Malware Scanner) and 2.1.1 (for Web Application Firewall). This makes it possible for unauthenticated attackers to escalate their privileges to that of an administrator.	2024-03-13	9.8	CVE-2024-2172
dell -- poweredge_platfor	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain an Improper SMM communication buffer verification vulnerability. A local low privileged	2024-03-13	7.2	CVE-2024-0161

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
m	attacker could potentially exploit this vulnerability leading to arbitrary writes to SMRAM.			
etoile_web_design -- ultimate_reviews	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Etoile Web Design Ultimate Reviews allows Stored XSS.This issue affects Ultimate Reviews: from n/a through 3.2.8.	2024-03-15	7.1	CVE-2024-25597
faronics -- deep_freeze_server_standard	A search path or unquoted item vulnerability in Faronics Deep Freeze Server Standard, which affects versions 8.30.020.4627 and earlier. This vulnerability affects the DFServ.exe file. An attacker with local user privileges could exploit this vulnerability to replace the legitimate DFServ.exe service executable with a malicious file of the same name and located in a directory that has a higher priority than the legitimate directory. Thus, when the service starts, it will run the malicious file instead of the legitimate executable, allowing the attacker to execute arbitrary code, gain unauthorized access to the compromised system or stop the service from running.	2024-03-12	7.8	CVE-2024-1618 cve-
fortinet -- forticlient_endpoint_management_server	A improper neutralization of formula elements in a csv file in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.10, 6.4.0 through 6.4.9, 6.2.0 through 6.2.9, 6.0.0 through 6.0.8 allows attacker to execute unauthorized code or commands via specially crafted packets.	2024-03-12	8.8	CVE-2023-47534
fortinet -- forticlient_enterprise_management_server	A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, FortiClientEMS 7.0.1 through 7.0.10 allows attacker to execute unauthorized code or commands via specially crafted packets.	2024-03-12	9.8	CVE-2023-48788
fortinet -- fortimanager	A improper access control in Fortinet FortiManager version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.10, version 6.4.0 through 6.4.13, 6.2 all versions allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.	2024-03-12	9.8	CVE-2023-36554
fortinet -- fortios	An improper authentication vulnerability [CWE-287] in FortiOS versions 7.4.1 and below, versions 7.2.6 and below, and versions 7.0.12 and below when configured with FortiAuthenticator in HA may allow a readonly user to gain read-write access via successive login attempts.	2024-03-12	7.5	CVE-2023-46717
fortinet -- fortiproxy	A out-of-bounds write in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.	2024-03-12	9.8	CVE-2023-42789
fortinet -- fortiproxy	A stack-based buffer overflow in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.	2024-03-12	8.1	CVE-2023-42790
fortra -- filecatalyst	A directory traversal within the 'ftpservlet' of the FileCatalyst Workflow Web Portal allows files to be uploaded outside of the intended 'uploadtemp' directory with a specially crafted POST request. In situations where a file is successfully uploaded to web portal's DocumentRoot, specially crafted JSP files could be used to execute code, including web shells.	2024-03-13	9.8	CVE-2024-25153
freescout-helpdesk -- freescout	FreeScout is an open source help desk and shared inbox built with PHP. A vulnerability has been identified in the Free Scout Application, which exposes SMTP server credentials used by an organization in the application to users of the application. This issue arises from the application storing complete stack traces of exceptions in its database. The sensitive information is then inadvertently disclosed to users via the `/conversation/ajax-html/send_log?folder_id=&thread_id={id}` endpoint. The stack trace reveals value of parameters, including the username and password, passed to the `Swift_Transport_Esmtp_Auth_LoginAuthenticator->authenticate()` function. Exploiting this vulnerability allows an attacker to gain unauthorized access to SMTP server credentials. With this sensitive information in hand, the attacker can potentially send unauthorized emails from the compromised SMTP server, posing a severe threat to the confidentiality and integrity of email communications. This could lead to targeted attacks on both the application users and the organization itself, compromising the security of email exchange servers. This issue has been addressed in version 1.8.124. Users are advised to upgrade. Users unable to upgrade should adopt the following measures: 1. Avoid Storing Complete Stack Traces, 2. Implement redaction mechanisms to filter and exclude sensitive information, and 3. Review and enhance the application's logging practices.	2024-03-12	7.1	CVE-2024-28186

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
givewp -- give	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GiveWP Give allows Reflected XSS.This issue affects Give: from n/a through 3.3.1.	2024-03-15	7.1	CVE-2024-27987
go-vela -- worker	Vela is a Pipeline Automation (CI/CD) framework built on Linux container technology written in Golang. Vela pipelines can use variable substitution combined with insensitive fields like `parameters`, `image` and `entrypoint` to inject secrets into a plugin/image and - by using common substitution string manipulation - can bypass log masking and expose secrets without the use of the commands block. This unexpected behavior primarily impacts secrets restricted by the "no commands" option. This can lead to unintended use of the secret value, and increased risk of exposing the secret during image execution bypassing log masking. **To exploit this** the pipeline author must be supplying the secrets to a plugin that is designed in such a way that will print those parameters in logs. Plugin parameters are not designed for sensitive values and are often intentionally printed throughout execution for informational/debugging purposes. Parameters should therefore be treated as insensitive. While Vela provides secrets masking, secrets exposure is not entirely solved by the masking process. A docker image (plugin) can easily expose secrets if they are not handled properly, or altered in some way. There is a responsibility on the end-user to understand how values injected into a plugin are used. This is a risk that exists for many CICD systems (like GitHub Actions) that handle sensitive runtime variables. Rather, the greater risk is that users who restrict a secret to the "no commands" option and use image restriction can still have their secret value exposed via substitution tinkering, which turns the image and command restrictions into a false sense of security. This issue has been addressed in version 0.23.2. Users are advised to upgrade. Users unable to upgrade should not provide sensitive values to plugins that can potentially expose them, especially in `parameters` that are not intended to be used for sensitive values, ensure plugins (especially those that utilize shared secrets) follow best practices to avoid logging parameters that are expected to be sensitive, minimize secrets with `pull_request` events enabled, as this allows users to change pipeline configurations and pull in secrets to steps not typically part of the CI process, make use of the build approval setting, restricting builds from untrusted users, and limit use of shared secrets, as they are less restrictive to access by nature.	2024-03-12	7.7	CVE-2024-28236
hammadh -- play.ht_-_make_your_blog_posts_accessible_with_text_to_speech_audio	The Play.ht - Make Your Blog Posts Accessible With Text to Speech Audio plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.6.4 via deserialization of untrusted input from the play_podcast_data post meta. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-03-13	8.8	CVE-2024-1772
hopsoft -- turbo_boost-commands	turbo_boost-commands is a set of commands to help you build robust reactive applications with Rails & Hotwire. TurboBoost Commands has existing protections in place to guarantee that only public methods on Command classes can be invoked; however, the existing checks aren't as robust as they should be. It's possible for a sophisticated attacker to invoke more methods than should be permitted depending on the the strictness of authorization checks that individual applications enforce. Being able to call some of these methods can have security implications. Commands verify that the class must be a `Command` and that the method requested is defined as a public method; however, this isn't robust enough to guard against all unwanted code execution. The library should more strictly enforce which methods are considered safe before allowing them to be executed. This issue has been addressed in versions 0.1.3, and 0.2.2. Users are advised to upgrade. Users unable to upgrade should see the repository GHSA for workaround advice.	2024-03-14	8.1	CVE-2024-28181
ibm -- i	Db2 for IBM i 7.2, 7.3, 7.4, and 7.5 infrastructure could allow a local user to gain elevated privileges due to an unqualified library call. A malicious actor could cause user-controlled code to run with administrator privilege. IBM X-Force ID: 280203.	2024-03-14	8.4	CVE-2024-22346
ibm -- maximo_asset_management	IBM Maximo Application Suite 7.6.1.3 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 284566.	2024-03-14	8.2	CVE-2024-27266
intumit -- smartrobot	Intumit SmartRobot uses a fixed encryption key for authentication. Remote attackers can use this key to encrypt a string composed of the user's name and timestamp to generate an authentication code. With this authentication code, they	2024-03-13	9.8	CVE-2024-2413 twcert@cert.org.tw

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	can obtain administrator privileges and subsequently execute arbitrary code on the remote server using built-in system functionality.			
inunosinsi -- soycms	SOY CMS is an open source CMS (content management system) that allows you to build blogs and online shops. SOY CMS versions prior to 3.14.2 are vulnerable to an OS Command Injection vulnerability within the file upload feature when accessed by an administrator. The vulnerability enables the execution of arbitrary OS commands through specially crafted file names containing a semicolon, affecting the jpegoptim functionality. This vulnerability has been patched in version 3.14.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-11	7.2	CVE-2024-28187
jfrog -- artifactory	JFrog Artifactory versions below 7.77.7, 7.82.1, are vulnerable to DOM-based cross-site scripting due to improper handling of the import override mechanism.	2024-03-13	8.8	CVE-2024-2247 reefs@jfrog.com
joel_starnes -- postmash_-_custom_post_order	Cross Site Scripting (XSS) vulnerability in Joel Starnes postMash - custom post order allows Reflected XSS.This issue affects postMash - custom post order: from n/a through 1.2.0.	2024-03-15	7.1	CVE-2024-27196
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability classified as critical was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected by this vulnerability is an unknown functionality of the file /login.php. The manipulation of the argument email leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256951. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-15	7.3	CVE-2024-2514
manageengine_ -- manageengine_desktop_central	Unrestricted file upload vulnerability in ManageEngine Desktop Central affecting version 9, build 90055. This vulnerability could allow a remote attacker to upload a malicious file to the system without any credentials provided.	2024-03-11	9.8	CVE-2024-2370 cve-
mattermost -- mattermost	Mattermost versions 8.1.x before 8.1.10, 9.2.x before 9.2.6, 9.3.x before 9.3.2, and 9.4.x before 9.4.3 fail to correctly verify account ownership when switching from email to SAML authentication, allowing an authenticated attacker to take over other user accounts via a crafted switch request under specific conditions.	2024-03-15	8.8	CVE-2024-2450
microsoft -- azure_data_studio	Azure Data Studio Elevation of Privilege Vulnerability	2024-03-12	7.3	CVE-2024-26203
microsoft -- azure_kubernetes_service	Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability	2024-03-12	9	CVE-2024-21400
microsoft -- azure_sdk	Azure SDK Spoofing Vulnerability	2024-03-12	7.5	CVE-2024-21421
microsoft -- microsoft_365_apps_for_enterprise	Microsoft Office Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-26199
microsoft -- microsoft_authenticator	Microsoft Authenticator Elevation of Privilege Vulnerability	2024-03-12	7.1	CVE-2024-21390
microsoft -- microsoft_dynamics_365_(on-premises)_version_9.1	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2024-03-12	7.6	CVE-2024-21419
microsoft -- microsoft_exchange_server_2019_cumulative_update_14	Microsoft Exchange Server Remote Code Execution Vulnerability	2024-03-12	8.8	CVE-2024-26198
microsoft -- microsoft_outlook	Outlook for Android Information Disclosure Vulnerability	2024-03-12	7.5	CVE-2024-26204

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_for_android				
microsoft -- microsoft_sharepoint_enterprise_server_2016	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-03-12	7.8	CVE-2024-21426
microsoft -- microsoft_visual_studio_2022_version_17.9	.NET and Visual Studio Denial of Service Vulnerability	2024-03-12	7.5	CVE-2024-21392
microsoft -- microsoft_visual_studio_2022_version_17.9	Microsoft QUIC Denial of Service Vulnerability	2024-03-12	7.5	CVE-2024-26190
microsoft -- skype_for_consumer	Skype for Consumer Remote Code Execution Vulnerability	2024-03-12	8.8	CVE-2024-21411
microsoft -- software_for_open_networking_in_the_cloud_(sonic)	Software for Open Networking in the Cloud (SONiC) Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-21418
microsoft -- sql_server_backend_for_django	Microsoft Django Backend for SQL Server Remote Code Execution Vulnerability	2024-03-12	8.8	CVE-2024-26164
microsoft -- system_center_operations_manager_(scom)_2019	Open Management Infrastructure (OMI) Remote Code Execution Vulnerability	2024-03-12	9.8	CVE-2024-21334
microsoft -- system_center_operations_manager_(scom)_2019	Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-21330
microsoft -- visual_studio_code	Visual Studio Code Elevation of Privilege Vulnerability	2024-03-12	8.8	CVE-2024-26165
microsoft -- windows_10_version_1809	Windows Hyper-V Remote Code Execution Vulnerability	2024-03-12	8.1	CVE-2024-21407
microsoft -- windows_10_version_1809	Microsoft ODBC Driver Remote Code Execution Vulnerability	2024-03-12	8.8	CVE-2024-21440
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-03-12	8.8	CVE-2024-21441
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-03-12	8.8	CVE-2024-21444
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-03-12	8.8	CVE-2024-21450
microsoft -- windows_10_versi	Microsoft ODBC Driver Remote Code Execution Vulnerability	2024-03-12	8.8	CVE-2024-21451

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
on_1809				
microsoft -- windows_10_version_1809	Microsoft ODBC Driver Remote Code Execution Vulnerability	2024-03-12	8.8	CVE-2024-26159
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-03-12	8.8	CVE-2024-26161
microsoft -- windows_10_version_1809	Microsoft ODBC Driver Remote Code Execution Vulnerability	2024-03-12	8.8	CVE-2024-26162
microsoft -- windows_10_version_1809	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-03-12	8.8	CVE-2024-26166
microsoft -- windows_10_version_1809	Windows Kerberos Security Feature Bypass Vulnerability	2024-03-12	7.5	CVE-2024-21427
microsoft -- windows_10_version_1809	Windows Update Stack Elevation of Privilege Vulnerability	2024-03-12	7	CVE-2024-21432
microsoft -- windows_10_version_1809	Windows Print Spooler Elevation of Privilege Vulnerability	2024-03-12	7	CVE-2024-21433
microsoft -- windows_10_version_1809	Microsoft Windows SCSI Class System File Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-21434
microsoft -- windows_10_version_1809	Windows Installer Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-21436
microsoft -- windows_10_version_1809	Windows Graphics Component Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-21437
microsoft -- windows_10_version_1809	Microsoft AllJoyn API Denial of Service Vulnerability	2024-03-12	7.5	CVE-2024-21438
microsoft -- windows_10_version_1809	Windows Telephony Server Elevation of Privilege Vulnerability	2024-03-12	7	CVE-2024-21439
microsoft -- windows_10_version_1809	Windows Kernel Elevation of Privilege Vulnerability	2024-03-12	7.3	CVE-2024-21443
microsoft -- windows_10_version_1809	NTFS Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-21446
microsoft -- windows_10_version_1809	Windows Error Reporting Service Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-26169
microsoft -- windows_10_versi	Windows Kernel Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-26173

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
on_1809				
microsoft -- windows_10_version_1809	Windows Kernel Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-26176
microsoft -- windows_10_version_1809	Windows Kernel Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-26178
microsoft -- windows_10_version_1809	Windows Kernel Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-26182
microsoft -- windows_11_version_22h2	Windows OLE Remote Code Execution Vulnerability	2024-03-12	8.8	CVE-2024-21435
microsoft -- windows_server_2022	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability	2024-03-12	7.8	CVE-2024-21431
microsoft -- windows_server_2022	Windows USB Print Driver Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-21442
microsoft -- windows_server_2022	Windows USB Print Driver Elevation of Privilege Vulnerability	2024-03-12	7	CVE-2024-21445
microsoft -- windows_server_2022	Windows Composite Image File System (CimFS) Elevation of Privilege Vulnerability	2024-03-12	7.8	CVE-2024-26170
mitsubishi_electric_corporation -- melsec-q_series_q03udecpu	Incorrect Pointer Scaling vulnerability in Mitsubishi Electric Corporation MELSEC-Q Series and MELSEC-L Series CPU modules allows a remote unauthenticated attacker to read arbitrary information from a target product or execute malicious code on a target product by sending a specially crafted packet.	2024-03-15	9.8	CVE-2024-0802
mitsubishi_electric_corporation -- melsec-q_series_q03udecpu	Integer Overflow or Wraparound vulnerability in Mitsubishi Electric Corporation MELSEC-Q Series and MELSEC-L Series CPU modules allows a remote unauthenticated attacker to execute malicious code on a target product by sending a specially crafted packet.	2024-03-15	9.8	CVE-2024-0803
mitsubishi_electric_corporation -- melsec-q_series_q03udecpu	Incorrect Pointer Scaling vulnerability in Mitsubishi Electric Corporation MELSEC-Q Series and MELSEC-L Series CPU modules allows a remote unauthenticated attacker to execute malicious code on a target product by sending a specially crafted packet.	2024-03-15	9.8	CVE-2024-1915
mitsubishi_electric_corporation -- melsec-q_series_q03udecpu	Integer Overflow or Wraparound vulnerability in Mitsubishi Electric Corporation MELSEC-Q Series and MELSEC-L Series CPU modules allows a remote unauthenticated attacker to execute malicious code on a target product by sending a specially crafted packet.	2024-03-15	9.8	CVE-2024-1916
mitsubishi_electric_corporation -- melsec-q_series_q03udecpu	Integer Overflow or Wraparound vulnerability in Mitsubishi Electric Corporation MELSEC-Q Series and MELSEC-L Series CPU modules allows a remote unauthenticated attacker to execute malicious code on a target product by sending a specially crafted packet.	2024-03-15	9.8	CVE-2024-1917

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mndpsingh287 -- file_manager	The File Manager and File Manager Pro plugins for WordPress are vulnerable to Directory Traversal in versions up to, and including version 7.2.1 (free version) and 8.3.4 (Pro version) via the target parameter in the mk_file_folder_manager_action_callback_shortcode function. This makes it possible for attackers to read the contents of arbitrary files on the server, which can contain sensitive information and to upload files into directories other than the intended directory for file uploads. The free version requires Administrator access for this vulnerability to be exploitable. The Pro version allows a file manager to be embedded via a shortcode and also allows admins to grant file handling privileges to other user levels, which could lead to this vulnerability being exploited by lower-level users.	2024-03-13	9.9	CVE-2023-6825
mostafas1990 -- wp_statistics	The WP Statistics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the URL search parameter in all versions up to, and including, 14.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	7.2	CVE-2024-2194
movistar_ -- router_movistar_4g	The primary channel is unprotected on Movistar 4G router affecting E version S_WLD71-T1_v2.0.201820. This device has the 'adb' service open on port 5555 and provides access to a shell with root privileges.	2024-03-13	8.8	CVE-2024-2414 cve-
movistar_ -- router_movistar_4g	Command injection vulnerability in Movistar 4G router affecting version ES_WLD71-T1_v2.0.201820. This vulnerability allows an authenticated user to execute commands inside the router by making a POST request to the URL '/cgi-bin/gui.cgi'.	2024-03-13	7.8	CVE-2024-2415 cve-
n/a -- 4th_generation_intel(r)_xeon(r)_processors_when_using_intel(r)_sgx_or_intel(r)_tdx	On-chip debug and test interface with improper access control in some 4th Generation Intel(R) Xeon(R) Processors when using Intel(R) SGX or Intel(R) TDX may allow a privileged user to potentially enable escalation of privilege via local access.	2024-03-14	7.2	CVE-2023-32666
n/a -- intel(r)_processors	Race condition in BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	2024-03-14	7.2	CVE-2023-32282
ni -- labview	An out of bounds write due to a missing bounds check in LabVIEW may result in remote code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	2024-03-11	7.8	CVE-2024-23608
ni -- labview	An improper error handling vulnerability in LabVIEW may result in remote code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	2024-03-11	7.8	CVE-2024-23609
ni -- labview	An out of bounds write due to a missing bounds check in LabVIEW may result in remote code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	2024-03-11	7.8	CVE-2024-23610
ni -- labview	An out of bounds write due to a missing bounds check in LabVIEW may result in remote code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	2024-03-11	7.8	CVE-2024-23611
ni -- labview	An improper error handling vulnerability in LabVIEW may result in remote code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	2024-03-11	7.8	CVE-2024-23612
open-metadata -- openmetadata	OpenMetadata is a unified platform for discovery, observability, and governance powered by a central metadata repository, in-depth lineage, and seamless team collaboration. `CompiledRule::validateExpression` is also called from `PolicyRepository.prepare`. `prepare()` is called from `EntityRepository.prepareInternal()` which, in turn, gets called from `EntityResource.createOrUpdate()`. Note that even though there is an authorization check (`authorizer.authorize()`), it gets called after `prepareInternal()` gets called and therefore after the SpEL expression has been evaluated. In order to reach this method, an attacker can send a PUT request to `/api/v1/policies` which gets handled by `PolicyResource.createOrUpdate()`. This vulnerability was discovered with the help of CodeQL's Expression language injection (Spring) query and is also tracked as `GHSL-2023-252`. This issue may lead	2024-03-15	9.4	CVE-2024-28253

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to Remote Code Execution and has been addressed in version 1.3.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.			
open-metadata -- openmetadata	OpenMetadata is a unified platform for discovery, observability, and governance powered by a central metadata repository, in-depth lineage, and seamless team collaboration. The `JwtFilter` handles the API authentication by requiring and verifying JWT tokens. When a new request comes in, the request's path is checked against this list. When the request's path contains any of the excluded endpoints the filter returns without validating the JWT. Unfortunately, an attacker may use Path Parameters to make any path contain any arbitrary strings. For example, a request to `GET /api/v1;v1%2fusers%2flogin/events/subscriptions/validation/condition/111` will match the excluded endpoint condition and therefore will be processed with no JWT validation allowing an attacker to bypass the authentication mechanism and reach any arbitrary endpoint, including the ones listed above that lead to arbitrary SpEL expression injection. This bypass will not work when the endpoint uses the `SecurityContext.getUserPrincipal()` since it will return `null` and will throw an NPE. This issue may lead to authentication bypass and has been addressed in version 1.2.4. Users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as `GHSL-2023-237`.	2024-03-15	9.8	CVE-2024-28255
open-metadata -- openmetadata	OpenMetadata is a unified platform for discovery, observability, and governance powered by a central metadata repository, in-depth lineage, and seamless team collaboration. The `?AlertUtil::validateExpression` method evaluates an SpEL expression using `getValue` which by default uses the `StandardEvaluationContext`, allowing the expression to reach and interact with Java classes such as `java.lang.Runtime`, leading to Remote Code Execution. The `/api/v1/events/subscriptions/validation/condition/<expression>` endpoint passes user-controlled data `AlertUtil::validateExpession` allowing authenticated (non-admin) users to execute arbitrary system commands on the underlaying operating system. In addition, there is a missing authorization check since `Authorizer.authorize()` is never called in the affected path and, therefore, any authenticated non-admin user is able to trigger this endpoint and evaluate arbitrary SpEL expressions leading to arbitrary command execution. This vulnerability was discovered with the help of CodeQL's Expression language injection (Spring) query and is also tracked as `GHSL-2023-235`. This issue may lead to Remote Code Execution and has been addressed in version 1.2.4. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-15	8.8	CVE-2024-28254
open-metadata -- openmetadata	OpenMetadata is a unified platform for discovery, observability, and governance powered by a central metadata repository, in-depth lineage, and seamless team collaboration. Similarly to the GHSL-2023-250 issue, `AlertUtil::validateExpression` is also called from `EventSubscriptionRepository.prepare()`, which can lead to Remote Code Execution. `prepare()` is called from `EntityRepository.prepareInternal()` which, in turn, gets called from `EntityResource.createOrUpdate()`. Note that, even though there is an authorization check (`authorizer.authorize()`), it gets called after `prepareInternal()` gets called and, therefore, after the SpEL expression has been evaluated. In order to reach this method, an attacker can send a PUT request to `/api/v1/events/subscriptions` which gets handled by `EventSubscriptionResource.createOrUpdateEventSubscription()`. This vulnerability was discovered with the help of CodeQL's Expression language injection (Spring) query. This issue may lead to Remote Code Execution and has been addressed in version 1.2.4. Users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as `GHSL-2023-251`.	2024-03-15	8.8	CVE-2024-28847
open-metadata -- openmetadata	OpenMetadata is a unified platform for discovery, observability, and governance powered by a central metadata repository, in-depth lineage, and seamless team collaboration. The `?CompiledRule::validateExpression` method evaluates an SpEL expression using an `StandardEvaluationContext`, allowing the expression to reach and interact with Java classes such as `java.lang.Runtime`, leading to Remote Code Execution. The `/api/v1/policies/validation/condition/<expression>` endpoint passes user-controlled data `CompiledRule::validateExpession` allowing authenticated (non-admin) users to execute arbitrary system commands on the underlaying operating system. In addition, there is a missing authorization check since `Authorizer.authorize()` is never called in the affected path and therefore any authenticated non-admin user is able to trigger this endpoint and evaluate arbitrary SpEL expressions leading to arbitrary command execution. This vulnerability was discovered with the help of CodeQL's Expression language injection (Spring) query and is also tracked as `GHSL-2023-236`. This issue may lead	2024-03-15	8.8	CVE-2024-28848

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to Remote Code Execution and has been resolved in version 1.2.4. Users are advised to upgrade. There are no known workarounds for this vulnerability.			
opentext -- netiq_privileged_account_manager	Allocation of Resources Without Limits or Throttling vulnerability in OpenText NetIQ Privileged Account Manager on Linux, Windows, 64 bit allows Flooding.This issue affects NetIQ Privileged Account Manager: before 3.7.0.2.	2024-03-13	8.6	CVE-2020-11862
opentextâ„¢ -- exceed_turbo_x	Improper authentication vulnerability in OpenText™ Exceed Turbo X affecting versions 12.5.0 and 12.5.1. The vulnerability could allow disclosure of restricted information in unauthenticated RPC.	2024-03-13	8.6	CVE-2023-38534
papercut -- papercut_ng,_papercut_mf	This allows attackers to use a maliciously formed API request to gain access to an API authorization level with elevated privileges. This applies to a small subset of PaperCut NG/MF API calls.	2024-03-14	8.6	CVE-2024-1222
papercut -- papercut_ng,_papercut_mf	This vulnerability potentially allows unauthorized write operations which may lead to remote code execution. An attacker must already have authenticated admin access and knowledge of both an internal system identifier and details of another valid user to exploit this.	2024-03-14	7.2	CVE-2024-1654
papercut -- papercut_ng,_papercut_mf	This vulnerability allows an already authenticated admin user to create a malicious payload that could be leveraged for remote code execution on the server hosting the PaperCut NG/MF application server.	2024-03-14	7.2	CVE-2024-1882
payu -- payu_india	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PayU PayU India allows Reflected XSS.This issue affects PayU India: from n/a through 3.8.2.	2024-03-15	7.1	CVE-2024-27193
peering-manager -- peering-manager	Peering Manager is a BGP session management tool. There is a Server Side Template Injection vulnerability that leads to Remote Code Execution in Peering Manager <=1.8.2. As a result arbitrary commands can be executed on the operating system that is running Peering Manager. This issue has been addressed in version 1.8.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-12	8.1	CVE-2024-28114
pegasystems -- pega_platform	Pega Platform from 6.x to 8.8.4 is affected by an XXE issue with PDF Generation.	2024-03-14	7.7	CVE-2023-50168 security@pega.com
phlex-ruby -- phlex	phlex is an open source framework for building object-oriented views in Ruby. There is a potential cross-site scripting (XSS) vulnerability that can be exploited via maliciously crafted user data. This was due to improper case-sensitivity in the code that was meant to prevent these attacks. If you render an `<a>` tag with an `href` attribute set to a user-provided link, that link could potentially execute JavaScript when clicked by another user. If you splat user-provided attributes when rendering any HTML tag, malicious event attributes could be included in the output, executing JavaScript when the events are triggered by another user. Patches are available on RubyGems for all 1.x minor versions. Users are advised to upgrade. Users unable to upgrade should consider configuring a content security policy that does not allow `unsafe-inline`.	2024-03-11	7.1	CVE-2024-28199
phoenix_contact -- charx_sec-3000	An unauthenticated remote attacker can modify configurations to perform a remote code execution due to a missing authentication for a critical function.	2024-03-12	9.8	CVE-2024-25995
phoenix_contact -- charx_sec-3000	An unauthenticated local attacker can perform a privilege escalation due to improper input validation in the OCPP agent service.	2024-03-12	8.4	CVE-2024-25999
phoenix_contact -- charx_sec-3000	An unauthenticated remote attacker can influence the communication due to the lack of encryption of sensitive data via a MITM. Charging is not affected.	2024-03-12	8.7	CVE-2024-26288
phoenix_contact -- charx_sec-3000	An unauthenticated remote attacker can perform a command injection in the OCPP Service with limited privileges due to improper input validation.	2024-03-12	7.3	CVE-2024-25998
phoenix_contact -- charx_sec-3000	An unauthenticated remote attacker can write memory out of bounds due to improper input validation in the MQTT stack. The brute force attack is not always successful because of memory randomization.	2024-03-12	7.4	CVE-2024-26001
phoenix_contact -- charx_sec-3000	An improper input validation in the Qualcom plctool allows a local attacker with low privileges to gain root access by changing the ownership of specific files.	2024-03-12	7.8	CVE-2024-26002
phoenix_contact -- charx_sec-3000	An unauthenticated remote attacker can DoS the control agent due to a out-of-bounds read which may prevent or disrupt the charging functionality.	2024-03-12	7.5	CVE-2024-26003

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phoenix_contact -- charx_sec-3000	An unauthenticated remote attacker can DoS a control agent due to access of a uninitialized pointer which may prevent or disrupt the charging functionality.	2024-03-12	7.5	CVE-2024-26004
pickplugins -- post_grid,_form_maker,_popup_maker,_woocommerce_blocks,_post_blocks,_post_carousel_-_combo_blocks	The Post Grid Combo - 36+ Gutenberg Blocks plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.2.68 via the 'get_posts' REST API Endpoint. This makes it possible for unauthenticated attackers to extract sensitive data including full draft posts and password protected posts, as well as the password for password-protected posts.	2024-03-12	7.5	CVE-2023-7072
pixelemu -- terraclassifieds	Cross-Site Request Forgery (CSRF) vulnerability in Pixelemu TerraClassifieds.This issue affects TerraClassifieds: from n/a through 2.0.3.	2024-03-16	8.8	CVE-2023-51474
plv8 -- plv8	A user who can create objects in a database with plv8 3.2.1 installed is able to cause deferred triggers to execute as the Superuser during autovacuum.	2024-03-14	7.2	CVE-2024-1713
projectdiscovery -- nuclei	projectdiscovery/nuclei is a fast and customisable vulnerability scanner based on simple YAML based DSL. A significant security oversight was identified in Nuclei v3, involving the execution of unsigned code templates through workflows. This vulnerability specifically affects users utilizing custom workflows, potentially allowing the execution of malicious code on the user's system. This advisory outlines the impacted users, provides details on the security patch, and suggests mitigation strategies. The vulnerability is addressed in Nuclei v3.2.0. Users are strongly recommended to update to this version to mitigate the security risk. Users should refrain from using custom workflows if unable to upgrade immediately. Only trusted, verified workflows should be executed.	2024-03-15	7.4	CVE-2024-27920
pterodactyl -- wings	Wings is the server control plane for Pterodactyl Panel. This vulnerability impacts anyone running the affected versions of Wings. The vulnerability can potentially be used to access files and directories on the host system. The full scope of impact is exactly unknown, but reading files outside of a server's base directory (sandbox root) is possible. In order to use this exploit, an attacker must have an existing "server" allocated and controlled by Wings. Details on the exploitation of this vulnerability are embargoed until March 27th, 2024 at 18:00 UTC. In order to mitigate this vulnerability, a full rewrite of the entire server filesystem was necessary. Because of this, the size of the patch is massive, however effort was made to reduce the amount of breaking changes. Users are advised to update to version 1.11.9. There are no known workarounds for this vulnerability.	2024-03-13	9.9	CVE-2024-27102
realmag777 -- husky_-_products_filter_professional_for_woocommerce	The HUSKY - Products Filter for WooCommerce Professional plugin for WordPress is vulnerable to SQL Injection via the 'name' parameter in the woof shortcode in all versions up to, and including, 1.3.5.2 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 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.	2024-03-15	8.8	CVE-2024-1795
rejetto_ -- http_file_server_	The software does not neutralize or incorrectly neutralizes certain characters before the data is included in outgoing HTTP headers. The inclusion of invalidated data in an HTTP header allows an attacker to specify the full HTTP response represented by the browser. An attacker could control the response and craft attacks such as cross-site scripting and cache poisoning attacks.	2024-03-12	7.5	CVE-2024-1226 cve-
renventura -- woocommerce_add_to_cart_custom_redirect	The WooCommerce Add to Cart Custom Redirect plugin for WordPress is vulnerable to unauthorized modification of data and loss of data due to a missing capability check on the 'wcr_dismiss_admin_notice' function in all versions up to, and including, 1.2.13. This makes it possible for authenticated attackers, with contributor access and above, to update the values of arbitrary site options to 'dismissed'.	2024-03-13	8.1	CVE-2024-1862
root3nl -- supportapp	Support App is an opensource application specialized in managing Apple devices. It's possible to abuse a vulnerability inside the postinstall installer script to make the installer execute arbitrary code as root. The cause of the vulnerability is the fact that the shebang `#!/bin/zsh` is being used. When the installer is executed it asks for the users password to be executed as root. However, it'll still be using the $HOME of the user and therefore loading the file `$HOME/.zshenv` when the `postinstall` script is executed. An attacker could add malicious code to `$HOME/.zshenv` and it will be executed when the app is installed. An attacker may leverage this vulnerability to escalate privilege on the system. This issue has	2024-03-14	7.3	CVE-2024-27301

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	been addressed in version 2.5.1 Rev 2. All users are advised to upgrade. There are no known workarounds for this vulnerability.			
sagemcom -- fast3686_v2_vodafone	Insufficient session timeout vulnerability in the FAST3686 V2 Vodafone router from Sagemcom. This vulnerability could allow a local attacker to access the administration panel without requiring login credentials. This vulnerability is possible because the 'Login.asp and logout.asp' files do not handle session details correctly.	2024-03-14	7.7	CVE-2024-1623 cve-
sandi_verdev -- watermark_reloaded	Cross-Site Request Forgery (CSRF) vulnerability in Sandi Verdev Watermark RELOADED allows Stored XSS.This issue affects Watermark RELOADED: from n/a through 1.3.5.	2024-03-16	7.1	CVE-2024-27195
sandisk -- privateaccess_windows_app	A potential DLL hijacking vulnerability in the SanDisk PrivateAccess application for Windows that could lead to arbitrary code execution in the context of the system user. This vulnerability is only exploitable locally if an attacker has access to a copy of the user's vault or has already gained access into a user's system. This attack is limited to the system in context and cannot be propagated.	2024-03-13	7.9	CVE-2024-22167 psirt@wdc.com
santesoft -- sante_fft_imaging	In Santesoft Sante FFT Imaging versions 1.4.1 and prior once a user opens a malicious DCM file on affected FFT Imaging installations, a local attacker could perform an out-of-bounds write, which could allow for arbitrary code execution.	2024-03-11	7.8	CVE-2024-1696
sap_se -- sap_netweaver_as_java_(administrator_log_viewer_plug-in)	SAP NetWeaver Administrator AS Java (Administrator Log Viewer plug-in) - version 7.50, allows an attacker with high privileges to upload potentially dangerous files which leads to command injection vulnerability. This would enable the attacker to run commands which can cause high impact on confidentiality, integrity and availability of the application.	2024-03-12	9.1	CVE-2024-22127
scott_reilly -- configure_smtp	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Scott Reilly Configure SMTP allows Reflected XSS.This issue affects Configure SMTP: from n/a through 3.1.	2024-03-15	7.1	CVE-2024-27192
siemens -- cerberus_pro_en_engineering_tool	A vulnerability has been identified in Cerberus PRO EN Engineering Tool (All versions < IP8), Cerberus PRO EN Fire Panel FC72x (All versions < IP8), Cerberus PRO EN X200 Cloud Distribution (All versions < V4.0.5016), Cerberus PRO EN X300 Cloud Distribution (All versions < V4.2.5015), Sinteso FS20 EN Engineering Tool (All versions < MP8), Sinteso FS20 EN Fire Panel FC20 (All versions < MP8), Sinteso FS20 EN X200 Cloud Distribution (All versions < V4.0.5016), Sinteso FS20 EN X300 Cloud Distribution (All versions < V4.2.5015), Sinteso Mobile (All versions < V3.0.0). The network communication library in affected systems does not validate the length of certain X.509 certificate attributes which might result in a stack-based buffer overflow. This could allow an unauthenticated remote attacker to execute code on the underlying operating system with root privileges.	2024-03-12	10	CVE-2024-22039
siemens -- cerberus_pro_en_engineering_tool	A vulnerability has been identified in Cerberus PRO EN Engineering Tool (All versions), Cerberus PRO EN Fire Panel FC72x (All versions < IP8 SR4), Cerberus PRO EN X200 Cloud Distribution (All versions < V4.3.5618), Cerberus PRO EN X300 Cloud Distribution (All versions < V4.3.5617), Sinteso FS20 EN Engineering Tool (All versions), Sinteso FS20 EN Fire Panel FC20 (All versions < MP8 SR4), Sinteso FS20 EN X200 Cloud Distribution (All versions < V4.3.5618), Sinteso FS20 EN X300 Cloud Distribution (All versions < V4.3.5617), Sinteso Mobile (All versions). The network communication library in affected systems insufficiently validates HMAC values which might result in a buffer overread. This could allow an unauthenticated remote attacker to crash the network service.	2024-03-12	7.5	CVE-2024-22040
siemens -- cerberus_pro_en_engineering_tool	A vulnerability has been identified in Cerberus PRO EN Engineering Tool (All versions), Cerberus PRO EN Fire Panel FC72x (All versions < IP8 SR4), Cerberus PRO EN X200 Cloud Distribution (All versions < V4.3.5618), Cerberus PRO EN X300 Cloud Distribution (All versions < V4.3.5617), Sinteso FS20 EN Engineering Tool (All versions), Sinteso FS20 EN Fire Panel FC20 (All versions < MP8 SR4), Sinteso FS20 EN X200 Cloud Distribution (All versions < V4.3.5618), Sinteso FS20 EN X300 Cloud Distribution (All versions < V4.3.5617), Sinteso Mobile (All versions). The network communication library in affected systems improperly handles memory buffers when parsing X.509 certificates. This could allow an unauthenticated remote attacker to crash the network service.	2024-03-12	7.5	CVE-2024-22041
siemens -- sentron_3kc_atc6_expansion_module_ethernet	A vulnerability has been identified in SENTRON 3KC ATC6 Expansion Module Ethernet (3KC9000-8TL75) (All versions). Affected devices expose an unused, unstable http service at port 80/tcp on the Modbus-TCP Ethernet. This could allow an attacker on the same Modbus network to create a denial of service condition that forces the device to reboot.	2024-03-12	7.5	CVE-2024-22044

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- simcenter_femap	A vulnerability has been identified in Simcenter Femap (All versions < V2306.0000). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted Catia MODEL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-22051)	2024-03-12	7.8	CVE-2024-27907
siemens -- sinema_remote_connect_client	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.1 SP1). The product places sensitive information into files or directories that are accessible to actors who are allowed to have access to the files, but not to the sensitive information. This information is also available via the web interface of the product.	2024-03-12	7.6	CVE-2024-22045
siemens -- sinema_remote_connect_server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2). The affected application consists of a web service that lacks proper access control for some of the endpoints. This could lead to unauthorized access to resources and potentially lead to code execution.	2024-03-12	9.8	CVE-2022-32257
smub -- giveaways_and_contests_by_rafflepress_-_get_more_website_traffic,_email_subscribers,_and_social_followers	The Giveaways and Contests by RafflePress - Get More Website Traffic, Email Subscribers, and Social Followers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'parent_url' parameter in all versions up to, and including, 1.12.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	7.2	CVE-2024-1935
softing -- edgeconnector	The affected product is vulnerable to a cleartext transmission of sensitive information vulnerability, which may allow an attacker to capture packets to craft their own requests.	2024-03-14	8	CVE-2024-0860
spring -- spring_framework	Applications that use UriComponentsBuilder in Spring Framework to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the parsed URL may be vulnerable to a open redirect https://cwe.mitre.org/data/definitions/601.html attack or to a SSRF attack if the URL is used after passing validation checks. This is the same as CVE-2024-22243 https://spring.io/security/cve-2024-22243 , but with different input.	2024-03-16	8.1	CVE-2024-22259
stimulusreflex -- stimulus_reflex	stimulus_reflex is a system to extend the capabilities of both Rails and Stimulus by intercepting user interactions and passing them to Rails over real-time websockets. In affected versions more methods than expected can be called on reflex instances. Being able to call some of them has security implications. To invoke a reflex a websocket message of the following shape is sent: `\"target\":\"[class_name]#[method_name]\",\"args\":[]`. The server will proceed to instantiate `reflex` using the provided `class_name` as long as it extends `StimulusReflex::Reflex`. It then attempts to call `method_name` on the instance with the provided arguments. This is problematic as `reflex.method method_name` can be more methods that those explicitly specified by the developer in their reflex class. A good example is the instance_variable_set method. This vulnerability has been patched in versions 3.4.2 and 3.5.0.rc4. Users unable to upgrade should: see the backing GHSA advisory for mitigation advice.	2024-03-12	8.8	CVE-2024-28121
storeapps -- news_announcement_scroll	The News Announcement Scroll plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 9.0.0 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 contributor-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-03-13	8.8	CVE-2023-5663
sygnoos -- social_media_share_buttons	The Social Media Share Buttons plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.1.0 via deserialization of untrusted input through the attachmentUrl parameter. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-03-16	8.8	CVE-2024-1685
tatvic -- conversios_-_google_analytics_4_(ga4),_meta_pixel_&_more_via_google_tag_manager_for_woocommerc	The Conversios - Google Analytics 4 (GA4), Meta Pixel & more Via Google Tag Manager For WooCommerce plugin for WordPress is vulnerable to SQL Injection via the 'valueData' parameter in all versions up to, and including, 6.9.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL	2024-03-13	8.8	CVE-2024-1203

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
e	queries into already existing queries that can be used to extract sensitive information from the database.			
tenda -- ac18	A vulnerability was found in Tenda AC18 15.03.05.05 and classified as critical. Affected by this issue is the function formSetSpeedWan of the file /goform/SetSpeedWan. The manipulation of the argument speed_dir leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256892. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-15	8.8	CVE-2024-2485
tenda -- ac18	A vulnerability was found in Tenda AC18 15.03.05.05. It has been classified as critical. This affects the function formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256893 was assigned to this vulnerability.	2024-03-15	8.8	CVE-2024-2486
tenda -- ac18	A vulnerability was found in Tenda AC18 15.03.05.05. It has been declared as critical. This vulnerability affects the function formSetDeviceName of the file /goform/SetOnlineDevName. The manipulation of the argument devName/mac leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-256894 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-15	8.8	CVE-2024-2487
tenda -- ac18	A vulnerability was found in Tenda AC18 15.03.05.05. It has been rated as critical. This issue affects the function formSetPPTPServer of the file /goform/SetPptpServerCfg. The manipulation of the argument startIP leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256895. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-15	8.8	CVE-2024-2488
tenda -- ac18	A vulnerability classified as critical has been found in Tenda AC18 15.03.05.05. Affected is the function formSetQosBand of the file /goform/SetNetControlList. The manipulation of the argument list leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256896. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-15	8.8	CVE-2024-2489
tenda -- ac18	A vulnerability classified as critical was found in Tenda AC18 15.03.05.05. Affected by this vulnerability is the function setSchedWifi of the file /goform/openSchedWifi. The manipulation of the argument schedStartTime/schedEndTime leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256897 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-15	8.8	CVE-2024-2490
themefusecom -- brizy_-_page_builder	The Brizy - Page Builder plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the storeImages function in all versions up to, and including, 2.4.40. This makes it possible for authenticated attackers, with contributor access or above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-03-13	8.8	CVE-2024-1311
themeum -- tutor_lms_-_elearning_and_online_course_solution	The Tutor LMS - eLearning and online course solution plugin for WordPress is vulnerable to time-based SQL Injection via the question_id parameter in all versions up to, and including, 2.6.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber/student access or higher, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-03-13	8.8	CVE-2024-1751
tibco_software_inc. -- tibco_ftl_-_enterprise_edition	The FTL Server component of TIBCO Software Inc.'s TIBCO FTL - Enterprise Edition contains a vulnerability that allows a low privileged attacker with network access to execute a privilege escalation on the affected ftlserver. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Enterprise Edition: versions 6.10.1 and below.	2024-03-12	8.8	CVE-2024-1138
tmccombs -- tls-listener	tls-listener is a rust lang wrapper around a connection listener to support TLS. With the default configuration of tls-listener, a malicious user can open 6.4 `TcpStream`s a second, sending 0 bytes, and can trigger a DoS. The default configuration options make any public service using `TlsListener::new()` vulnerable to a slow-loris DoS attack. This impacts any publicly accessible service using the default configuration of tls-listener in versions prior to 0.10.0. Users are advised to upgrade. Users	2024-03-15	7.5	CVE-2024-28854

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unable to upgrade may mitigate this by passing a large value, such as `usize::MAX` as the parameter to `Builder::max_handshakes`.			
totolink -- x6000r	A vulnerability, which was classified as critical, has been found in Totolink X6000R 9.4.0cu.852_20230719. This issue affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi of the component shttpd. The manipulation of the argument ip leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256313 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-10	8.8	CVE-2024-2353
ultimatemember -- ultimate_member_-_user_profile,_registration,_login,_member_directory,_content_restriction_&_membership_plugin	The Ultimate Member - User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to SQL Injection via the 'sorting' parameter in versions 2.1.3 to 2.8.2 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.	2024-03-13	9.8	CVE-2024-1071
ultimatemember -- ultimate_member_-_user_profile,_registration,_login,_member_directory,_content_restriction_&_membership_plugin	The Ultimate Member - User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the several parameters in all versions up to, and including, 2.8.3 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.	2024-03-13	7.2	CVE-2024-2123
ultimatemember -- ultimate_member_-_user_profile,_registration,_login,_member_directory,_content_restriction_&_membership_plugin	In FileCatalyst Direct 3.8.8 and earlier through 3.8.6, the web server does not properly sanitize illegal characters in a URL which is then displayed on a subsequent error page. A malicious actor could craft a URL which would then execute arbitrary code within an HTML script tag.	2024-03-13	7.2	CVE-2024-25155
wago -- controller_bacnet/ip	An unautheticated remote attacker could send specifically crafted packets to a affected device. If an authenticated user then views that data in a specific page of the web-based management a buffer overflow will be triggered to gain full access of the device.	2024-03-13	8.8	CVE-2015-10123
webtechstreet -- elementor_addon_elements	The Elementor Addon Elements plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.12.12 via the render function. This makes it possible for authenticated attackers, with contributor access or higher, to include the contents of arbitrary PHP files on the server, which may expose sensitive information.	2024-03-13	8.8	CVE-2024-1358
wp_codeus -- advanced_sermons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Codeus Advanced Sermons allows Reflected XSS.This issue affects Advanced Sermons: from n/a through 3.2.	2024-03-13	7.1	CVE-2024-27952
wpdevteam -- essential_addons_for_elementor_-_best_elementor_templates,_widgets,_kits_&_woocommerce_builders	The Essential Addons for Elementor - Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's event calendar widget in all versions up to, and including, 5.9.9 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.	2024-03-13	7.4	CVE-2024-1536
wpmudev -- hustle_-_email_marketing,_lead_generation,	The Hustle - Email Marketing, Lead Generation, Optins, Popups plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 7.8.3 via hardcoded API Keys. This makes it possible for unauthenticated attackers to extract sensitive data including PII.	2024-03-13	8.6	CVE-2024-0368

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_optins,_popups				
wpwax -- logo_showcase_ultimate_-_logo_carousel,_logo_slider_&_logo_grid	The Logo Showcase Ultimate - Logo Carousel, Logo Slider & Logo Grid plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.3.8 via deserialization via shortcode of untrusted input. This makes it possible for authenticated attackers, with contributor access and above, to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-03-13	7.5	CVE-2024-1951
wpwax -- post_grid,_slider_&_carousel_ultimate_-_with_shortcode,_gutenberg_block_&_elementor_widget	The Post Grid, Slider & Carousel Ultimate - with Shortcode, Gutenberg Block & Elementor Widget plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.6.7 via deserialization of untrusted input in the outpost_shortcode_metabox_markup function. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a PHP Object. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-03-13	8.8	CVE-2024-2006
wpwax -- product_carousel_slider_&_grid_ultimate_for_woocommerce	The Product Carousel Slider & Grid Ultimate for WooCommerce plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.9.7 via deserialization of untrusted input via shortcode. This makes it possible for authenticated attackers, with contributor access and above, to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-03-13	7.5	CVE-2024-1950
yooooomi -- your_spotify	your_spotify is an open source, self hosted Spotify tracking dashboard. YourSpotify versions < 1.8.0 use a hardcoded JSON Web Token (JWT) secret to sign authentication tokens. Attackers can use this well-known value to forge valid authentication tokens for arbitrary users. This vulnerability allows attackers to bypass authentication and authenticate as arbitrary YourSpotify users, including admin users. This issue has been addressed in version 1.8.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-13	9.1	CVE-2024-28194
yooooomi -- your_spotify	your_spotify is an open source, self hosted Spotify tracking dashboard. YourSpotify versions < 1.9.0 do not protect the API and login flow against Cross-Site Request Forgery (CSRF). Attackers can use this to execute CSRF attacks on victims, allowing them to retrieve, modify or delete data on the affected YourSpotify instance. Using repeated CSRF attacks, it is also possible to create a new user on the victim instance and promote the new user to instance administrator if a legitimate administrator visits a website prepared by an attacker. Note: Real-world exploitability of this vulnerability depends on the browser version and browser settings in use by the victim. This issue has been addressed in version 1.9.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-13	8.1	CVE-2024-28195
zephyrproject-rtos -- zephyr	Zephyr OS IP packet handling does not properly drop IP packets arriving on an external interface with a source address equal to 127.0.01 or the destination address.	2024-03-15	8.6	CVE-2023-7060 vulnerabilities@zephyrproject.org
zephyrproject-rtos -- zephyr	Privilege escalation in windows agent plugin in Checkmk before 2.2.0p23, 2.1.0p40 and 2.0.0 (EOL) allows local user to escalate privileges	2024-03-11	8.8	CVE-2024-0670
zitadel -- zitadel	Zitadel is an open source identity management system. Zitadel uses a cookie to identify the user agent (browser) and its user sessions. Although the cookie was handled according to best practices, it was accessible on subdomains of the ZITADEL instance. An attacker could take advantage of this and provide a malicious link hosted on the subdomain to the user to gain access to the victim's account in certain scenarios. A possible victim would need to login through the malicious link for this exploit to work. If the possible victim already had the cookie present, the attack would not succeed. The attack would further only be possible if there was an initial vulnerability on the subdomain. This could either be the attacker being able to control DNS or a XSS vulnerability in an application hosted on a subdomain. Versions 2.46.0, 2.45.1, and 2.44.3 have been patched. Zitadel recommends upgrading to the latest versions available in due course. Note that applying the patch will invalidate the current cookie and thus users will need to start a new session and existing sessions (user selection) will be empty. For self-hosted environments unable to upgrade to a patched version, prevent setting the following cookie name on subdomains of your Zitadel instance (e.g. within your WAF): `__Secure-zitadel-useragent`.	2024-03-11	7.5	CVE-2024-28197

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zoom_video_communications,_inc. -- zoom_rooms_client_for_windows	Improper access control in the installer for Zoom Rooms Client for Windows before version 5.17.5 may allow an authenticated user to conduct a denial of service via local access.	2024-03-13	7.2	CVE-2024-24693

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
10web -- photogallery	The current_url parameter of the AJAX call to the GalleryBox action of admin-ajax.php is vulnerable to reflected Cross Site Scripting. The value of the current_url parameter is embedded within an existing JavaScript within the response allowing arbitrary JavaScript to be inserted and executed. No authentication is required to exploit this issue. Note that other parameters within a AJAX call, such as image_id, must be valid for this vulnerability to be successfully exploited.	2024-03-26	6.1	CVE-2024-29832
10web -- photogallery	The image_id parameter of the AJAX call to the editimage_bwg action of admin-ajax.php is vulnerable to reflected Cross Site Scripting. The value of the image_id parameter is embedded within an existing JavaScript within the response allowing arbitrary JavaScript to be inserted and executed. The attacker must target a an authenticated user with permissions to access this component to exploit this issue.	2024-03-26	5.4	CVE-2024-29808
10web -- photogallery	The image_url parameter of the AJAX call to the editimage_bwg action of admin-ajax.php is vulnerable to reflected Cross Site Scripting. The value of the image_url parameter is embedded within an existing JavaScript within the response allowing arbitrary JavaScript to be inserted and executed. The attacker must target a an authenticated user with permissions to access this component to exploit this issue.	2024-03-26	5.4	CVE-2024-29809
10web -- photogallery	The thumb_url parameter of the AJAX call to the editimage_bwg action of admin-ajax.php is vulnerable to reflected Cross Site Scripting. The value of the thumb_url parameter is embedded within an existing JavaScript within the response allowing arbitrary JavaScript to be inserted and executed. The attacker must target a an authenticated user with permissions to access this component to exploit this issue.	2024-03-26	5.4	CVE-2024-29810
10web -- photogallery	The image upload component allows SVG files and the regular expression used to remove script tags can be bypassed by using a Cross Site Scripting payload which does not match the regular expression; one example of this is the inclusion of whitespace within the script tag. An attacker must target an authenticated user with permissions to access this feature, however once uploaded the payload is also accessible to unauthenticated users.	2024-03-26	5.4	CVE-2024-29833
accessally -- popupally	Missing Authorization vulnerability in AccessAlly PopupAlly.This issue affects PopupAlly: from n/a through 2.1.0.	2024-03-26	4.3	CVE-2024-23520
algoritim -- e-commerce_software	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Algoritim E-commerce Software allows Reflected XSS.This issue affects E-commerce Software: before 3.9.2.	2024-03-29	6.1	CVE-2023-6047
alireza_sedghi -- aparat_for_wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alireza Sedghi Aparat for WordPress allows Stored XSS.This issue affects Aparat for WordPress: from n/a through 2.2.0.	2024-03-27	6.5	CVE-2024-29765
all_in_one_wp_security_&_firewall_team -- all_in_one_wp_security_&_firewall	Cross-Site Request Forgery (CSRF) vulnerability in All In One WP Security & Firewall Team All In One WP Security & Firewall.This issue affects All In One WP Security & Firewall: from n/a through 5.2.6.	2024-03-29	4.3	CVE-2024-30468
alordiel -- dropdown_multisite_selector	A vulnerability has been found in Tenda FH1203 2.0.1.6 and classified as critical. This vulnerability affects the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258160. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	6.3	CVE-2024-2991

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alordiel -- dropdown_multisite_selector	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alordiel Dropdown Multisite selector allows Stored XSS.This issue affects Dropdown Multisite selector: from n/a through 0.9.2.	2024-03-27	6.5	CVE-2024-29910
aminur_islam -- wp_change_email_sender	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aminur Islam WP Change Email Sender allows Stored XSS.This issue affects WP Change Email Sender: from n/a before 1.3.0.	2024-03-27	5.9	CVE-2024-29815
ampache -- ampache	Ampache is a web based audio/video streaming application and file manager. Ampache has multiple reflective XSS vulnerabilities,this means that all forms in the Ampache that use `rule` as a variable are not secure. For example, when querying a song, when querying a podcast, we need to use `$rule` variable. This vulnerability is fixed in 6.3.1	2024-03-27	6.1	CVE-2024-28852
andy_moyle -- church_admin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Andy Moyle Church Admin allows Stored XSS.This issue affects Church Admin: from n/a through 4.1.17.	2024-03-27	6.5	CVE-2024-30193
andy_moyle -- church_admin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Andy Moyle Church Admin allows Stored XSS.This issue affects Church Admin: from n/a through 4.0.26.	2024-03-27	6.5	CVE-2024-30197
andy_moyle -- church_admin	Missing Authorization vulnerability in Andy Moyle Church Admin.This issue affects Church Admin: from n/a through 4.1.18.	2024-03-29	5.4	CVE-2024-30505
andy_moyle -- church_admin	Cross-Site Request Forgery (CSRF) vulnerability in Andy Moyle Church Admin.This issue affects Church Admin: from n/a through 4.1.7.	2024-03-29	4.3	CVE-2024-30493
antoine_hurkmans -- football_pool	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Antoine Hurkmans Football Pool allows Stored XSS.This issue affects Football Pool: from n/a through 2.11.3.	2024-03-27	6.5	CVE-2024-29802
appneta -- tcpreplay	A vulnerability was found in appneta tcpreplay up to 4.4.4. It has been classified as problematic. This affects the function get_layer4_v6 of the file /tcpreplay/src/common/get.c. The manipulation leads to heap-based buffer overflow. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-258333 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-28	5.3	CVE-2024-3024
appsmav -- gratisfaction	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Appsmav Gratisfaction allows Stored XSS.This issue affects Gratisfaction: from n/a through 4.3.4.	2024-03-27	6.5	CVE-2024-29798
argoproj -- argo-cd	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. All versions of ArgoCD starting from v2.4 have a bug where the ArgoCD repo-server component is vulnerable to a Denial-of-Service attack vector. Specifically, it's possible to crash the repo server component through an out of memory error by pointing it to a malicious Helm registry. The loadRepoIndex() function in the ArgoCD's helm package, does not limit the size nor time while fetching the data. It fetches it and creates a byte slice from the retrieved data in one go. If the registry is implemented to push data continuously, the repo server will keep allocating	2024-03-29	6.5	CVE-2024-29893

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	memory until it runs out of it. A patch for this vulnerability has been released in v2.10.3, v2.9.8, and v2.8.12.			
athemes -- sydney_toolbox	The Sydney Toolbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the _id attribute of widgets in all versions up to, and including, 1.26 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.	2024-03-29	6.4	CVE-2024-2936
automationdirect -- c-more_ea9_hmi_ea9-t6cl	In AutomationDirect C-MORE EA9 HMI, credentials used by the platform are stored as plain text on the device.	2024-03-26	6.5	CVE-2024-25138
automationdirect -- c-more_ea9_hmi_ea9-t6cl	In AutomationDirect C-MORE EA9 HMI there is a program that copies a buffer of a size controlled by the user into a limited sized buffer on the stack which may lead to a stack overflow. The result of this stack-based buffer overflow can lead to denial-of-service conditions.	2024-03-26	4.3	CVE-2024-25137
azure -- azure-c-shared-utility	The azure-c-shared-utility is a C library for AMQP/MQTT communication to Azure Cloud Services. This library may be used by the Azure IoT C SDK for communication between IoT Hub and IoT Hub devices. An attacker can cause an integer wraparound or under-allocation or heap buffer overflow due to vulnerabilities in parameter checking mechanism, by exploiting the buffer length parameter in Azure C SDK, which may lead to remote code execution. Requirements for RCE are 1. Compromised Azure account allowing malformed payloads to be sent to the device via IoT Hub service, 2. By passing IoT hub service max message payload limit of 128KB, and 3. Ability to overwrite code space with remote code. Fixed in commit https://github.com/Azure/azure-c-shared-utility/commit/1129147c38ac02ad974c4c701a1e01b2141b9fe2.	2024-03-26	6	CVE-2024-29195
backie -- wp-eggdrop	The WP-Eggdrop plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.1. This is due to missing or incorrect nonce validation on the wpegg_updateOptions() function. This makes it possible for unauthenticated attackers to update the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-29	5.4	CVE-2024-2969
backie -- wp-eggdrop	The WP-Eggdrop plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-03-29	4.4	CVE-2024-2968
baptiste_placÃƒÆ'Ã‚Â© -- icalendrier	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Baptiste PlacÃƒÂ© iCalendrier allows Stored XSS.This issue affects iCalendrier: from n/a through 1.80.	2024-03-27	6.5	CVE-2024-29912
bdthemes -- element_pack_elementor_addons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BdThemes Element Pack Elementor Addons allows Stored XSS.This issue affects Element Pack Elementor Addons: from n/a through 5.5.3.	2024-03-27	6.5	CVE-2024-30185
bdthemes -- prime_slider_-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BdThemes Prime Slider - Addons For Elementor allows	2024-03-27	6.5	CVE-2024-30186

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_addons_for_elementor	Stored XSS.This issue affects Prime Slider - Addons For Elementor: from n/a through 3.13.1.			
betteraddons -- better_elementor_addons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BetterAddons Better Elementor Addons allows Stored XSS.This issue affects Better Elementor Addons: from n/a through 1.3.7.	2024-03-29	6.5	CVE-2024-30423
blocksera -- image_hover_effects_-_elementor_addon	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Blocksera Image Hover Effects - Elementor Addon allows Stored XSS.This issue affects Image Hover Effects - Elementor Addon: from n/a through 1.4.	2024-03-27	6.5	CVE-2024-29936
boldgrid -- boldgrid_easy_seo_-_simple_and_effective_seo	The BoldGrid Easy SEO - Simple and Effective SEO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the meta description field in all versions up to, and including, 1.6.13 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.	2024-03-30	6.4	CVE-2024-1692
boldgrid -- post_and_page_builder_by_boldgrid_-_visual_drag_and_drop_editor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BoldGrid Post and Page Builder by BoldGrid - Visual Drag and Drop Editor allows Stored XSS.This issue affects Post and Page Builder by BoldGrid - Visual Drag and Drop Editor: from n/a through 1.26.2.	2024-03-26	6.5	CVE-2024-2888
boldthemes -- bold_page_builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BoldThemes Bold Page Builder allows Stored XSS.This issue affects Bold Page Builder: from n/a through 4.7.6.	2024-03-27	6.5	CVE-2024-30179
boldthemes -- bold_page_builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BoldThemes Bold Page Builder allows Stored XSS.This issue affects Bold Page Builder: from n/a through 4.8.0.	2024-03-29	6.5	CVE-2024-30442
booster -- booster_plus_for_woocommerce	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Booster Booster Plus for WooCommerce.This issue affects Booster Plus for WooCommerce: from n/a before 7.1.2.	2024-03-28	6.5	CVE-2023-52231
booster -- booster_plus_for_woocommerce	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Booster Booster Elite for WooCommerce.This issue affects Booster Elite for WooCommerce: from n/a before 7.1.2.	2024-03-28	6.5	CVE-2023-52234
bplugins -- b_slider_-_slider_for_your_block_editor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins B Slider - Slider for your block editor allows Stored XSS.This issue affects B Slider - Slider for your block editor: from n/a through 1.1.12.	2024-03-29	6.5	CVE-2024-30432

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bplugins -- print_page_block	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Print Page block allows Stored XSS.This issue affects Print Page block: from n/a through 1.0.8.	2024-03-29	6.5	CVE-2024-30438
brainstorm_force -- astra	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force Astra allows Stored XSS.This issue affects Astra: from n/a through 4.6.4.	2024-03-27	5.9	CVE-2024-29768
brainstormforce -- ultimate_addons_for_beaver_builder_-_lite	The Ultimate Addons for Beaver Builder - Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Button widget in all versions up to, and including, 1.5.7 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.	2024-03-30	6.4	CVE-2024-2141
brainstormforce -- ultimate_addons_for_beaver_builder_-_lite	The Ultimate Addons for Beaver Builder - Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Info Table widget in all versions up to, and including, 1.5.7 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.	2024-03-30	6.4	CVE-2024-2142
brainstormforce -- ultimate_addons_for_beaver_builder_-_lite	The Ultimate Addons for Beaver Builder - Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Heading widget in all versions up to, and including, 1.5.7 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.	2024-03-30	6.4	CVE-2024-2143
brainstormforce -- ultimate_addons_for_beaver_builder_-_lite	The Ultimate Addons for Beaver Builder - Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Image Separator widget in all versions up to, and including, 1.5.7 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.	2024-03-30	6.4	CVE-2024-2144
brainstormforce -- ultimate_addons_for_beaver_builder_-_lite	The Ultimate Addons for Beaver Builder - Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Advanced Icons widget in all versions up to, and including, 1.5.7 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.	2024-03-30	6.4	CVE-2024-2140
brave -- brave_popup_builder	Server-Side Request Forgery (SSRF) vulnerability in Brave Brave Popup Builder.This issue affects Brave Popup Builder: from n/a through 0.6.5.	2024-03-29	5.4	CVE-2024-30453
brice_capobianco -- simple_revisions_delete	Cross-Site Request Forgery (CSRF) vulnerability in Brice CAPOBIANCO Simple Revisions Delete.This issue affects Simple Revisions Delete: from n/a through 1.5.3.	2024-03-29	4.3	CVE-2024-30482
camille_verrier -- travelers'_map	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Camille Verrier Travelers' Map allows Stored XSS.This issue affects Travelers' Map: from n/a through 2.2.0.	2024-03-27	6.5	CVE-2024-29909
campcodes -- house_rental_man	A vulnerability was found in Campcodes House Rental Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown	2024-03-26	5.4	CVE-2024-2917

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
agement_system	functionality of the file index.php. The manipulation of the argument page leads to file inclusion. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257983.			
campcodes -- online_art_gallery_management_system	A vulnerability classified as critical has been found in Campcodes Online Art Gallery Management System 1.0. This affects an unknown part of the file /admin/adminHome.php. The manipulation of the argument uname leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258201 was assigned to this vulnerability.	2024-03-27	6.3	CVE-2024-2999
campcodes -- online_examination_system	A vulnerability was found in Campcodes Online Examination System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /adminpanel/admin/facebox_modal/updateCourse.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258029 was assigned to this vulnerability.	2024-03-27	6.3	CVE-2024-2938
campcodes -- online_examination_system	A vulnerability, which was classified as critical, has been found in Campcodes Online Examination System 1.0. Affected by this issue is some unknown functionality of the file /adminpanel/admin/query/loginExe.php. The manipulation of the argument pass leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258032.	2024-03-27	6.3	CVE-2024-2941
campcodes -- online_examination_system	A vulnerability, which was classified as critical, was found in Campcodes Online Examination System 1.0. This affects an unknown part of the file /adminpanel/admin/query/deleteQuestionExe.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258033 was assigned to this vulnerability.	2024-03-27	6.3	CVE-2024-2942
campcodes -- online_examination_system	A vulnerability has been found in Campcodes Online Examination System 1.0 and classified as critical. This vulnerability affects unknown code of the file /adminpanel/admin/query/deleteExamExe.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. VDB-258034 is the identifier assigned to this vulnerability.	2024-03-27	6.3	CVE-2024-2943
campcodes -- online_examination_system	A vulnerability was found in Campcodes Online Examination System 1.0 and classified as critical. This issue affects some unknown processing of the file /adminpanel/admin/query/deleteCourseExe.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258035.	2024-03-27	6.3	CVE-2024-2944
campcodes -- online_examination_system	A vulnerability was found in Campcodes Online Examination System 1.0. It has been classified as critical. Affected is an unknown function of the file /adminpanel/admin/facebox_modal/updateExaminee.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258036.	2024-03-27	6.3	CVE-2024-2945
carrierwaveuploader -- carrierwave	CarrierWave is a solution for file uploads for Rails, Sinatra and other Ruby web frameworks. The vulnerability CVE-2023-49090 wasn't fully addressed. This vulnerability is caused by the fact that when uploading to object storage, including Amazon S3, it is possible to set a Content-Type value that is interpreted by browsers to be different from what's allowed by `content_type_allowlist`, by providing multiple values separated by commas. This bypassed value can be used to cause XSS. Upgrade to 3.0.7 or 2.2.6.	2024-03-24	6.8	CVE-2024-29034

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cartflows_inc. -- funnel_builder_by_cartflows	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CartFlows Inc. Funnel Builder by CartFlows allows Stored XSS.This issue affects Funnel Builder by CartFlows: from n/a through 2.0.1.	2024-03-27	5.9	CVE-2024-29813
cincopa -- post_video_players	Cross-Site Request Forgery (CSRF) vulnerability in Cincopa Post Video Players.This issue affects Post Video Players: from n/a through 1.159.	2024-03-27	5.4	CVE-2024-23515
cisco -- cisco_aironet_access_point_software	A vulnerability in the handling of encrypted wireless frames of Cisco Aironet Access Point (AP) Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on the affected device. This vulnerability is due to incomplete cleanup of resources when dropping certain malformed frames. An attacker could exploit this vulnerability by connecting as a wireless client to an affected AP and sending specific malformed frames over the wireless connection. A successful exploit could allow the attacker to cause degradation of service to other clients, which could potentially lead to a complete DoS condition.	2024-03-27	4.7	CVE-2024-20354
cisco -- cisco_digital_network_architecture_center_(dna_center)	A vulnerability in the web-based management interface of Cisco Catalyst Center, formerly Cisco DNA Center, could allow an authenticated, remote attacker to change specific data within the interface on an affected device. This vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to change a specific field within the web-based management interface, even though they should not have access to change that field.	2024-03-27	4.3	CVE-2024-20333
cisco -- cisco_ios_xe_software	A vulnerability in the NETCONF feature of Cisco IOS XE Software could allow an authenticated, remote attacker to elevate privileges to root on an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input over NETCONF to an affected device. A successful exploit could allow the attacker to elevate privileges from Administrator to root.	2024-03-27	6.5	CVE-2024-20278
cisco -- cisco_ios_xe_software	A vulnerability in the Unified Threat Defense (UTD) configuration CLI of Cisco IOS XE Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying host operating system. To exploit this vulnerability, an attacker must have level 15 privileges on the affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by submitting a crafted CLI command to an affected device. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying operating system.	2024-03-27	6	CVE-2024-20306
cisco -- cisco_ios_xe_software	A vulnerability in the boot process of Cisco Access Point (AP) Software could allow an unauthenticated, physical attacker to bypass the Cisco Secure Boot functionality and load a software image that has been tampered with on an affected device. This vulnerability exists because unnecessary commands are available during boot time at the physical console. An attacker could exploit this vulnerability by interrupting the boot process and executing specific commands to bypass the Cisco Secure Boot validation checks and load an image that has been tampered with. This image would have been previously downloaded onto the targeted device. A successful exploit could allow the attacker to load the image once. The Cisco Secure Boot functionality is not permanently compromised.	2024-03-27	5.9	CVE-2024-20265
cisco -- cisco_ios_xe_software	A vulnerability in auxiliary asynchronous port (AUX) functions of Cisco IOS XE Software could allow an authenticated, local attacker to cause an affected device to reload or stop responding. This vulnerability is due to the incorrect handling of specific ingress traffic when flow control hardware is enabled on the AUX port. An attacker could exploit this vulnerability by reverse telnetting to the AUX port and sending specific data after connecting. A successful exploit could allow the attacker	2024-03-27	5.6	CVE-2024-20309

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to cause the device to reset or stop responding, resulting in a denial of service (DoS) condition.			
cisco -- cisco_ios_xe_software	A vulnerability in the data model interface (DMI) services of Cisco IOS XE Software could allow an unauthenticated, remote attacker to access resources that should have been protected by a configured IPv4 access control list (ACL). This vulnerability is due to improper handling of error conditions when a successfully authorized device administrator updates an IPv4 ACL using the NETCONF or RESTCONF protocol, and the update would reorder access control entries (ACEs) in the updated ACL. An attacker could exploit this vulnerability by accessing resources that should have been protected across an affected device.	2024-03-27	5.8	CVE-2024-20316
cisco -- cisco_ios_xe_software	A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, low-privileged, local attacker to access WLAN configuration details including passwords. This vulnerability is due to improper privilege checks. An attacker could exploit this vulnerability by using the show and show tech wireless CLI commands to access configuration details, including passwords. A successful exploit could allow the attacker to access configuration details that they are not authorized to access.	2024-03-27	5.5	CVE-2024-20324
cisco -- ios	A vulnerability in the IKEv1 fragmentation code of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a heap overflow, resulting in an affected device reloading. This vulnerability exists because crafted, fragmented IKEv1 packets are not properly reassembled. An attacker could exploit this vulnerability by sending crafted UDP packets to an affected system. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: Only traffic that is directed to the affected system can be used to exploit this vulnerability. This vulnerability can be triggered by IPv4 and IPv6 traffic.	2024-03-27	6.8	CVE-2024-20307
cloudways -- breeze	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cloudways Breeze allows Stored XSS.This issue affects Breeze: from n/a through 2.1.3.	2024-03-27	5.9	CVE-2024-27188
code-projects -- online_book_system	A vulnerability, which was classified as critical, has been found in code-projects Online Book System 1.0. This issue affects some unknown processing of the file /Product.php. The manipulation of the argument value leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258203.	2024-03-27	6.3	CVE-2024-3001
code-projects -- online_book_system	A vulnerability, which was classified as critical, was found in code-projects Online Book System 1.0. Affected is an unknown function of the file /description.php. The manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258204.	2024-03-27	6.3	CVE-2024-3002
code-projects -- online_book_system	A vulnerability has been found in code-projects Online Book System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /cart.php. The manipulation of the argument quantity/remove leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258205 was assigned to this vulnerability.	2024-03-27	6.3	CVE-2024-3003
codepeople -- google_maps_cp	Missing Authorization vulnerability in CodePeople Google Maps CP.This issue affects Google Maps CP: from n/a through 1.0.43.	2024-03-25	4.3	CVE-2023-25039
codesupplyco -- networker_-_tech_news_wordpress_theme_with	The Networker - Tech News WordPress Theme with Dark Mode theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the admin_reload_nav_menu() function in all versions up to,	2024-03-27	5.3	CVE-2024-2962

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_dark_mode	and including, 1.1.9. This makes it possible for unauthenticated attackers to modify the location of display menus.			
codexthemes -- thegem_(elementor)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem (Elementor), CodexThemes TheGem (WPBakery) allows Stored XSS.This issue affects TheGem (Elementor): from n/a before 5.8.1.1; TheGem (WPBakery): from n/a before 5.8.1.1.	2024-03-26	6.5	CVE-2023-32237
collect.chat_inc. -- collectchat	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Collect.Chat Inc. Collectchat allows Stored XSS.This issue affects Collectchat: from n/a through 2.4.1.	2024-03-29	6.5	CVE-2024-30436
crm_perks -- crm_perks_forms	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CRM Perks CRM Perks Forms allows Stored XSS.This issue affects CRM Perks Forms: from n/a through 1.1.4.	2024-03-29	6.5	CVE-2024-30446
currencyrate.today -- crypto_converter_widget	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CurrencyRate.Today Crypto Converter Widget allows Stored XSS.This issue affects Crypto Converter Widget: from n/a through 1.8.4.	2024-03-27	6.5	CVE-2024-29930
currencyrate.today -- exchange_rates_widget	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CurrencyRate.Today Exchange Rates Widget allows Stored XSS.This issue affects Exchange Rates Widget: from n/a through 1.4.0.	2024-03-27	6.5	CVE-2024-29814
cyberaz0r -- webrat	A vulnerability has been found in cyberaz0r WebRAT up to 20191222 and classified as critical. This vulnerability affects the function download_file of the file Server/api.php. The manipulation of the argument name leads to unrestricted upload. The attack can be initiated remotely. The patch is identified as 0c394a795b9c10c07085361e6fcea286ee793701. It is recommended to apply a patch to fix this issue. VDB-257782 is the identifier assigned to this vulnerability.	2024-03-24	6.3	CVE-2020-36825
dearhive -- dearflip	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DearHive DearFlip allows Stored XSS.This issue affects DearFlip: from n/a through 2.2.26.	2024-03-27	6.5	CVE-2024-29807
deepak_anand -- wp_dummy_content_generator	Missing Authorization vulnerability in Deepak anand WP Dummy Content Generator.This issue affects WP Dummy Content Generator: from n/a through 3.1.2.	2024-03-26	4.3	CVE-2024-24805
dell -- dell_openmanage_enterprise	Dell OpenManage Enterprise, v4.0 and prior, contain(s) a path traversal vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, to gain unauthorized access to the files stored on the server filesystem, with the privileges of the running web application.	2024-03-29	5.7	CVE-2024-25944
dell -- grab_for_windows	Dell Grab for Windows, versions up to and including 5.0.4, contain Weak Application Folder Permissions vulnerability. A local authenticated attacker could potentially exploit this vulnerability, leading to privilege escalation, unauthorized access to application data, unauthorized modification of application data and service disruption.	2024-03-26	6.7	CVE-2024-25958
dell -- grab_for_windows	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in mbbhatti Upload Resume.This issue affects Upload Resume: from n/a through 1.2.0.	2024-03-26	5.9	CVE-2023-25965

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- grab_for_windows	Dell Grab for Windows, versions 5.0.4 and below, contains an improper file permissions vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to the information disclosure of certain system information.	2024-03-26	5.5	CVE-2024-25956
dell -- grab_for_windows	Dell Grab for Windows, versions 5.0.4 and below, contains a cleartext storage of sensitive information vulnerability in its appsync module. An authenticated local attacker could potentially exploit this vulnerability, leading to information disclosure that could be used to access the appsync application with elevated privileges.	2024-03-26	4.8	CVE-2024-25957
dell -- powerprotect_data_manager	Dell PowerProtect Data Manager, version 19.15, contains an XML External Entity Injection vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to information disclosure, denial-of-service.	2024-03-28	5.5	CVE-2024-25971
dell -- powerscale_onefs	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.x contains an UNIX symbolic link (symlink) following vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to denial of service, information tampering.	2024-03-28	6	CVE-2024-25952
dell -- powerscale_onefs	Dell PowerScale OneFS versions 9.4.0.x through 9.7.0.x contains an UNIX symbolic link (symlink) following vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to denial of service, information tampering.	2024-03-28	6	CVE-2024-25953
dell -- powerscale_onefs	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.x contains an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to escalation of privileges.	2024-03-28	6	CVE-2024-25961
dell -- powerscale_onefs	Dell PowerScale OneFS, versions 9.5.0.x through 9.7.0.x, contain an insufficient session expiration vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service.	2024-03-28	5.3	CVE-2024-25954
dell -- powerscale_onefs	Dell PowerScale OneFS, versions 8.2.2.x through 9.5.0.x contains a use of a broken cryptographic algorithm vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to information disclosure.	2024-03-28	5.9	CVE-2024-25963
dell -- powerscale_onefs	Dell PowerScale OneFS 9.5.0.x through 9.7.0.x contain a covert timing channel vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service.	2024-03-25	5.3	CVE-2024-25964
dglingren -- media_library_assistant	The Media Library Assistant plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes in all versions up to, and including, 3.13 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.	2024-03-29	6.4	CVE-2024-2475
easy_social_feed -- easy_social_feed	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Easy Social Feed allows Stored XSS.This issue affects Easy Social Feed: from n/a through 6.5.3.	2024-03-27	6.5	CVE-2024-30180
elastic -- elasticsearch	An uncaught exception in Elasticsearch >= 8.4.0 and < 8.11.1 occurs when an encrypted PDF is passed to an attachment processor through the REST API. The Elasticsearch ingest node that attempts to parse the PDF file will crash. This does not happen with password-protected PDF files or with unencrypted PDF files.	2024-03-29	4.3	CVE-2024-23449 bressers@elastic.co
elastic -- elasticsearch	A flaw was discovered in Elasticsearch, where processing a document in a deeply nested pipeline on an ingest node could cause the Elasticsearch node to crash.	2024-03-27	4.9	CVE-2024-23450 bressers@elastic.co

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				bressers@elastic.co
elastic -- elasticsearch	Incorrect Authorization issue exists in the API key based security model for Remote Cluster Security, which is currently in Beta, in Elasticsearch 8.10.0 and before 8.13.0. This allows a malicious user with a valid API key for a remote cluster configured to use the new Remote Cluster Security to read arbitrary documents from any index on the remote cluster, and only if they use the Elasticsearch custom transport protocol to issue requests with the target index ID, the shard ID and the document ID. None of Elasticsearch REST API endpoints are affected by this issue.	2024-03-27	4.4	CVE-2024-23451 bressers@elastic.co
envialosimple -- envÃƒÆ'Ã‚Â-alosimple	Cross-Site Request Forgery (CSRF) vulnerability in EnvialoSimple EnvÃƒÂ-aloSimple.This issue affects EnvÃƒÂaloSimple: from n/a through 2.3.	2024-03-26	6.5	CVE-2023-51416
epsiloncool -- wp_fast_total_search	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Epsiloncool WP Fast Total Search allows Stored XSS.This issue affects WP Fast Total Search: from n/a through 1.59.211.	2024-03-27	6.5	CVE-2024-29799
espressif -- esp-idf	ESP-IDF is the development framework for Espressif SoCs supported on Windows, Linux and macOS. A Time-of-Check to Time-of-Use (TOCTOU) vulnerability was discovered in the implementation of the ESP-IDF bootloader which could allow an attacker with physical access to flash of the device to bypass anti-rollback protection. Anti-rollback prevents rollback to application with security version lower than one programmed in eFuse of chip. This attack can allow to boot past (passive) application partition having lower security version of the same device even in the presence of the flash encryption scheme. The attack requires carefully modifying the flash contents after the anti-rollback checks have been performed by the bootloader (before loading the application). The vulnerability is fixed in 4.4.7 and 5.2.1.	2024-03-25	6.1	CVE-2024-28183
exclusive_addons -- exclusive_addons_elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Exclusive Addons Exclusive Addons Elementor allows Stored XSS.This issue affects Exclusive Addons Elementor: from n/a through 2.6.8.	2024-03-27	6.5	CVE-2024-30177
exclusive_addons -- exclusive_addons_elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Exclusive Addons Exclusive Addons Elementor allows Stored XSS.This issue affects Exclusive Addons Elementor: from n/a through 2.6.9.	2024-03-26	6.5	CVE-2024-30232
expressjs -- express	Express.js minimalist web framework for node. Versions of Express.js prior to 4.19.0 and all pre-release alpha and beta versions of 5.0 are affected by an open redirect vulnerability using malformed URLs. When a user of Express performs a redirect using a user-provided URL Express performs an encode [using `encodeurl`](https://github.com/pillarjs/encodeurl) on the contents before passing it to the `location` header. This can cause malformed URLs to be evaluated in unexpected ways by common redirect allow list implementations in Express applications, leading to an Open Redirect via bypass of a properly implemented allow list. The main method impacted is `res.location()` but this is also called from within `res.redirect()`. The vulnerability is fixed in 4.19.2 and 5.0.0-beta.3.	2024-03-25	6.1	CVE-2024-29041
extend_themes -- calliope	Cross-Site Request Forgery (CSRF) vulnerability in Extend Themes Calliope.This issue affects Calliope: from n/a through 1.0.33.	2024-03-26	4.3	CVE-2024-2904

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
extendthemes -- colibri_page_builder	Missing Authorization vulnerability in ExtendThemes Colibri Page Builder.This issue affects Colibri Page Builder: from n/a through 1.0.248.	2024-03-28	5.4	CVE-2024-28004
fernandobt -- list_category_posts	The List category posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'catlist' shortcode in all versions up to, and including, 0.89.6 due to insufficient input sanitization and output escaping on user supplied attributes like 'title_tag'. 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.	2024-03-30	6.4	CVE-2024-1051
flector -- easy_textillate	The Easy Textillate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'textillate' shortcode in all versions up to, and including, 2.01 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.	2024-03-26	6.4	CVE-2024-2303
flir -- ax8	A vulnerability was found in FLIR AX8 up to 1.46.16. It has been rated as critical. This issue affects some unknown processing of the file /tools/test_login.php?action=register of the component User Registration. The manipulation leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258299. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-28	6.3	CVE-2024-3013
fr-d-ric_gilles -- fg_prestashop_to_woocommerce	Insertion of Sensitive Information into Log File vulnerability in FrÃƒÂ©dÃƒÂ©ric GILLES FG PrestaShop to WooCommerce.This issue affects FG PrestaShop to WooCommerce: from n/a through 4.45.1.	2024-03-29	5.3	CVE-2024-30511
gamipress -- gamipress	Cross-Site Request Forgery (CSRF) vulnerability in GamiPress.This issue affects GamiPress: from n/a through 6.8.5.	2024-03-29	4.3	CVE-2024-30455
geonode -- geonode	GeoNode is a geospatial content management system, a platform for the management and publication of geospatial data. An issue exists within GEONODE where the current rich text editor is vulnerable to Stored XSS. The applications cookies are set securely, but it is possible to retrieve a victims CSRF token and issue a request to change another user's email address to perform a full account takeover. Due to the script element not impacting the CORS policy, requests will succeed. This vulnerability is fixed in 4.2.3.	2024-03-27	6.1	CVE-2024-27091
ghozylab_inc. -- web_icons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GhozyLab, Inc. Web Icons allows Stored XSS.This issue affects Web Icons: from n/a through 1.0.0.10.	2024-03-27	6.5	CVE-2024-29933
ghozylab_inc. -- web_icons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GhozyLab, Inc. Web Icons allows Stored XSS.This issue affects Web Icons: from n/a through 1.0.0.10.	2024-03-29	6.5	CVE-2024-30445
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions before 16.8.5, all versions starting from 16.9 before 16.9.3, all versions starting from 16.10 before 16.10.1. It was possible for an attacker to cause a denial of service using malicious crafted description parameter for labels.	2024-03-28	4.3	CVE-2024-2818
grafana -- grafana	It is possible for a user in a different organization from the owner of a snapshot to bypass authorization and delete a snapshot by issuing a DELETE request to /api/snapshots/<key> using its view key. This functionality is intended to only be	2024-03-26	6.5	CVE-2024-1313

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	available to individuals with the permission to write/edit to the snapshot in question, but due to a bug in the authorization logic, deletion requests issued by an unprivileged user in a different organization than the snapshot owner are treated as authorized. Grafana Labs would like to thank Ravid Mazon and Jay Chen of Palo Alto Research for discovering and disclosing this vulnerability. This issue affects Grafana: from 9.5.0 before 9.5.18, from 10.0.0 before 10.0.13, from 10.1.0 before 10.1.9, from 10.2.0 before 10.2.6, from 10.3.0 before 10.3.5.			
gs_plugins -- gs_testimonial_slider	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GS Plugins GS Testimonial Slider allows Stored XSS.This issue affects GS Testimonial Slider: from n/a through 3.1.4.	2024-03-29	6.5	CVE-2024-30443
hans_matzen -- wp-forecast	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hans Matzen allows Stored XSS.This issue affects wp-forecast: from n/a through 9.2.	2024-03-29	6.5	CVE-2024-30429
hashthemes -- hash_elements	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HashThemes Hash Elements allows Stored XSS.This issue affects Hash Elements: from n/a through 1.3.3.	2024-03-29	6.5	CVE-2024-30426
hashthemes -- viral_news	Missing Authorization vulnerability in HashThemes Viral News, HashThemes Viral, HashThemes HashOne.This issue affects Viral News: from n/a through 1.4.5; Viral: from n/a through 1.8.0; HashOne: from n/a through 1.3.0.	2024-03-25	4.3	CVE-2023-33923
hastheme -- wishsuite	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasTheme WishSuite allows Stored XSS.This issue affects WishSuite: from n/a through 1.3.7.	2024-03-27	6.5	CVE-2024-29927
hasthemes -- ht_mega	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasThemes HT Mega allows Stored XSS.This issue affects HT Mega: from n/a through 2.4.3.	2024-03-27	6.5	CVE-2024-30182
hasthemes -- wc_builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasThemes WC Builder allows Stored XSS.This issue affects WC Builder: from n/a through 1.0.18.	2024-03-27	6.5	CVE-2024-29926
hewlett_packard_enterprise_(hpe) -- arubaos-s_switch	Authenticated Denial of Service Vulnerability in ArubaOS-Switch SSH Daemon	2024-03-26	4.9	CVE-2024-26303
hewlett_packard_enterprise_(hpe) -- icewall_gen11_icewall_sso_agent	A security vulnerability in HPE IceWall Agent products could be exploited remotely to cause a denial of service.	2024-03-26	6.5	CVE-2024-22436
hitachi_energy -- asset_suite_eam	REST service authentication anomaly with "valid username/no password" credential combination for batch job processing resulting in successful service invocation. The anomaly doesn't exist with other credential combinations.	2024-03-27	5.3	CVE-2024-2244
hitachi_energy -- rtu500_series_cmu_firmware	A vulnerability exists in the stb-language file handling that affects the RTU500 series product versions listed below. A malicious actor could enforce diagnostic texts being displayed as empty strings, if an authorized user uploads a specially crafted stb-language file.	2024-03-27	6.8	CVE-2024-1532

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hot_themes -- hot_random_image	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hot Themes Hot Random Image allows Stored XSS.This issue affects Hot Random Image: from n/a through 1.8.1.	2024-03-27	6.5	CVE-2024-29796
htdat -- woo_viet	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in htdat Woo Viet allows Stored XSS.This issue affects Woo Viet: from n/a through 1.5.2.	2024-03-27	5.9	CVE-2024-29816
https://elementor.com/ -- elementor_website_builder_pro	The Elementor Website Builder Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via widget's custom_id in all versions up to, and including, 3.20.1 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.	2024-03-27	6.4	CVE-2024-1364
https://elementor.com/ -- elementor_website_builder_pro	The Elementor Website Builder Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an SVGZ file uploaded via the Form widget in all versions up to, and including, 3.20.1 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. NOTE: This vulnerability is only exploitable on web servers running NGINX. It is not exploitable on web servers running Apache HTTP Server.	2024-03-27	6.4	CVE-2024-1521
https://elementor.com/ -- elementor_website_builder_pro	The Elementor Website Builder Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the video_html_tag attribute in all versions up to, and including, 3.20.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-27	6.4	CVE-2024-2781
https://elementor.com/ -- elementor_website_builder_pro	The Elementor Website Builder - More than Just a Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Post Navigation widget in all versions up to, and including, 3.20.1 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.	2024-03-27	5.4	CVE-2024-2120
https://elementor.com/ -- elementor_website_builder_pro	The Elementor Website Builder Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Media Carousel widget in all versions up to, and including, 3.20.1 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.	2024-03-27	5.4	CVE-2024-2121
ibm -- app_connect_enterprise	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.23, 12.0.1.0 through 12.0.9.0 and IBM Integration Bus for z/OS 10.1 through 10.1.0.2store potentially sensitive information in log or trace files that could be read by a privileged user. IBM X-Force ID: 280893.	2024-03-26	4.9	CVE-2024-22356
ibm -- qradar_siem	IBM QRadar SIEM 7.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 285893.	2024-03-27	5.4	CVE-2024-28784
ibm -- qradar_siem	IBM QRadar SIEM 7.5 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the	2024-03-27	4.8	CVE-2023-50961

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 275939.			
ibm -- websphere_application_server_liberty	IBM WebSphere Application Server Liberty 23.0.0.3 through 24.0.0.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in a specially crafted URI. IBM X-Force ID: 284576.	2024-03-27	4.7	CVE-2024-27270
ideaboxcreations -- powerpack_addons_for_elementor_(free_widgets_extensions_and_templates)	The PowerPack Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the *_html_tag* attribute of multiple widgets in all versions up to, and including, 2.7.17 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.	2024-03-30	6.4	CVE-2024-2491
infinitum_form -- geo_controller	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in INFINITUM FORM Geo Controller allows Stored XSS.This issue affects Geo Controller: from n/a through 8.6.4.	2024-03-29	6.5	CVE-2024-30451
inspirythemes -- realhomes	Missing Authorization vulnerability in InspiryThemes RealHomes.This issue affects RealHomes: from n/a through 4.0.2.	2024-03-25	5.4	CVE-2023-37886
inspirythemes -- realhomes	Missing Authorization vulnerability in InspiryThemes RealHomes.This issue affects RealHomes: from n/a through 4.0.2.	2024-03-25	4.3	CVE-2023-37885
interfacelab -- media_cloud_for_amazon_s3_imgix_google_cloud_storage_digitalocean_spaces_and_more	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Interfacelab Media Cloud for Amazon S3, Imgix, Google Cloud Storage, DigitalOcean Spaces and more allows Stored XSS.This issue affects Media Cloud for Amazon S3, Imgix, Google Cloud Storage, DigitalOcean Spaces and more: from n/a through 4.5.24.	2024-03-27	6.5	CVE-2024-29795
jeff_starr -- user_submitted_posts	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeff Starr User Submitted Posts allows Stored XSS.This issue affects User Submitted Posts: from n/a through 20230901.	2024-03-26	6.5	CVE-2023-7251
jetbrains -- teamcity	In JetBrains TeamCity before 2024.03 authenticated users without administrative permissions could register other users when self-registration was disabled	2024-03-28	6.5	CVE-2024-31134
jetbrains -- teamcity	In JetBrains TeamCity before 2024.03 open redirect was possible on the login page	2024-03-28	6.1	CVE-2024-31135
jetbrains -- teamcity	In JetBrains TeamCity before 2024.03 reflected XSS was possible via Space connection configuration	2024-03-28	6.8	CVE-2024-31137
jetbrains -- teamcity	In JetBrains TeamCity before 2024.03 xXE was possible in the Maven build steps detector	2024-03-28	5.9	CVE-2024-31139

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jetbrains -- teamcity	In JetBrains TeamCity before 2024.03 xSS was possible via Agent Distribution settings	2024-03-28	4.6	CVE-2024-31138
jetbrains -- teamcity	In JetBrains TeamCity before 2024.03 server administrators could remove arbitrary files from the server by installing tools	2024-03-28	4.1	CVE-2024-31140
jewel_theme -- master_addons_for_elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jewel Theme Master Addons for Elementor allows Stored XSS.This issue affects Master Addons for Elementor: from n/a through 2.0.5.4.1.	2024-03-27	6.5	CVE-2024-29911
jordy_meow -- ai_engine:_chatgpt_chatbot	Server-Side Request Forgery (SSRF) vulnerability in Jordy Meow AI Engine: ChatGPT Chatbot.This issue affects AI Engine: ChatGPT Chatbot: from n/a through 2.1.4.	2024-03-28	6.8	CVE-2024-29090
jory_hogeveen -- off-canvas_sidebars_&_menus_(slidebars)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jory Hogeveen Off-Canvas Sidebars & Menus (Slidebars) allows Stored XSS.This issue affects Off-Canvas Sidebars & Menus (Slidebars): from n/a through 0.5.8.1.	2024-03-27	6.5	CVE-2024-29762
jumpserver -- jumpserver	JumpServer is an open source bastion host and an operation and maintenance security audit system. An authorized attacker can obtain sensitive information contained within playbook files if they manage to learn the playbook_id of another user. This breach of confidentiality can lead to information disclosure and exposing sensitive data. This vulnerability is fixed in v3.10.6.	2024-03-29	4.6	CVE-2024-29020
jumpserver -- jumpserver	JumpServer is an open source bastion host and an operation and maintenance security audit system. An authenticated user can exploit the Insecure Direct Object Reference (IDOR) vulnerability in the file manager's bulk transfer by manipulating job IDs to upload malicious files, potentially compromising the integrity and security of the system. This vulnerability is fixed in v3.10.6.	2024-03-29	4.6	CVE-2024-29024
katex -- katex	KaTeX is a JavaScript library for TeX math rendering on the web. KaTeX users who render untrusted mathematical expressions could encounter malicious input using `\edef` that causes a near-infinite loop, despite setting `maxExpand` to avoid such loops. This can be used as an availability attack, where e.g. a client rendering another user's KaTeX input will be unable to use the site due to memory overflow, tying up the main thread, or stack overflow. Upgrade to KaTeX v0.16.10 to remove this vulnerability.	2024-03-25	6.5	CVE-2024-28243
katex -- katex	KaTeX is a JavaScript library for TeX math rendering on the web. KaTeX users who render untrusted mathematical expressions could encounter malicious input using `\def` or `\newcommand` that causes a near-infinite loop, despite setting `maxExpand` to avoid such loops. KaTeX supports an option named maxExpand which aims to prevent infinitely recursive macros from consuming all available memory and/or triggering a stack overflow error. Unfortunately, support for "Unicode (sub|super)script characters" allows an attacker to bypass this limit. Each sub/superscript group instantiated a separate Parser with its own limit on macro executions, without inheriting the current count of macro executions from its parent. This has been corrected in KaTeX v0.16.10.	2024-03-25	6.5	CVE-2024-28244
katex -- katex	KaTeX is a JavaScript library for TeX math rendering on the web. KaTeX users who render untrusted mathematical expressions could encounter malicious input using	2024-03-25	6.3	CVE-2024-28245

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`\includegraphics` that runs arbitrary JavaScript, or generate invalid HTML. Upgrade to KaTeX v0.16.10 to remove this vulnerability.			
katex -- katex	KaTeX is a JavaScript library for TeX math rendering on the web. Code that uses KaTeX's `trust` option, specifically that provides a function to blacklist certain URL protocols, can be fooled by URLs in malicious inputs that use uppercase characters in the protocol. In particular, this can allow for malicious input to generate `javascript:` links in the output, even if the `trust` function tries to forbid this protocol via `trust: (context) => context.protocol !== 'javascript'`. Upgrade to KaTeX v0.16.10 to remove this vulnerability.	2024-03-25	5.5	CVE-2024-28246
kienso -- co-marquage_service-public.fr	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kienso Co-marquage service-public.Fr allows Stored XSS.This issue affects Co-marquage service-public.Fr: from n/a through 0.5.71.	2024-03-27	6.5	CVE-2024-29908
kimai -- kimai	Kimai is a web-based multi-user time-tracking application. The permission `view_other_timesheet` performs differently for the Kimai UI and the API, thus returning unexpected data through the API. When setting the `view_other_timesheet` permission to true, on the frontend, users can only see timesheet entries for teams they are a part of. When requesting all timesheets from the API, however, all timesheet entries are returned, regardless of whether the user shares team permissions or not. This vulnerability is fixed in 2.13.0.	2024-03-28	6.8	CVE-2024-29200
kitforest -- better_elementor_addons	The Better Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the widget link URL values in all versions up to, and including, 1.4.1 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.	2024-03-29	6.4	CVE-2024-2280
klarna -- klarna_payments_for_woocommerce	Missing Authorization vulnerability in Klarna Klarna Payments for WooCommerce.This issue affects Klarna Payments for WooCommerce: from n/a through 3.2.4.	2024-03-29	5.3	CVE-2024-30477
klbtheme -- clotya_theme	Cross-Site Request Forgery (CSRF) vulnerability in KlbTheme Clotya theme, KlbTheme Cosmetsy theme, KlbTheme Furnob theme, KlbTheme Bacola theme, KlbTheme Partdo theme, KlbTheme Medibazar theme, KlbTheme Machic theme.This issue affects Clotya theme: from n/a through 1.1.6; Cosmetsy theme: from n/a through 1.7.7; Furnob theme: from n/a through 1.2.2; Bacola theme: from n/a through 1.3.3; Partdo theme: from n/a through 1.1.1; Medibazar theme: from n/a through 1.8.6; Machic theme: from n/a through 1.2.8.	2024-03-26	4.3	CVE-2023-49838
krunal_prajapati -- wp_post_disclaimer	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Krunal Prajapati WP Post Disclaimer allows Stored XSS.This issue affects WP Post Disclaimer: from n/a through 1.0.3.	2024-03-27	6.5	CVE-2024-29761
kstover -- ninja_forms_contact_form_-_the_drag_and_drop_form_builder_for_wordpress	The Ninja Forms Contact Form - The Drag and Drop Form Builder for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via an image title embedded into a form in all versions up to, and including, 3.8.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-29	4.6	CVE-2024-2108
kstover -- ninja_forms_contact_form_-	The Ninja Forms Contact Form - The Drag and Drop Form Builder for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.8.0. This is due to missing or incorrect nonce validation on the	2024-03-29	4.3	CVE-2024-2113

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_the_drag_and_drop_form_builder_for_wordpress	nf_download_all_subs AJAX action. This makes it possible for unauthenticated attackers to trigger an export of a form's submission to a publicly accessible location via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.			
kurudrive -- vk_all_in_one_expansion_unit	The VK All in One Expansion Unit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the child page index widget in all versions up to, and including, 9.96.0.1 due to insufficient input sanitization and output escaping on user supplied attributes such as 'className.' 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.	2024-03-26	6.4	CVE-2024-2170
labib_ahmed -- carousel_anything_for_wpbakery_page_builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Labib Ahmed Carousel Anything For WPBakery Page Builder allows Stored XSS.This issue affects Carousel Anything For WPBakery Page Builder: from n/a through 2.1.	2024-03-29	6.5	CVE-2024-30520
landingi -- landingi_landing_pages	Cross-Site Request Forgery (CSRF) vulnerability in Landingi Landingi Landing Pages.This issue affects Landingi Landing Pages: from n/a through 3.1.1.	2024-03-29	5.4	CVE-2024-30521
lg_electronics -- lg_led_assistant	This vulnerability allows remote attackers to traverse paths via file upload on the affected LG LED Assistant.	2024-03-25	5.3	CVE-2024-2863 product.security@lge.com
litonice13 -- master_addons_-_free_widgets_hover_effects_toggle_conditions_animations_for_elementor	The Master Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Pricing Table widget in all versions up to, and including, 2.0.5.6 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.	2024-03-27	6.4	CVE-2024-2139
livemesh -- livemesh_addons_for_wpbakery_page_builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Livemesh Livemesh Addons for WPBakery Page Builder allows Stored XSS.This issue affects Livemesh Addons for WPBakery Page Builder: from n/a through 3.7.	2024-03-27	6.5	CVE-2024-30183
loncar -- easy_appointments	The Easy Appointments plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ea_full_calendar' shortcode in all versions up to, and including, 3.11.18 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.	2024-03-29	6.4	CVE-2024-2842
loncar -- easy_appointments	The Easy Appointments plugin for WordPress is vulnerable to unauthorized modification of data due to insufficient user validation on the ajax_cancel_appointment() function in all versions up to, and including, 3.11.18. This makes it possible for unauthenticated attackers to cancel other users orders.	2024-03-29	4.3	CVE-2024-2844
looking_forward_software_incorporated. -- popup_builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Looking Forward Software Incorporated. Popup Builder allows Stored XSS.This issue affects Popup Builder: from n/a through 4.2.6.	2024-03-27	6.5	CVE-2024-30184

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
lordicon -- lordicon_animated_icons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Lordicon Lordicon Animated Icons allows Stored XSS.This issue affects Lordicon Animated Icons: from n/a through 2.0.1.	2024-03-29	6.5	CVE-2024-30519
mailmunch -- mailchimp_forms_by_mailmunch	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MailMunch MailChimp Forms by MailMunch allows Stored XSS.This issue affects MailChimp Forms by MailMunch: from n/a through 3.2.2.	2024-03-27	6.5	CVE-2024-29793
mainwp -- mainwp_wordfence_extension	Missing Authorization vulnerability in MainWP MainWP Wordfence Extension.This issue affects MainWP Wordfence Extension: from n/a through 4.0.7.	2024-03-25	5.4	CVE-2023-22699
mark_kinchin -- beds24_online_booking	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mark Kinchin Beds24 Online Booking allows Stored XSS.This issue affects Beds24 Online Booking: from n/a through 2.0.24.	2024-03-27	6.5	CVE-2023-52228
martyn_chamberlin -- don't_muck_my_markup	Cross-Site Request Forgery (CSRF) vulnerability in Martyn Chamberlin Don't Muck My Markup.This issue affects Don't Muck My Markup: from n/a through 1.8.	2024-03-27	4.3	CVE-2024-23510
marubon -- pocket_news_generator	The Pocket News Generator plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.2.0. This is due to missing or incorrect nonce validation on the option_page() function. This makes it possible for unauthenticated attackers to update the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-29	5.4	CVE-2024-2964
marubon -- pocket_news_generator	The Pocket News Generator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings such as "Consumer Key" and "Access Token" in all versions up to, and including, 0.2.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-03-29	4.4	CVE-2024-2963
megamenu -- max_mega_menu	Missing Authorization vulnerability in Megamenu Max Mega Menu.This issue affects Max Mega Menu: from n/a through 3.3.	2024-03-28	5.4	CVE-2024-28003
mehanoid.pro -- flatpm	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mehanoid.Pro FlatPM allows Stored XSS.This issue affects FlatPM: from n/a before 3.1.05.	2024-03-27	6.5	CVE-2024-29803
metagauss -- eventprime	Cross Site Scripting (XSS) vulnerability in Metagauss EventPrime.This issue affects EventPrime: from n/a through 3.3.9.	2024-03-27	5.9	CVE-2024-29776
metagauss -- profilegrid_	Authorization Bypass Through User-Controlled Key vulnerability in Metagauss ProfileGrid.This issue affects ProfileGrid : from n/a through 5.7.2.	2024-03-29	6.5	CVE-2024-30513

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
metagauss -- registrationmagic	Cross-Site Request Forgery (CSRF) vulnerability in Metagauss RegistrationMagic.This issue affects RegistrationMagic: from n/a through 5.3.0.0.	2024-03-26	4.3	CVE-2024-2951
miraheze -- createwiki	CreateWiki is Miraheze's MediaWiki extension for requesting & creating wikis. Suppression of wiki requests does not work as intended, and always restricts visibility to those with the `(createwiki)` user right regardless of the settings one sets on a given wiki request. This may expose information to users who are not supposed to be able to access it.	2024-03-26	4.9	CVE-2024-29883
miraheze -- createwiki	CreateWiki is Miraheze's MediaWiki extension for requesting & creating wikis. It is possible for users with (delete) or (suppressrevision) on any wiki in the farm to access suppressed wiki requests by going to the request's entry on Special:RequestWikiQueue on the wiki where they have these rights. The same vulnerability was present briefly on the REST API before being quickly corrected in commit `6bc0685`. To our knowledge, the vulnerable commits of the REST API are not running in production anywhere. This vulnerability is fixed in 23415c17ffb4832667c06abcf1eadadefd4c8937.	2024-03-28	4.9	CVE-2024-29897
miraheze -- createwiki	CreateWiki is Miraheze's MediaWiki extension for requesting & creating wikis. An oversight during the writing of the patch for CVE-2024-29897 may have exposed suppressed wiki requests to private wikis that added Special:RequestWikiQueue to the read whitelist to users without the `(read)` permission. This vulnerability is fixed in 8f8442ed5299510ea3e58416004b9334134c149c.	2024-03-28	4.9	CVE-2024-29898
molongui -- molongui	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Molongui allows Stored XSS.This issue affects Molongui: from n/a through 4.7.7.	2024-03-27	6.5	CVE-2024-29764
motopress -- stratum	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MotoPress Stratum allows Stored XSS.This issue affects Stratum: from n/a through 1.3.15.	2024-03-27	6.5	CVE-2024-29914
moveaddons -- move_addons_for_elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Moveaddons Move Addons for Elementor allows Stored XSS.This issue affects Move Addons for Elementor: from n/a through 1.2.9.	2024-03-27	6.5	CVE-2024-29920
muffingroup -- betheme	Missing Authorization vulnerability in Muffingroup Betheme.This issue affects Betheme: from n/a through 26.6.1.	2024-03-25	5.4	CVE-2022-45351
muffingroup -- betheme	Missing Authorization vulnerability in Muffingroup Betheme.This issue affects Betheme: from n/a through 26.6.1.	2024-03-25	5.4	CVE-2022-45352
muffingroup -- betheme	Missing Authorization vulnerability in Muffingroup Betheme.This issue affects Betheme: from n/a through 26.6.1.	2024-03-25	5.4	CVE-2022-45356
muffingroup -- betheme	Missing Authorization vulnerability in Muffingroup Betheme.This issue affects Betheme: from n/a through 26.6.1.	2024-03-25	4.3	CVE-2022-45349
multivendorx -- wc_marketplace	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MultiVendorX WC Marketplace allows Stored XSS.This issue affects WC Marketplace: from n/a through 4.1.3.	2024-03-29	6.5	CVE-2024-30433

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
munirkamal -- gutenberg_block_editor_toolkit_-_editorskit	The Gutenberg Block Editor Toolkit - EditorsKit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'editorskit' shortcode in all versions up to, and including, 1.40.4 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.	2024-03-30	6.4	CVE-2024-2794
n/a -- compact_wp_audio_player	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Compact WP Audio Player allows Stored XSS.This issue affects Compact WP Audio Player: from n/a through 1.9.9.	2024-03-27	6.5	CVE-2024-29917
n/a -- portfolio_gallery_-_image_gallery_plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Portfolio Gallery - Image Gallery Plugin allows Stored XSS.This issue affects Portfolio Gallery - Image Gallery Plugin: from n/a through 1.5.6.	2024-03-27	6.5	CVE-2024-29769
n/a -- qdrant	A vulnerability was found in Qdrant up to 1.6.1/1.7.4/1.8.2 and classified as critical. This issue affects some unknown processing of the file lib/collection/src/collection/snapshots.rs of the component Full Snapshot REST API. The manipulation leads to path traversal. Upgrading to version 1.8.3 is able to address this issue. The patch is named 3ab5172e9c8f14fa1f7b24e7147eac74e2412b62. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-258611.	2024-03-29	5.5	CVE-2024-3078
n/a -- wp-crm_system	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP-CRM System allows Stored XSS.This issue affects WP-CRM System: from n/a through 3.2.9.	2024-03-29	5.9	CVE-2024-30434
netentsec -- ns-asg_application_security_gateway	A vulnerability, which was classified as critical, was found in Netentsec NS-ASG Application Security Gateway 6.3. This affects an unknown part of the file /admin/list_crl_conf. The manipulation of the argument CRLId leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258429 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-28	6.3	CVE-2024-3040
netentsec -- ns-asg_application_security_gateway	A vulnerability has been found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. This vulnerability affects unknown code of the file /protocol/log/listloginfo.php. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-258430 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-28	6.3	CVE-2024-3041
netty -- netty	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. The `HttpPostRequestDecoder` can be tricked to accumulate data. While the decoder can store items on the disk if configured so, there are no limits to the number of fields the form can have, an attacher can send a chunked post consisting of many small fields that will be accumulated in the `bodyListHttpData` list. The decoder cumulates bytes in the `undecodedChunk` buffer until it can decode a field, this field can cumulate data without limits. This vulnerability is fixed in 4.1.108.Final.	2024-03-25	5.3	CVE-2024-29025
netweblogic -- events_manager_-_calendar_bookings_tickets_and_mor	The Events Manager - Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the physical location value in all versions up to, and including, 6.4.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with	2024-03-28	6.4	CVE-2024-2111

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
e!	contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
netweblogic -- events_manager_-_calendar_bookings_tickets_and_more!	The Events Manager - Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.4.7.1. This is due to missing or incorrect nonce validation on several actions. This makes it possible for unauthenticated attackers to modify booking statuses via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-28	4.3	CVE-2024-2110
nickys -- image_map_pro	Cross-Site Request Forgery (CSRF) vulnerability in Nickys Image Map Pro allows Stored XSS.This issue affects Image Map Pro: from n/a before 5.6.9.	2024-03-28	6.1	CVE-2022-45850
niteothemes -- cmp_-_coming_soon_&_maintenance	Server-Side Request Forgery (SSRF) vulnerability in NiteoThemes CMP - Coming Soon & Maintenance.This issue affects CMP - Coming Soon & Maintenance: from n/a through 4.1.10.	2024-03-28	5.5	CVE-2023-50374
nuuo -- camera	A vulnerability was found in NUUO Camera up to 20240319 and classified as problematic. This issue affects some unknown processing of the file /deletefile.php. The manipulation of the argument filename leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258197 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	5.4	CVE-2024-2995
nvidia -- gpu_display_driver_vgpu_driver_cloud_gaming_driver	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability where a user may cause a NULL-pointer dereference by accessing passed parameters the validity of which has not been checked. A successful exploit of this vulnerability may lead to denial of service and limited information disclosure.	2024-03-27	6.1	CVE-2024-0075
nvidia -- gpu_display_driver_vgpu_driver_cloud_gaming_driver	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user in a guest can cause a NULL-pointer dereference in the host, which may lead to denial of service.	2024-03-27	6.5	CVE-2024-0078
nvidia -- vgpu_driver,_cloud_gaming_driver	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a user in a guest VM can cause a NULL-pointer dereference in the host. A successful exploit of this vulnerability may lead to denial of service.	2024-03-27	6.5	CVE-2024-0079
oceanwp -- oceanwp	The OceanWP theme for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the load_theme_panel_pane function in all versions up to, and including, 3.5.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to expose sensitive information such as system/environment data and API keys.	2024-03-29	4.3	CVE-2024-2476
oroinc -- orocommerce	OroPlatform is a PHP Business Application Platform (BAP). Navigation history, most viewed and favorite navigation items are returned to storefront user in JSON navigation response if ID of storefront user matches ID of back-office user. This vulnerability is fixed in 5.1.4.	2024-03-25	4.3	CVE-2023-48296
oroinc -- platform	OroPlatform is a PHP Business Application Platform (BAP). A logged in user can access page state data of pinned pages of other users by pageId hash. This vulnerability is fixed in 5.1.4.	2024-03-25	4.3	CVE-2023-45824

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
paid_memberships_pro -- paid_memberships_pro_-_payfast_gateway_add_on	Insertion of Sensitive Information into Log File vulnerability in Paid Memberships Pro Paid Memberships Pro - Payfast Gateway Add On.This issue affects Paid Memberships Pro - Payfast Gateway Add On: from n/a through 1.4.1.	2024-03-29	5.3	CVE-2024-30514
patrick_posner -- simply_static	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Patrick Posner Simply Static allows Stored XSS.This issue affects Simply Static: from n/a through 3.1.3.	2024-03-27	5.9	CVE-2024-30178
peepso -- community_by_peepso	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in PeepSo Community by PeepSo.This issue affects Community by PeepSo: from n/a through 6.0.9.0.	2024-03-26	5.3	CVE-2023-27630
peepso -- community_by_peepso	Insertion of Sensitive Information into Log File vulnerability in PeepSo Community by PeepSo.This issue affects Community by PeepSo: from n/a through 6.2.7.0.	2024-03-28	5.3	CVE-2024-25923
petri_damstÃƒÆ'Ã,Â©n -- fullscreen_galleria	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Petri DamstÃƒÂ©n Fullscreen Galleria allows Stored XSS.This issue affects Fullscreen Galleria: from n/a through 1.6.11.	2024-03-27	6.5	CVE-2024-29801
phpgurukul -- emergency_ambulance_hiring_portal	A vulnerability was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. It has been rated as problematic. This issue affects some unknown processing of the component Hire an Ambulance Page. The manipulation of the argument Patient Name/Relative Name/Relative Phone Number/City/State/Message leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258677 was assigned to this vulnerability.	2024-03-30	4.3	CVE-2024-3084
phpgurukul -- emergency_ambulance_hiring_portal	A vulnerability classified as problematic was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. Affected by this vulnerability is an unknown functionality of the file ambulance-tracking.php of the component Ambulance Tracking Page. The manipulation of the argument searchdata leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258679.	2024-03-30	4.3	CVE-2024-3086
phpgurukul -- emergency_ambulance_hiring_portal	A vulnerability has been found in PHPGurukul Emergency Ambulance Hiring Portal 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/manage-ambulance.php of the component Manage Ambulance Page. The manipulation of the argument del leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-258682 is the identifier assigned to this vulnerability.	2024-03-30	4.3	CVE-2024-3089
pimcore -- pimcore	Pimcore is an Open Source Data & Experience Management Platform. Any call with the query argument `?pimcore_preview=true` allows to view unpublished sites. In previous versions of Pimcore, session information would propagate to previews, so only a logged in user could open a preview. This no longer applies. Previews are broad open to any user and with just the hint of a restricted link one could gain access to possible confident / unreleased information. This vulnerability is fixed in 11.2.2 and 11.1.6.1.	2024-03-26	6.5	CVE-2024-29197

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
piotnet -- piotnet_addons_for_elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Piotnet Piotnet Addons For Elementor allows Stored XSS.This issue affects Piotnet Addons For Elementor: from n/a through 2.4.25.	2024-03-27	6.5	CVE-2024-29934
pixelite -- events_manager	Cross-Site Request Forgery (CSRF) vulnerability in Pixelite Events Manager.This issue affects Events Manager: from n/a through 6.4.7.1.	2024-03-28	4.3	CVE-2024-30421
plainware -- locatoraid_store_locator	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Plainware Locatoraid Store Locator allows Stored XSS.This issue affects Locatoraid Store Locator: from n/a through 3.9.30.	2024-03-27	5.9	CVE-2024-30181
pluginops -- landing_page_builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PluginOps Landing Page Builder allows Stored XSS.This issue affects Landing Page Builder: from n/a through 1.5.1.7.	2024-03-29	5.9	CVE-2024-30452
podlove -- podlove_web_player	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Podlove Podlove Web Player allows Stored XSS.This issue affects Podlove Web Player: from n/a through 5.7.1.	2024-03-27	6.5	CVE-2024-29788
poll_maker_&_voting_plugin_team_(infotheme) -- wp_poll_maker	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Poll Maker & Voting Plugin Team (InfoTheme) WP Poll Maker allows Stored XSS.This issue affects WP Poll Maker: from n/a through 3.1.	2024-03-27	5.9	CVE-2024-29818
posimyththemes -- the_plus_addons_for_elementor	The The Plus Addons for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 5.4.1 via the Clients widget. This makes it possible for authenticated attackers, with contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.	2024-03-27	6.4	CVE-2024-2203
posimyththemes -- the_plus_addons_for_elementor	The The Plus Addons for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 5.4.1 via the Team Member Listing widget. This makes it possible for authenticated attackers, with contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.	2024-03-27	6.4	CVE-2024-2210
propertyhive -- propertyhive	Missing Authorization vulnerability in PropertyHive.This issue affects PropertyHive: from n/a through 2.0.6.	2024-03-26	4.3	CVE-2024-24718
quantum_cloud -- slider_hero	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Quantum Cloud Slider Hero allows Stored XSS.This issue affects Slider Hero: from n/a through 8.6.1.	2024-03-27	5.9	CVE-2024-29922
realmag777 -- bear	Missing Authorization vulnerability in realmag777 BEAR.This issue affects BEAR: from n/a through 1.1.4.3.	2024-03-29	4.3	CVE-2024-30463
realmag777 -- husky_-_products_filter_f	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 HUSKY - Products Filter for WooCommerce (formerly WOOF).This issue affects HUSKY - Products Filter for WooCommerce (formerly WOOF): from n/a through 1.3.5.1.	2024-03-29	4.3	CVE-2024-30462

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
or_woocommerce_(formerly_woof)				
realmag777 -- woocs_-_woocommerce_currency_switcher	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 WOOCS - WooCommerce Currency Switcher.This issue affects WOOCS - WooCommerce Currency Switcher: from n/a through 1.4.1.7.	2024-03-29	4.3	CVE-2024-30458
realmag777 -- wordpress_meta_data_and_taxonomies_filter_(mdtf)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in realmag777 WordPress Meta Data and Taxonomies Filter (MDTF) allows Stored XSS.This issue affects WordPress Meta Data and Taxonomies Filter (MDTF): from n/a through 1.3.2.	2024-03-27	6.5	CVE-2024-29906
realmag777 -- wordpress_meta_data_and_taxonomies_filter_(mdtf)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in realmag777 WordPress Meta Data and Taxonomies Filter (MDTF) allows Stored XSS.This issue affects WordPress Meta Data and Taxonomies Filter (MDTF): from n/a through 1.3.2.	2024-03-27	6.5	CVE-2024-29932
realmag777 -- wordpress_meta_data_and_taxonomies_filter_(mdtf)	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 WordPress Meta Data and Taxonomies Filter (MDTF).This issue affects WordPress Meta Data and Taxonomies Filter (MDTF): from n/a through 1.3.3.1.	2024-03-29	4.3	CVE-2024-30457
realmag777 -- wpcs	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 WPCS.This issue affects WPCS: from n/a through 1.2.0.1.	2024-03-29	4.3	CVE-2024-30456
rednao -- pdf_builder_for_wpforms	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RedNao PDF Builder for WPForms allows Stored XSS.This issue affects PDF Builder for WPForms: from n/a through 1.2.88.	2024-03-27	6.5	CVE-2024-29820
reviewx -- reviewx	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ReviewX allows Stored XSS.This issue affects ReviewX: from n/a through 1.6.22.	2024-03-27	6.5	CVE-2024-29812
rockwell_automation -- arena_simulation	A memory buffer vulnerability in Rockwell Automation Arena Simulation could potentially let a threat actor read beyond the intended memory boundaries. This could reveal sensitive information and even cause the application to crash, resulting in a denial-of-service condition. To trigger this, the user would unwittingly need to open a malicious file shared by the threat actor.	2024-03-26	4.4	CVE-2024-21920
rockwell_automation -- factorytalk-_view_me	A vulnerability exists in the affected product that allows a malicious user to restart the Rockwell Automation PanelViewÃ¢â€žÂ¢ Plus 7 terminal remotely without security protections. If the vulnerability is exploited, it could lead to the loss of view or control of the PanelViewÃ¢â€žÂ¢ product.	2024-03-25	5.3	CVE-2024-21914
ruijie -- rg-eg350	A vulnerability, which was classified as critical, has been found in Ruijie RG-EG350 up to 20240318. Affected by this issue is the function vpnAction of the file /itbox_pi/vpn_quickset_service.php?a=set_vpn of the component HTTP POST Request Handler. The manipulation of the argument ip/port/user/pass/dns/startIp leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257978 is the identifier	2024-03-26	6.3	CVE-2024-2910

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
saleor -- saleor	Saleor is an e-commerce platform that serves high-volume companies. When using `Pickup: Local stock only` click-and-collect as a delivery method in specific conditions the customer could overwrite the warehouse address with its own, which exposes its address as click-and-collect address. This issue has been patched in versions: `3.14.61`, `3.15.37`, `3.16.34`, `3.17.32`, `3.18.28`, `3.19.15`.	2024-03-27	4.2	CVE-2024-29888
seraphinite_solutions -- seraphinite_accelerator	Insertion of Sensitive Information into Log File vulnerability in Seraphinite Solutions Seraphinite Accelerator.This issue affects Seraphinite Accelerator: from n/a through 2.20.47.	2024-03-28	5.3	CVE-2024-22138
serverpod -- serverpod	Serverpod is an app and web server, built for the Flutter and Dart ecosystem. An issue was identified with the old password hash algorithm that made it susceptible to rainbow attacks if the database was compromised. This vulnerability is fixed by 1.2.6.	2024-03-27	5.3	CVE-2024-29886
servit_software_solutions -- affiliate-toolkit	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SERVIT Software Solutions affiliate-toolkit allows Stored XSS.This issue affects affiliate-toolkit: from n/a through 3.4.5.	2024-03-27	6.5	CVE-2024-29817
shanghai_brad_technology -- bladex	A vulnerability classified as critical has been found in Shanghai Brad Technology BladeX 3.4.0. Affected is an unknown function of the file /api/blade-user/export-user of the component API. The manipulation with the input updatexml(1,concat(0x3f,md5(123456),0x3f),1)=1 leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-258426 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-28	6.3	CVE-2024-3039
sharethis -- sharethis_dashboard_for_google_analytics	Missing Authorization vulnerability in ShareThis ShareThis Dashboard for Google Analytics.This issue affects ShareThis Dashboard for Google Analytics: from n/a through 3.1.4.	2024-03-25	5.4	CVE-2022-45851
simple_sponsorships -- sponsors	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Simple Sponsorships Sponsors allows Stored XSS.This issue affects Sponsors: from n/a through 3.5.1.	2024-03-29	6.5	CVE-2024-30483
sinaextra -- sina_extension_for_elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SinaExtra Sina Extension for Elementor allows Stored XSS.This issue affects Sina Extension for Elementor: from n/a through 3.5.0.	2024-03-27	6.5	CVE-2024-29935
snp_digital -- salesking	Missing Authorization vulnerability in SNP Digital SalesKing.This issue affects SalesKing: from n/a through 1.6.15.	2024-03-26	6.5	CVE-2024-22156

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
softlab -- dracula_dark_mode_-_the_revolutionary_dark_mode_plugin_for_wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SoftLab Dracula Dark Mode - The Revolutionary Dark Mode Plugin For WordPress allows Stored XSS.This issue affects Dracula Dark Mode - The Revolutionary Dark Mode Plugin For WordPress: from n/a through 1.0.8.	2024-03-27	6.5	CVE-2024-29771
softlab -- radio_player	Missing Authorization vulnerability in SoftLab Radio Player.This issue affects Radio Player: from n/a through 2.0.73.	2024-03-26	6.5	CVE-2024-2906
softlab -- radio_player	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SoftLab Radio Player allows Stored XSS.This issue affects Radio Player: from n/a through 2.0.73.	2024-03-27	6.5	CVE-2024-29811
sourcecodester -- online_chatting_system	A vulnerability classified as critical has been found in SourceCodester Online Chatting System 1.0. Affected is an unknown function of the file admin/update_room.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258012.	2024-03-27	6.3	CVE-2024-2932
sourcecodester -- simple_subscription_website	A vulnerability classified as critical has been found in SourceCodester Simple Subscription Website 1.0. Affected is an unknown function of the file Actions.php. The manipulation of the argument title leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258300.	2024-03-28	6.3	CVE-2024-3014
sourcecodester -- simple_subscription_website	A vulnerability classified as critical was found in SourceCodester Simple Subscription Website 1.0. Affected by this vulnerability is an unknown functionality of the file manage_plan.php. The 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. The identifier VDB-258301 was assigned to this vulnerability.	2024-03-28	6.3	CVE-2024-3015
sourcecodester -- simple_subscription_website	A vulnerability was found in SourceCodester Simple Subscription Website 1.0 and classified as critical. This issue affects some unknown processing of the file manage_user.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258431.	2024-03-28	6.3	CVE-2024-3042
sourcecodester -- todo_list_in_kanban_board	A vulnerability classified as critical was found in SourceCodester Todo List in Kanban Board 1.0. Affected by this vulnerability is an unknown functionality of the file /endpoint/delete-todo.php. The manipulation of the argument list leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-258013 was assigned to this vulnerability.	2024-03-27	6.3	CVE-2024-2934
sparkle_wp -- educenter	Missing Authorization vulnerability in Sparkle WP Educenter.This issue affects Educenter: from n/a through 1.5.5.	2024-03-25	4.3	CVE-2023-30480
specialk -- simple_ajax_chat_-_add_a_fast_secure_chat_box	The Simple Ajax Chat - Add a Fast, Secure Chat Box plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 20231101 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	2024-03-27	4.4	CVE-2024-2956

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.			
squirrly -- seo_plugin_by_squirrly_seo	Missing Authorization vulnerability in Squirrly SEO Plugin by Squirrly SEO.This issue affects SEO Plugin by Squirrly SEO: from n/a through 12.1.20.	2024-03-25	6.3	CVE-2022-44626
step-byte-service_gmbh -- openstreetmap_for_gutenberg_and_wpbakery_page_builder_(formerly_visual_composer)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Step-Byte-Service GmbH OpenStreetMap for Gutenberg and WPBakery Page Builder (formerly Visual Composer) allows Stored XSS.This issue affects OpenStreetMap for Gutenberg and WPBakery Page Builder (formerly Visual Composer): from n/a through 1.1.1.	2024-03-29	6.5	CVE-2024-30450
stormhill_media -- mybooktable_bookstore	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stormhill Media MyBookTable Bookstore allows Stored XSS.This issue affects MyBookTable Bookstore: from n/a through 3.3.7.	2024-03-27	6.5	CVE-2024-29772
streamweasels -- streamweasels_twitch_integration	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in StreamWeasels StreamWeasels Twitch Integration allows Stored XSS.This issue affects StreamWeasels Twitch Integration: from n/a through 1.7.5.	2024-03-27	6.5	CVE-2024-29766
supsystic -- photo_gallery_by_supsystic	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Supsystic Photo Gallery by Supsystic allows Stored XSS.This issue affects Photo Gallery by Supsystic: from n/a through 1.15.16.	2024-03-27	5.9	CVE-2024-29921
supsystic -- slider_by_supsystic	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Supsystic Slider by Supsystic allows Stored XSS.This issue affects Slider by Supsystic: from n/a through 1.8.10.	2024-03-29	5.9	CVE-2024-30448
swift-server -- swift-prometheus	Swift Prometheus is a Swift client for the Prometheus monitoring system, supporting counters, gauges and histograms. In code which applies _un-sanitized string values into metric names or labels_, an attacker could make use of this and send a `?lang` query parameter containing newlines, `}` or similar characters which can lead to the attacker taking over the exported format -- including creating unbounded numbers of stored metrics, inflating server memory usage, or causing "bogus" metrics. This vulnerability is fixed in2.0.0-alpha.2.	2024-03-29	5.9	CVE-2024-28867
syam_mohan -- wpfront_notification_bar	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Syam Mohan WPFront Notification Bar allows Stored XSS.This issue affects WPFront Notification Bar: from n/a through 3.3.2.	2024-03-27	5.9	CVE-2024-29819
synology -- surveillance_station	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Layout.LayoutSave webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	CVE-2024-29227
synology -- surveillance_station	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in SnapShot.CountByCategory webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	CVE-2024-29230

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
synology -- surveillance_station	Improper validation of array index vulnerability in UserPrivilege.Enum webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to bypass security constraints via unspecified vectors.	2024-03-28	5.4	CVE-2024-29231
synology -- surveillance_station	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Alert.Enum webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	CVE-2024-29232
synology -- surveillance_station	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Emap.Delete webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	CVE-2024-29233
synology -- surveillance_station	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Group.Save webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	CVE-2024-29234
synology -- surveillance_station	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in IOModule.EnumLog webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	CVE-2024-29235
synology -- surveillance_station	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in AudioPattern.Delete webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	CVE-2024-29236
synology -- surveillance_station	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in ActionRule.Delete webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	CVE-2024-29237
synology -- surveillance_station	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Log.CountByCategory webapi component in Synology Surveillance Station before 9.2.0-9289 and 9.2.0-11289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	CVE-2024-29238
synology -- surveillance_station	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Recording.CountByCategory webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to inject SQL commands via unspecified vectors.	2024-03-28	5.4	CVE-2024-29239
synology -- surveillance_station	Missing authorization vulnerability in LayoutSave webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to conduct denial-of-service attacks via unspecified vectors.	2024-03-28	4.3	CVE-2024-29240
team_heateor -- fancy_comments_wordpress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Team Heateor Fancy Comments WordPress allows Stored XSS.This issue affects Fancy Comments WordPress: from n/a through 1.2.14.	2024-03-27	6.5	CVE-2024-29804
technocrackers -- christmas_greetings	The Christmas Greetings plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the code parameter in all versions up to, and including, 1.2.5 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.	2024-03-29	6.1	CVE-2024-2116

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenda -- ac7	A vulnerability classified as critical has been found in Tenda AC7 15.03.06.44. Affected is the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257940. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	6.3	CVE-2024-2897
tenda -- fh1202	A vulnerability has been found in Tenda FH1202 1.2.0.14(408) and classified as critical. Affected by this vulnerability is the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac leads to command injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258151. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	5.5	CVE-2024-2982
tenda -- fh1205	A vulnerability has been found in Tenda FH1205 2.0.0.7(775) and classified as critical. Affected by this vulnerability is the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258295. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-28	6.3	CVE-2024-3009
the_beaver_builder_team -- beaver_builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in The Beaver Builder Team Beaver Builder allows Stored XSS.This issue affects Beaver Builder: from n/a through 2.7.4.4.	2024-03-29	6.5	CVE-2024-30425
themehunk -- advance_wordpress_search_plugin	Missing Authorization vulnerability in ThemeHunk Advance WordPress Search Plugin.This issue affects Advance WordPress Search Plugin: from n/a through 1.2.1.	2024-03-25	6.5	CVE-2022-38057
themeisle -- multiple_page_generator_plugin_-_mpg	Missing Authorization vulnerability in Themeisle Multiple Page Generator Plugin - MPG.This issue affects Multiple Page Generator Plugin - MPG: from n/a through 3.4.0.	2024-03-26	4.3	CVE-2024-30235
themeisle -- otter_blocks_-_gutenberg_blocks_page_builder_for_gutenberg_editor_&_fse	The Otter Blocks - Gutenberg Blocks, Page Builder for Gutenberg Editor & FSE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 2.6.5 due to insufficient input sanitization and output escaping on user supplied attributes such as 'id'. 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.	2024-03-29	6.4	CVE-2024-2841
themekraft -- buddyforms	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeKraft BuddyForms allows Reflected XSS.This issue affects BuddyForms: from n/a through 2.8.5.	2024-03-27	5.8	CVE-2024-30198
themelocation -- custom_woocommerce_checkout_fields_editor	Cross-Site Request Forgery (CSRF) vulnerability in ThemeLocation Custom WooCommerce Checkout Fields Editor.This issue affects Custom WooCommerce Checkout Fields Editor: from n/a through 1.3.0.	2024-03-29	4.3	CVE-2024-30518
themeum -- tutor_lms_elementor_addons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeum Tutor LMS Elementor Addons allows Stored XSS.This issue affects Tutor LMS Elementor Addons: from n/a through 2.1.3.	2024-03-27	6.5	CVE-2024-29913

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
themify -- themify_event_post	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themify Themify Event Post allows Stored XSS.This issue affects Themify Event Post: from n/a through 1.2.7.	2024-03-29	5.9	CVE-2024-30440
themifyme -- themify_shortcodes	The Themify Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'themify_post_slider shortcode in all versions up to, and including, 2.0.8 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.	2024-03-26	5.4	CVE-2024-2732
thimpress -- wp_hotel_booking	Missing Authorization vulnerability in ThimPress WP Hotel Booking.This issue affects WP Hotel Booking: from n/a through 2.0.9.2.	2024-03-29	6.5	CVE-2024-30508
thorsten -- phpmyfaq	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. The `email` field in phpMyFAQ's user control panel page is vulnerable to stored XSS attacks due to the inadequacy of PHP's `FILTER_VALIDATE_EMAIL` function, which only validates the email format, not its content. This vulnerability enables an attacker to execute arbitrary client-side JavaScript within the context of another user's phpMyFAQ session. This vulnerability is fixed in 3.2.6.	2024-03-25	5.5	CVE-2024-27300
thorsten -- phpmyfaq	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. By manipulating the news parameter in a POST request, an attacker can inject malicious JavaScript code. Upon browsing to the compromised news page, the XSS payload triggers. This vulnerability is fixed in 3.2.6.	2024-03-25	4.3	CVE-2024-28106
thorsten -- phpmyfaq	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. Due to insufficient validation on the `contentLink` parameter, it is possible for unauthenticated users to inject HTML code to the page which might affect other users. _Also, requires that adding new FAQs is allowed for guests and that the admin doesn't check the content of a newly added FAQ._ This vulnerability is fixed in 3.2.6.	2024-03-25	4.7	CVE-2024-28108
tianjin -- publicms	A vulnerability, which was classified as problematic, was found in Tianjin PubliCMS 4.0.202302.e. This affects an unknown part. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257979. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-26	4.3	CVE-2024-2911
tinymce -- tinymce	TinyMCE is an open source rich text editor. A cross-site scripting (XSS) vulnerability was discovered in TinyMCE's content insertion code. This allowed `iframe` elements containing malicious code to execute when inserted into the editor. These `iframe` elements are restricted in their permissions by same-origin browser protections, but could still trigger operations such as downloading of malicious assets. This vulnerability is fixed in 6.8.1.	2024-03-26	4.3	CVE-2024-29203
tinymce -- tinymce	TinyMCE is an open source rich text editor. A cross-site scripting (XSS) vulnerability was discovered in TinyMCE's content loading and content inserting code. A SVG image could be loaded though an `object` or `embed` element and that image could potentially contain a XSS payload. This vulnerability is fixed in 6.8.1 and 7.0.0.	2024-03-26	4.3	CVE-2024-29881
tsina -- news_wall	The News Wall plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.0. This is due to missing or incorrect nonce validation on the nwap_newslist_page() function. This makes it possible for	2024-03-29	4.3	CVE-2024-2970

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthenticated attackers to update the plugin's settings and modify news lists via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.			
tumult_inc -- tumult_hype_animations	Cross-Site Request Forgery (CSRF) vulnerability in Tumult Inc Tumult Hype Animations.This issue affects Tumult Hype Animations: from n/a through 1.9.11.	2024-03-29	4.3	CVE-2024-30460
uncanny_owl -- uncanny_toolkit_for_learndash	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Uncanny Owl Uncanny Toolkit for LearnDash.This issue affects Uncanny Toolkit for LearnDash: from n/a through 3.6.4.3.	2024-03-27	4.7	CVE-2023-34020
unitecms -- unlimited_elements_for_elementor_(free_widgets,_addons,_templates)	The Unlimited Elements For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the link field of an installed widget (e.g., 'Button Link') in all versions up to, and including, 1.5.96 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.	2024-03-30	6.4	CVE-2024-0367
uriahs_victor -- location_picker_at_checkout_for_woocommerce	Missing Authorization vulnerability in Uriahs Victor Location Picker at Checkout for WooCommerce.This issue affects Location Picker at Checkout for WooCommerce: from n/a through 1.8.9.	2024-03-26	4.3	CVE-2024-24719
veronalabs -- wp_sms	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VeronaLabs WP SMS allows Stored XSS.This issue affects WP SMS: from n/a through 6.3.4.	2024-03-27	6.5	CVE-2024-25920
veronalabs -- wp_sms	Cross-Site Request Forgery (CSRF) vulnerability in VeronaLabs WP SMS.This issue affects WP SMS: from n/a through 6.6.2.	2024-03-29	4.3	CVE-2024-30454
vinoth06. -- frontend_dashboard	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in vinoth06. Frontend Dashboard allows Stored XSS.This issue affects Frontend Dashboard: from n/a through 2.2.1.	2024-03-27	6.5	CVE-2024-29775
voidcoders -- void_contact_form_7_widget_for_elementor_page_builder	Missing Authorization vulnerability in voidCoders Void Contact Form 7 Widget For Elementor Page Builder.This issue affects Void Contact Form 7 Widget For Elementor Page Builder: from n/a through 2.3.	2024-03-26	4.3	CVE-2023-52214
walter_pinem -- oneclick_chat_to_order	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Walter Pinem OneClick Chat to Order allows Stored XSS.This issue affects OneClick Chat to Order: from n/a through 1.0.5.	2024-03-27	6.5	CVE-2024-29789
wc_lovers -- wcfm_-_frontend_manager_for_woocommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WC Lovers WCFM - Frontend Manager for WooCommerce allows Stored XSS.This issue affects WCFM - Frontend Manager for WooCommerce: from n/a through 6.7.8.	2024-03-27	5.9	CVE-2024-29929

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
weblizar -- lightbox_slider_-_responsive_lightbox_gallery	The Lightbox slider - Responsive Lightbox Gallery plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.9.9 via deserialization of untrusted input through post meta data. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-03-29	5.4	CVE-2024-1858
webtechstreet -- elementor_addon_elements	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 1.13.1 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.	2024-03-28	5.4	CVE-2024-2091
webtoffee -- import_export_wordpress_users	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WebToffee Import Export WordPress Users.This issue affects Import Export WordPress Users: from n/a through 2.5.2.	2024-03-29	4.3	CVE-2024-30492
wedevs -- woocommerce_conversion_tracking	Missing Authorization vulnerability in weDevs WooCommerce Conversion Tracking.This issue affects WooCommerce Conversion Tracking: from n/a through 2.0.11.	2024-03-26	4.3	CVE-2024-24711
wholesale_team -- wholesalex	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wholesale Team WholesaleX.This issue affects WholesaleX: from n/a through 1.3.1.	2024-03-26	6.5	CVE-2024-30233
wholesale_team -- wholesalex	Missing Authorization vulnerability in Wholesale Team WholesaleX.This issue affects WholesaleX: from n/a through 1.3.1.	2024-03-26	6.5	CVE-2024-30234
woocommerce -- woocommerce_box_office	Missing Authorization vulnerability in WooCommerce WooCommerce Box Office.This issue affects WooCommerce Box Office: from n/a through 1.2.2.	2024-03-26	6.5	CVE-2024-24799
woocommerce -- woocommerce_stripe_payment_gateway	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce WooCommerce Stripe Payment Gateway.This issue affects WooCommerce Stripe Payment Gateway: from n/a through 7.6.0.	2024-03-27	5.4	CVE-2023-44999
workos -- authkit-nextjs	The AuthKit library for Next.js provides helpers for authentication and session management using WorkOS & AuthKit with Next.js. A user can reuse an expired session by controlling the `x-workos-session` header. The vulnerability is patched in v0.4.2.	2024-03-29	4.8	CVE-2024-29901
wp_darko -- grid_shortcodes	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Darko Grid Shortcodes allows Stored XSS.This issue affects Grid Shortcodes: from n/a through 1.1.	2024-03-27	6.5	CVE-2024-29797
wp_email_newsletter_team_-_fluentcrm -- fluent_crm	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Email Newsletter Team - FluentCRM Fluent CRM allows Stored XSS.This issue affects Fluent CRM: from n/a through 2.8.44.	2024-03-29	5.9	CVE-2024-30430

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wp_lab -- wp-lister_lite_for_amazon	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Lab WP-Lister Lite for Amazon allows Stored XSS.This issue affects WP-Lister Lite for Amazon: from n/a through 2.6.11.	2024-03-26	5.9	CVE-2024-2889
wp_sunshine -- sunshine_photo_cart	Deserialization of Untrusted Data vulnerability in WP Sunshine Sunshine Photo Cart.This issue affects Sunshine Photo Cart: from n/a through 3.1.1.	2024-03-28	5.4	CVE-2024-30221
wp_swings -- points_and_rewards_for_woocommerce	Missing Authorization vulnerability in WP Swings Points and Rewards for WooCommerce.This issue affects Points and Rewards for WooCommerce: from n/a through 1.5.0.	2024-03-25	6.5	CVE-2023-27608
wpassist.me -- wordpress_countdown_widget	Cross-Site Request Forgery (CSRF) vulnerability in WPAssist.Me WordPress Countdown Widget allows Cross-Site Scripting (XSS).This issue affects WordPress Countdown Widget: from n/a through 3.1.9.1.	2024-03-27	6.1	CVE-2022-45847
wpexperts -- wholesale_for_woocommerce	Missing Authorization vulnerability in WPExperts Wholesale For WooCommerce.This issue affects Wholesale For WooCommerce: from n/a through 2.3.0.	2024-03-29	5.3	CVE-2024-30469
wppool -- webinar_and_video_conference_with_jitsi_meet	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPPOOL Webinar and Video Conference with Jitsi Meet allows Stored XSS.This issue affects Webinar and Video Conference with Jitsi Meet: from n/a through 2.6.3.	2024-03-29	6.5	CVE-2024-30437
wpvibes -- elementor_addon_elements	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPVibes Elementor Addon Elements allows Stored XSS.This issue affects Elementor Addon Elements: from n/a through 1.13.1.	2024-03-28	6.5	CVE-2024-30422
wpwax -- post_grid_slider_&_carousel_ultimate	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpWax Post Grid, Slider & Carousel Ultimate allows Stored XSS.This issue affects Post Grid, Slider & Carousel Ultimate: from n/a through 1.6.6.	2024-03-27	6.5	CVE-2024-29925
xpeedstudio -- elementskit_elementor_addons	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the button ID parameter in all versions up to, and including, 3.0.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-30	6.4	CVE-2024-1238
xpro -- 140+_widgets_|_best_addons_for_elementor_-_free	The 130+ Widgets | Best Addons For Elementor - FREE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 1.4.2 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 arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-29	6.4	CVE-2024-2250

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zephyrproject-rtos -- zephyr	An malicious BLE device can crash BLE victim device by sending malformed gatt packet	2024-03-29	6.8	CVE-2024-3077 vulnerabilities@zephyrproject.org
zionbuilder.io -- wordpress_page_builder_-_zion_builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in zionbuilder.Io WordPress Page Builder - Zion Builder allows Stored XSS.This issue affects WordPress Page Builder - Zion Builder: from n/a through 3.6.9.	2024-03-29	5.9	CVE-2024-30444
zitadel -- zitadel	ZITADEL, open source authentication management software, uses Go templates to render the login UI. Under certain circumstances an action could set reserved claims managed by ZITADEL. For example it would be possible to set the claim `urn:zitadel:iam:user:resourceowner:name`. To compensate for this we introduced a protection that does prevent actions from changing claims that start with `urn:zitadel:iam`. This vulnerability is fixed in 2.48.3, 2.47.8, 2.46.5, 2.45.5, 2.44.7, 2.43.11, and 2.42.17.	2024-03-27	6.1	CVE-2024-29892
3uu -- shariff_wrapper	The Shariff Wrapper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'shariff' shortcode in all versions up to, and including, 4.6.9 due to insufficient input sanitization and output escaping on user supplied attributes such as 'secondarycolor' and 'maincolor'. 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.	2024-03-21	6.4	CVE-2023-6500
3uu -- shariff_wrapper	The Shariff Wrapper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'shariff' shortcode in all versions up to, and including, 4.6.9 due to insufficient input sanitization and output escaping on user supplied attributes like 'info_text'. 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 and clicks the information icon.	2024-03-21	6.4	CVE-2024-0966
3uu -- shariff_wrapper	The Shariff Wrapper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'shariff' shortcode in all versions up to, and including, 4.6.10 due to insufficient input sanitization and output escaping on user supplied attributes such as 'align'. 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.	2024-03-21	6.4	CVE-2024-1450
N/A -- N/A	Directory Traversal vulnerability in Speedy11CZ MCRPX v.1.4.0 and before allows a local attacker to execute arbitrary code via a crafted file.	2024-03-19	5.5	CVE-2024-24043
N/A -- N/A	The SolarEdge mySolarEdge application before 2.20.1 for Android has a certificate verification issue that allows a Machine-in-the-middle (MitM) attacker to read and alter all network traffic between the application and the server.	2024-03-21	5.9	CVE-2024-28756
aam -- advanced_access_manager	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AAM Advanced Access Manager allows Stored XSS.This issue affects Advanced Access Manager: from n/a through 6.9.20.	2024-03-19	5.9	CVE-2024-29124
aankit -- easy_maintenance_mode	The Easy Maintenance Mode plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.2 via the REST API. This makes it possible for authenticated attackers to obtain post and page content via REST API thus bypassign the protection provided by the plugin.	2024-03-20	5.3	CVE-2024-1477
adobe -- adobe_experience	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject	2024-03-18	5.4	CVE-2024-20760

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_manager	malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.			
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-20768
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26028
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26030
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26031
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable web pages. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable script. This could result in arbitrary code execution in the context of the victim's browser. Exploitation of this issue requires user interaction.	2024-03-18	5.4	CVE-2024-26032
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26033
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26034
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26035
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26038
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26040
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26041
adobe -- adobe_experience	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable web pages. Malicious JavaScript may be	2024-03-18	5.4	CVE-2024-26042

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_manager	executed in a victim's browser when they browse to the page containing the vulnerable script. This could result in arbitrary code execution in the context of the victim's browser.			
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26043
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into a webpage. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable script. This could result in arbitrary code execution in the context of the victim's browser.	2024-03-18	5.4	CVE-2024-26044
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26045
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26052
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26056
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26059
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26061
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26062
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by an Information Exposure vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to gain unauthorized access to sensitive information, potentially bypassing security measures. Exploitation of this issue does not require user interaction.	2024-03-18	5.3	CVE-2024-26063
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into a webpage. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable script. This could result in arbitrary code execution in the context of the victim's browser. Exploitation of this issue requires user interaction.	2024-03-18	5.4	CVE-2024-26064
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26065

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26067
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26069
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26073
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable web pages. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable script.	2024-03-18	5.4	CVE-2024-26080
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26094
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26096
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	CVE-2024-26101
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	CVE-2024-26102
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	CVE-2024-26103
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	CVE-2024-26104
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	CVE-2024-26105
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	CVE-2024-26106
adobe -- adobe_experience	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to	2024-03-18	5.4	CVE-2024-26107

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_manager	visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.			
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	CVE-2024-26118
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized access. Exploitation of this issue does not require user interaction.	2024-03-18	5.3	CVE-2024-26119
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26120
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26124
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	5.4	CVE-2024-26125
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	4.8	CVE-2024-26050
adobe -- animate	Animate versions 24.0, 23.0.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-03-18	5.5	CVE-2024-20762
adobe -- animate	Animate versions 24.0, 23.0.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-03-18	5.5	CVE-2024-20763
adobe -- animate	Animate versions 24.0, 23.0.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-03-18	5.5	CVE-2024-20764
adobe -- bridge	Bridge versions 13.0.5, 14.0.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-03-18	5.5	CVE-2024-20757
advantech -- webaccess/scada	There is an SQL injection vulnerability in Advantech WebAccess/SCADA software that allows an authenticated attacker to remotely inject SQL code in the database. Successful exploitation of this vulnerability could allow an attacker to read or modify data on the remote database.	2024-03-21	6.4	CVE-2024-2453
anshuln90 -- animated_headline	The Animated Headline plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'animated-headline' shortcode in all versions up to, and including, 4.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with	2024-03-20	6.4	CVE-2024-2304

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
axis_communications_ab -- axis_os	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX APIs local_list.cgi, create_overlay.cgi and irissetup.cgi was vulnerable for file globbing which could lead to a resource exhaustion attack. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	2024-03-19	6.5	CVE-2024-0054
axis_communications_ab -- axis_os	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX APIs mediaclip.cgi and playclip.cgi was vulnerable for file globbing which could lead to a resource exhaustion attack. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	2024-03-19	6.5	CVE-2024-0055
bdtask -- wholesale_inventory_management_system	A vulnerability was found in Bdtask Wholesale Inventory Management System up to 20240311. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to session fixiation. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257245 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-19	4.3	CVE-2024-2639
bdthemes -- element_pack_elementor_addons	Missing Authorization vulnerability in BdThemes Element Pack Elementor Addons.This issue affects Element Pack Elementor Addons: from n/a through 5.4.11.	2024-03-23	4.3	CVE-2024-24840
benjamin_rojas -- wp_editor	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Benjamin Rojas WP Editor.This issue affects WP Editor: from n/a through 1.2.7.	2024-03-17	5.3	CVE-2024-25591
bmc -- control-m	Improper authorization in the report management and creation module of BMC Control-M branches 9.0.20 and 9.0.21 allows logged-in users to read and make unauthorized changes to any reports available within the application, even without proper permissions. The attacker must know the unique identifier of the report they want to manipulate. Fix for 9.0.20 branch was released in version 9.0.20.238. Fix for 9.0.21 branch was released in version 9.0.21.201.	2024-03-18	6.4	CVE-2024-1604
bmc -- control-m	BMC Control-M branches 9.0.20 and 9.0.21 upon user login load all Dynamic Link Libraries (DLL) from a directory that grants Write and Read permissions to all users. Leveraging it leads to loading of a potentially malicious libraries, which will execute with the application's privileges. Fix for 9.0.20 branch was released in version 9.0.20.238. Fix for 9.0.21 branch was released in version 9.0.21.201.	2024-03-18	6.6	CVE-2024-1605
bmc -- control-m	Lack of input sanitization in BMC Control-M branches 9.0.20 and 9.0.21 allows logged-in users for manipulation of generated web pages via injection of HTML code. This might lead to a successful phishing attack for example by tricking users into using a hyperlink pointing to a website controlled by an attacker. Fix for 9.0.20 branch was released in version 9.0.20.238. Fix for 9.0.21 branch was released in version 9.0.21.200.	2024-03-18	4.6	CVE-2024-1606
brefphp -- bref	Bref is an open-source project that helps users go serverless on Amazon Web Services with PHP. When Bref prior to version 2.1.17 is used with the Event-Driven Function runtime and the handler is a `RequestHandlerInterface`, then the Lambda event is converted to a PSR7 object. During the conversion process, if the request is a MultiPart, each part is parsed. In the parsing process, the `Content-Type` header of each part is read using the `Riverline/multipart-parser` library. The library, in the `StreamedPart::parseHeaderContent` function, performs slow multi-byte string operations on the header value. Precisely, the `mb_convert_encoding` function is used with the first (`$string`) and third (`$from_encoding`) parameters read from the header value. An attacker could send specifically crafted requests which would force the server into performing long operations with a consequent long billed	2024-03-22	5.3	CVE-2024-29186

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	duration. The attack has the following requirements and limitations: The Lambda should use the Event-Driven Function runtime and the `RequestHandlerInterface` handler and should implement at least an endpoint accepting POST requests; the attacker can send requests up to 6MB long (this is enough to cause a billed duration between 400ms and 500ms with the default 1024MB RAM Lambda image of Bref); and if the Lambda uses a PHP runtime <= php-82, the impact is higher as the billed duration in the default 1024MB RAM Lambda image of Bref could be brought to more than 900ms for each request. Notice that the vulnerability applies only to headers read from the request body as the request header has a limitation which allows a total maximum size of ~10KB. Version 2.1.17 contains a fix for this issue.			
calameo -- wp_calameo	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Calameo WP Calameo allows Stored XSS.This issue affects WP Calameo: from n/a through 2.1.7.	2024-03-19	6.5	CVE-2024-29098
campcodes -- complete_online_beauty_parlor_management_system	A vulnerability has been found in Campcodes Complete Online Beauty Parlor Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/index.php. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257602 is the identifier assigned to this vulnerability.	2024-03-21	6.3	CVE-2024-2766
campcodes -- complete_online_beauty_parlor_management_system	A vulnerability was found in Campcodes Complete Online Beauty Parlor Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/forgot-password.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257603.	2024-03-21	6.3	CVE-2024-2767
campcodes -- complete_online_beauty_parlor_management_system	A vulnerability was found in Campcodes Complete Online Beauty Parlor Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/edit-services.php. The manipulation of the argument editid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257604.	2024-03-21	6.3	CVE-2024-2768
campcodes -- complete_online_beauty_parlor_management_system	A vulnerability was found in Campcodes Complete Online Beauty Parlor Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/admin-profile.php. The manipulation of the argument adminname leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257605 was assigned to this vulnerability.	2024-03-21	6.3	CVE-2024-2769
campcodes -- complete_online_beauty_parlor_management_system	A vulnerability was found in Campcodes Complete Online Beauty Parlor Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/contact-us.php. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257606 is the identifier assigned to this vulnerability.	2024-03-21	6.3	CVE-2024-2770
campcodes -- complete_online_beauty_parlor_management_system	A vulnerability classified as critical was found in Campcodes Online Marriage Registration System 1.0. This vulnerability affects unknown code of the file /user/search.php. The manipulation of the argument searchdata leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257608.	2024-03-21	6.3	CVE-2024-2774
campcodes -- complete_online_beauty_parlor_ma	A vulnerability, which was classified as critical, was found in Campcodes Online Marriage Registration System 1.0. Affected is an unknown function of the file /admin/search.php. The manipulation of the argument searchdata leads to sql injection. It is possible to launch the attack remotely. The exploit has been	2024-03-22	6.3	CVE-2024-2776

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nagement_system	disclosed to the public and may be used. VDB-257610 is the identifier assigned to this vulnerability.			
campcodes -- complete_online_beauty_parlor_management_system	A vulnerability has been found in Campcodes Online Marriage Registration System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/application-bwdates-reports-details.php. The manipulation of the argument fromdate leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257611.	2024-03-22	6.3	CVE-2024-2777
campcodes -- complete_online_dj_booking_system	A vulnerability, which was classified as critical, has been found in Campcodes Complete Online DJ Booking System 1.0. This issue affects some unknown processing of the file /admin/user-search.php. The manipulation of the argument searchdata leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257465 was assigned to this vulnerability.	2024-03-21	6.3	CVE-2024-2712
campcodes -- complete_online_dj_booking_system	A vulnerability, which was classified as critical, was found in Campcodes Complete Online DJ Booking System 1.0. Affected is an unknown function of the file /admin/booking-search.php. The manipulation of the argument searchdata leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257466 is the identifier assigned to this vulnerability.	2024-03-21	6.3	CVE-2024-2713
campcodes -- complete_online_dj_booking_system	A vulnerability has been found in Campcodes Complete Online DJ Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/booking-bwdates-reports-details.php. The manipulation of the argument fromdate leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257467.	2024-03-20	6.3	CVE-2024-2714
campcodes -- online_job_finder_system	A vulnerability has been found in Campcodes Online Job Finder System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/vacancy/controller.php. The manipulation of the argument id/CATEGORY leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257368.	2024-03-20	6.3	CVE-2024-2668
campcodes -- online_job_finder_system	A vulnerability was found in Campcodes Online Job Finder System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/employee/controller.php of the component GET Parameter Handler. The manipulation of the argument EMPLOYEEID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257369 was assigned to this vulnerability.	2024-03-20	6.3	CVE-2024-2669
campcodes -- online_job_finder_system	A vulnerability was found in Campcodes Online Job Finder System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/vacancy/index.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257370 is the identifier assigned to this vulnerability.	2024-03-20	6.3	CVE-2024-2670
campcodes -- online_job_finder_system	A vulnerability was found in Campcodes Online Job Finder System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/user/index.php. The 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. The associated identifier of this vulnerability is VDB-257371.	2024-03-20	6.3	CVE-2024-2671
campcodes -- online_job_finder_	A vulnerability was found in Campcodes Online Job Finder System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/user/controller.php. The manipulation of the argument UESRID leads to sql	2024-03-20	6.3	CVE-2024-2672

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
system	injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257372.			
campcodes -- online_job_finder_system	A vulnerability classified as critical has been found in Campcodes Online Job Finder System 1.0. This affects an unknown part of the file /admin/login.php. The manipulation of the argument user_email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257373 was assigned to this vulnerability.	2024-03-20	6.3	CVE-2024-2673
campcodes -- online_job_finder_system	A vulnerability classified as critical was found in Campcodes Online Job Finder System 1.0. This vulnerability affects unknown code of the file /admin/employee/index.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. VDB-257374 is the identifier assigned to this vulnerability.	2024-03-20	6.3	CVE-2024-2674
campcodes -- online_job_finder_system	A vulnerability, which was classified as critical, has been found in Campcodes Online Job Finder System 1.0. This issue affects some unknown processing of the file /admin/company/index.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257375.	2024-03-20	6.3	CVE-2024-2675
campcodes -- online_job_finder_system	A vulnerability, which was classified as critical, was found in Campcodes Online Job Finder System 1.0. Affected is an unknown function of the file /admin/company/controller.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257376.	2024-03-20	6.3	CVE-2024-2676
campcodes -- online_job_finder_system	A vulnerability has been found in Campcodes Online Job Finder System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/category/controller.php. The manipulation of the argument CATEGORYID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257377 was assigned to this vulnerability.	2024-03-20	6.3	CVE-2024-2677
campcodes -- online_job_finder_system	A vulnerability was found in Campcodes Online Job Finder System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/applicants/controller.php. The manipulation of the argument JOBREGID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257378 is the identifier assigned to this vulnerability.	2024-03-20	6.3	CVE-2024-2678
campcodes -- online_job_finder_system	A vulnerability was found in Campcodes Online Job Finder System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/applicants/index.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257387.	2024-03-20	6.3	CVE-2024-2687
cegid -- meta4_hr	A Cross-Site Scripting Vulnerability has been found on Meta4 HR affecting version 819.001.022 and earlier. The endpoint '/sitetest/english/dumpenv.jsp' is vulnerable to XSS attack by 'lang' query, i.e. '/sitetest/english/dumpenv.jsp?snoop=yes&lang=%27%3Cimg%20src/onerror=alert(1)%3E&params'.	2024-03-19	6.1	CVE-2024-2633 cve-
cegid -- meta4_hr	A Cross-Site Scripting Vulnerability has been found on Meta4 HR affecting version 819.001.022 and earlier. The endpoint '/sse_generico/generico_login.jsp' is vulnerable to XSS attack via 'lang' query, i.e.	2024-03-19	6.1	CVE-2024-2634 cve-

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	'/sse_generico/generico_login.jsp?lang=%27%3balert(%27BLEUSS%27)%2f%2f&params='.			
ciges -- cigesv2	Stored Cross-Site Scripting (Stored-XSS) vulnerability affecting the CIGESv2 system, allowing an attacker to execute and store malicious javascript code in the application form without prior registration.	2024-03-22	6.1	CVE-2024-2726 cve-
ciges -- cigesv2	HTML injection vulnerability affecting the CIGESv2 system, which allows an attacker to inject arbitrary code and modify elements of the website and email confirmation message.	2024-03-22	6.1	CVE-2024-2727 cve-
ciges -- cigesv2	Information exposure vulnerability in the CIGESv2 system. This vulnerability could allow a local attacker to intercept traffic due to the lack of proper implementation of the TLS protocol.	2024-03-22	4.1	CVE-2024-2728 cve-
cilium -- cilium	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.13.13, 1.14.8, and 1.15.2, in Cilium clusters with IPsec enabled and traffic matching Layer 7 policies, IPsec-eligible traffic between a node's Envoy proxy and pods on other nodes is sent unencrypted and IPsec-eligible traffic between a node's DNS proxy and pods on other nodes is sent unencrypted. This issue has been resolved in Cilium 1.15.2, 1.14.8, and 1.13.13. There is no known workaround for this issue.	2024-03-18	6.1	CVE-2024-28249
cilium -- cilium	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Starting in version 1.14.0 and prior to versions 1.14.8 and 1.15.2, In Cilium clusters with WireGuard enabled and traffic matching Layer 7 policies Wireguard-eligible traffic that is sent between a node's Envoy proxy and pods on other nodes is sent unencrypted and Wireguard-eligible traffic that is sent between a node's DNS proxy and pods on other nodes is sent unencrypted. This issue has been resolved in Cilium 1.14.8 and 1.15.2 in in native routing mode (`routingMode=native`) and in Cilium 1.14.4 in tunneling mode (`routingMode=tunnel`). Not that in tunneling mode, `encryption.wireguard.encapsulate` must be set to `true`. There is no known workaround for this issue.	2024-03-18	6.1	CVE-2024-28250
colorlibplugins -- coming_soon_&_maintenance_mode_by_colorlib	The Coming Soon & Maintenance Mode by Colorlib plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.0.99 via the REST API. This makes it possible for unauthenticated attackers to obtain post and page contents via REST API thus bypassing maintenance mode protection provided by the plugin.	2024-03-20	5.3	CVE-2024-1473
cozmoslabs,_sareiodata -- passwordless_login	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cozmoslabs, sareiodata Passwordless Login passwordless-login allows Stored XSS.This issue affects Passwordless Login: from n/a through 1.1.2.	2024-03-19	6.5	CVE-2024-29143
creativethemeshq -- blocksy_companion	The Blocksy Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Newsletter widget in all versions up to, and including, 2.0.31 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.	2024-03-22	6.5	CVE-2024-2392
crisp -- crisp	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crisp allows Stored XSS.This issue affects Crisp: from n/a through 0.44.	2024-03-21	6.5	CVE-2024-27963
data443 -- tracking_code_ma	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Data443 Tracking Code Manager.This issue affects Tracking Code Manager: from n/a through 2.0.16.	2024-03-21	5.9	CVE-2024-2579

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nager				
dazzlersoft -- coming_soon_under_construction_&_maintenance_mode_by_dazzler	The Coming Soon, Under Construction & Maintenance Mode By Dazzler plugin for WordPress is vulnerable to maintenance mode bypass in all versions up to, and including, 2.1.2. This is due to the plugin relying on the REQUEST_URI to determine if the page being accesses is an admin area. This makes it possible for unauthenticated attackers to bypass maintenance mode and access the site which may be considered confidential when in maintenance mode.	2024-03-20	5.3	CVE-2024-1181
delabon -- live_sales_notification_for_woocommerce_-_woomotiv	The Live Sales Notification for Woocommerce - Woomotiv plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.4.3. This is due to missing or incorrect nonce validation on the 'ajax_cancel_review' function. This makes it possible for unauthenticated attackers to reset the site's review count via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-20	4.3	CVE-2024-1325
dell -- poweredge_platform	Dell PowerEdge Server BIOS contains an Improper SMM communication buffer verification vulnerability. A physical high privileged attacker could potentially exploit this vulnerability leading to arbitrary writes to SMRAM.	2024-03-19	4.4	CVE-2024-25942
delta_electronics -- diaenergie	Improper neutralization of input within the affected product could lead to cross-site scripting.	2024-03-21	4.6	CVE-2024-28045
denoland -- deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Starting in version 1.8.0 and prior to version 1.40.4, Deno improperly checks that an import specifier's hostname is equal to or a child of a token's hostname, which can cause tokens to be sent to servers they shouldn't be sent to. An auth token intended for `example[.]com` may be sent to `notexample[.]com`. Anyone who uses DENO_AUTH_TOKENS and imports potentially untrusted code is affected. Version 1.40.0 contains a patch for this issue	2024-03-21	4.6	CVE-2024-27932
devklan -- alma_blog	Improper access control vulnerability in Devklan's Alma Blog that affects versions 2.1.10 and earlier. This vulnerability could allow an unauthenticated user to access the application's functionalities without the need for credentials.	2024-03-19	6.5	CVE-2024-1144 cve-
devklan -- alma_blog	User enumeration vulnerability in Devklan's Alma Blog that affects versions 2.1.10 and earlier. This vulnerability could allow a remote user to retrieve all valid users registered in the application just by looking at the request response.	2024-03-19	5.3	CVE-2024-1145 cve-
devklan -- alma_blog	Cross-Site Scripting vulnerability in Devklan's Alma Blog that affects versions 2.1.10 and earlier. This vulnerability could allow an attacker to store a malicious JavaScript payload within the application by adding the payload to 'Community Description' or 'Community Rules'.	2024-03-19	5.8	CVE-2024-1146 cve-
diygod -- rsshub	RSSHub is an open source RSS feed generator. Starting in version 1.0.0-master.cbbd829 and prior to version 1.0.0-master.d8ca915, ahen the specially crafted image is supplied to the internal media proxy, it proxies the image without handling XSS vulnerabilities, allowing for the execution of arbitrary JavaScript code. Users who access the deliberately constructed URL are affected. This vulnerability was fixed in version 1.0.0-master.d8ca915. No known workarounds are available.	2024-03-21	6.1	CVE-2024-27926
diygod -- rsshub	RSSHub is an open source RSS feed generator. Prior to version 1.0.0-master.a429472, RSSHub allows remote attackers to use the server as a proxy to send HTTP GET requests to arbitrary targets and retrieve information in the internal network or conduct Denial-of-Service (DoS) attacks. The attacker can send malicious requests to a RSSHub server, to make the server send HTTP GET requests to arbitrary destinations and see partial responses. This may lead to leak the server IP address, which could be hidden behind a CDN; retrieving information in the internal network, e.g. which addresses/ports are accessible, the titles and meta	2024-03-21	6.5	CVE-2024-27927

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	descriptions of HTML pages; and denial of service amplification. The attacker could request the server to download some large files, or chain several SSRF requests in a single attacker request.			
espocrm -- espocrm	EspoCRM is an Open Source Customer Relationship Management software. An attacker can inject arbitrary IP or domain in "Password Change" page and redirect victim to malicious page that could lead to credential stealing or another attack. This vulnerability is fixed in 8.1.2.	2024-03-21	5.9	CVE-2024-24818
five_star_plugins -- five_star_restaurant_menu	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Five Star Plugins Five Star Restaurant Menu allows Stored XSS.This issue affects Five Star Restaurant Menu: from n/a through 2.4.14.	2024-03-19	6.5	CVE-2024-29089
folio -- spring_module_core	A vulnerability was found in Folio Spring Module Core up to 1.1.5. It has been rated as critical. Affected by this issue is the function dropSchema of the file tenant/src/main/java/org/folio/spring/tenant/hibernate/HibernateSchemaService.java of the component Schema Name Handler. The manipulation leads to sql injection. Upgrading to version 2.0.0 is able to address this issue. The name of the patch is d374a5f77e6b58e36f0e0e4419be18b95edcd7ff. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-257516.	2024-03-21	5.5	CVE-2022-4963
foliovision:_making_the_web_work_for_you -- fv_flowplayer_video_player	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Foliovision: Making the web work for you FV Flowplayer Video Player allows Stored XSS.This issue affects FV Flowplayer Video Player: from n/a through 7.5.41.7212.	2024-03-19	6.5	CVE-2024-29122
franciscop -- translate	Translate is a package that allows users to convert text to different languages on Node.js and the browser. Prior to version 3.0.0, an attacker controlling the second variable of the `translate` function is able to perform a cache poisoning attack. They can change the outcome of translation requests made by subsequent users. The `opt.id` parameter allows the overwriting of the cache key. If an attacker sets the `id` variable to the cache key that would be generated by another user, they can choose the response that user gets served. Version 3.0.0 fixes this issue.	2024-03-22	5.3	CVE-2024-29042
fujian_kelixin_communication -- command_and_dispatch_platform	A vulnerability has been found in Fujian Kelixin Communication Command and Dispatch Platform up to 20240318 and classified as critical. Affected by this vulnerability is an unknown functionality of the file api/client/down_file.php. The manipulation of the argument uuid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257197 was assigned to this vulnerability.	2024-03-19	6.3	CVE-2024-2620
fujian_kelixin_communication -- command_and_dispatch_platform	A vulnerability was found in Fujian Kelixin Communication Command and Dispatch Platform up to 20240318 and classified as critical. Affected by this issue is some unknown functionality of the file api/client/user/pwd_update.php. The manipulation of the argument uuid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257198 is the identifier assigned to this vulnerability.	2024-03-19	6.3	CVE-2024-2621
fujian_kelixin_communication -- command_and_dispatch_platform	A vulnerability was found in Fujian Kelixin Communication Command and Dispatch Platform up to 20240318. It has been classified as critical. This affects an unknown part of the file /api/client/editemedia.php. The manipulation of the argument number/enterprise_uuid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257199.	2024-03-19	6.3	CVE-2024-2622
funnelkit -- automation_by_au	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FunnelKit Automation By Autonami allows Stored XSS.This issue affects Automation By Autonami: from n/a through 2.8.2.	2024-03-21	6.5	CVE-2024-2580

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tonami				
geoserver -- geoserver	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. An arbitrary file renaming vulnerability exists in versions prior to 2.23.5 and 2.24.2 that enables an authenticated administrator with permissions to modify stores through the REST Coverage Store or Data Store API to rename arbitrary files and directories with a name that does not end in `.zip`. Store file uploads rename zip files to have a `.zip` extension if it doesn't already have one before unzipping the file. This is fine for file and url upload methods where the files will be in a specific subdirectory of the data directory but, when using the external upload method, this allows arbitrary files and directories to be renamed. Renaming GeoServer files will most likely result in a denial of service, either completely preventing GeoServer from running or effectively deleting specific resources (such as a workspace, layer or style). In some cases, renaming GeoServer files could revert to the default settings for that file which could be relatively harmless like removing contact information or have more serious consequences like allowing users to make OGC requests that the customized settings would have prevented them from making. The impact of renaming non-GeoServer files depends on the specific environment although some sort of denial of service is a likely outcome. Versions 2.23.5 and 2.24.2 contain a fix for this issue.	2024-03-20	6	CVE-2024-23634
geoserver -- geoserver	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.3 and 2.24.0 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in uploaded style/legend resources that will execute in the context of another administrator's browser when viewed in the REST Resources API. Access to the REST Resources API is limited to full administrators by default and granting non-administrators access to this endpoint should be carefully considered as it may allow access to files containing sensitive information. Versions 2.23.3 and 2.24.0 contain a patch for this issue.	2024-03-20	4.8	CVE-2023-51445
geoserver -- geoserver	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.3 and 2.24.0 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in uploaded style/legend resources or in a specially crafted datastore file that will execute in the context of another user's browser when viewed in the Style Publisher. Access to the Style Publisher is available to all users although data security may limit users' ability to trigger the XSS. Versions 2.23.3 and 2.24.0 contain a fix for this issue.	2024-03-20	4.8	CVE-2024-23640
geoserver -- geoserver	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.4 and 2.24.1 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in the GeoServer catalog that will execute in the context of another user's browser when viewed in the WMS GetMap SVG Output Format when the Simple SVG renderer is enabled. Access to the WMS SVG Format is available to all users by default although data and service security may limit users' ability to trigger the XSS. Versions 2.23.4 and 2.24.1 contain a fix for this issue.	2024-03-20	4.8	CVE-2024-23642
geoserver -- geoserver	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.2 and 2.24.1 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in the GeoServer catalog that will execute in the context of another administrator's browser when viewed in the GWC Seed Form. Access to the GWC Seed Form is limited to full administrators by default and granting non-administrators access to	2024-03-20	4.8	CVE-2024-23643

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	this endpoint is not recommended. Versions 2.23.2 and 2.24.1 contain a fix for this issue.			
geoserver -- geoserver	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.3 and 2.24.1 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in the GeoServer catalog that will execute in the context of another user's browser when viewed in the WMS GetMap OpenLayers Output Format. Access to the WMS OpenLayers Format is available to all users by default although data and service security may limit users' ability to trigger the XSS. Versions 2.23.3 and 2.24.1 contain a patch for this issue.	2024-03-20	4.8	CVE-2024-23818
geoserver -- geoserver	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.4 and 2.24.1 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in the GeoServer catalog that will execute in the context of another user's browser when viewed in the MapML HTML Page. The MapML extension must be installed and access to the MapML HTML Page is available to all users although data security may limit users' ability to trigger the XSS. Versions 2.23.4 and 2.24.1 contain a patch for this issue.	2024-03-20	4.8	CVE-2024-23819
geoserver -- geoserver	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.4 and 2.24.1 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in the GeoServer catalog that will execute in the context of another user's browser when viewed in the GWC Demos Page. Access to the GWC Demos Page is available to all users although data security may limit users' ability to trigger the XSS. Versions 2.23.4 and 2.24.1 contain a patch for this issue.	2024-03-20	4.8	CVE-2024-23821
github -- enterprise_server	An Improper Privilege Management vulnerability was identified in GitHub Enterprise Server that allowed an attacker to use the Enterprise Actions GitHub Connect download token to fetch private repository data. An attacker would require an account on the server instance with non-default settings for GitHub Connect. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.8.16, 3.9.11, 3.10.8, and 3.11.6. This vulnerability was reported via the GitHub Bug Bounty program.	2024-03-21	6.3	CVE-2024-1908
github_ -- enterprise_server	A Cross Site Request Forgery vulnerability was identified in GitHub Enterprise Server that allowed an attacker to execute unauthorized actions on behalf of an unsuspecting user. A mitigating factor is that user interaction is required. This vulnerability affected GitHub Enterprise Server 3.12.0 and was fixed in versions 3.12.1. This vulnerability was reported via the GitHub Bug Bounty program.	2024-03-21	4.3	CVE-2024-2748
glpi-project -- glpi	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. An authenticated user can execute a SSRF based attack using Arbitrary Object Instantiation. This issue has been patched in version 10.0.13.	2024-03-18	6.4	CVE-2024-27098
glpi-project -- glpi	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. An authenticated user can access sensitive fields data from items on which he has read access. This issue has been patched in version 10.0.13.	2024-03-18	6.5	CVE-2024-27930
glpi-project -- glpi	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. An authenticated user can obtain the email address of all GLPI users. This issue has been patched in version 10.0.13.	2024-03-18	6.5	CVE-2024-27937

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
glpi-project -- glpi	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. An unauthenticated user can provide a malicious link to a GLPI administrator in order to exploit a reflected XSS vulnerability. The XSS will only trigger if the administrator navigates through the debug bar. This issue has been patched in version 10.0.13.	2024-03-18	5.3	CVE-2024-27914
glpi-project -- glpi	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. A user with rights to create and share dashboards can build a dashboard containing javascript code. Any user that will open this dashboard will be subject to an XSS attack. This issue has been patched in version 10.0.13.	2024-03-18	4.5	CVE-2024-27104
godaddy -- page_builder_gutenberg_blocks_-_coblocks	The Page Builder Gutenberg Blocks - CoBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Icon Widget's in all versions up to, and including, 3.1.6 due to insufficient input sanitization and output escaping on the link value. 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.	2024-03-23	6.4	CVE-2024-1049
gpriday -- page_builder_by_siteorigin	The Page Builder by SiteOrigin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the legacy Image widget in all versions up to, and including, 2.29.6 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.	2024-03-23	6.4	CVE-2024-2202
heyewei -- jfinalcms	A vulnerability has been found in heyewei JFinalCMS 5.0.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/div_data/delete?divId=9 of the component Custom Data Page. The manipulation leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257071.	2024-03-17	4.7	CVE-2024-2568
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 280361.	2024-03-21	6.5	CVE-2024-22352
ibm -- mq	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS and 9.3 CD is vulnerable to a denial-of-service attack due to an error within the MQ clustering logic. IBM X-Force ID: 268066.	2024-03-20	5.3	CVE-2023-45177
ibm -- security_verify_directory	IBM Security Verify Directory 10.0.0 could disclose sensitive server information that could be used in further attacks against the system. IBM X-Force ID: 228437.	2024-03-22	5.3	CVE-2022-32751
ibm -- security_verify_directory	IBM Security Verify Directory 10.0.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 228444.	2024-03-22	4.5	CVE-2022-32753
ibm -- security_verify_directory	IBM Security Verify Directory 10.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 228445.	2024-03-22	4.8	CVE-2022-32754
ibm -- security_verify_governance	IBM Security Verify Governance 10.0.2 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. IBM X-Force ID: 258375.	2024-03-20	5.9	CVE-2023-35888

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- storage_protect_plus_server	The private key for the IBM Storage Protect Plus Server 10.1.0 through 10.1.16 certificate can be disclosed, undermining the security of the certificate. IBM X-Force ID: 285205.	2024-03-21	6.2	CVE-2024-27277
ibm -- storage_protect_plus_server	IBM Storage Protect Plus Server 10.1.0 through 10.1.16 could allow an authenticated user with read-only permissions to add or delete entries from an existing HyperVisor configuration. IBM X-Force ID: 271538.	2024-03-21	4.3	CVE-2023-47715
inc2734 -- smart_custom_fields	The Smart Custom Fields plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the relational_posts_search() function in all versions up to, and including, 4.2.2. This makes it possible for authenticated attackers, with subscrber-level access and above, to retrieve post content that is password protected and/or private.	2024-03-20	4.3	CVE-2024-1995
infosatech -- revivepress_-_keep_your_old_content_evergreen	The RevivePress - Keep your Old Content Evergreen plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on the import_data and copy_data functions in all versions up to, and including, 1.5.6. This makes it possible for authenticated attackers, with subscriber-level access or higher, to overwrite plugin settings and view them.	2024-03-20	4.3	CVE-2024-1844
isaacs -- node-tar	node-tar is a Tar for Node.js. node-tar prior to version 6.2.1 has no limit on the number of sub-folders created in the folder creation process. An attacker who generates a large number of sub-folders can consume memory on the system running node-tar and even crash the Node.js client within few seconds of running it using a path with too many sub-folders inside. Version 6.2.1 fixes this issue by preventing extraction in excessively deep sub-folders.	2024-03-21	6.5	CVE-2024-28863
jan-peter_lambeck_&_3uu -- shariff_wrapper	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jan-Peter Lambeck & 3UU Shariff Wrapper allows Stored XSS.This issue affects Shariff Wrapper: from n/a through 4.6.10.	2024-03-19	6.5	CVE-2024-29109
jean-david_daviet -- download_media	Missing Authorization vulnerability in Jean-David Daviet Download Media.This issue affects Download Media: from n/a through 1.4.2.	2024-03-21	4.3	CVE-2024-27190
jegtheme -- jeg_elementor_kit	The Jeg Elementor Kit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via HTML Tag attributes in all versions up to, and including, 2.6.2 due to insufficient input sanitization and output escaping. 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.	2024-03-21	6.4	CVE-2024-1326
jegtheme -- jeg_elementor_kit	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jegtheme Jeg Elementor Kit allows Stored XSS.This issue affects Jeg Elementor Kit: from n/a through 2.6.2.	2024-03-19	6.5	CVE-2024-29101
jetbrains -- teamcity	In JetBrains TeamCity before 2023.11 users with access to the agent machine might obtain permissions of the user running the agent process	2024-03-21	4.2	CVE-2024-29880
jhpyle -- docassemble	Docassemble is an expert system for guided interviews and document assembly. Prior to 1.4.97, a user could type HTML into a field, including the field for the user's name, and then that HTML could be displayed on the screen as HTML. The vulnerability has been patched in version 1.4.97 of the master branch.	2024-03-21	6.1	CVE-2024-27290
jhpyle -- docassemble	Docassemble is an expert system for guided interviews and document assembly. Prior to 1.4.97, it is possible to create a URL that acts as an open redirect. The vulnerability has been patched in version 1.4.97 of the master branch.	2024-03-21	6.1	CVE-2024-27291

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jp2112 -- standout_color_boxes_and_buttons	The Standout Color Boxes and Buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'color-button' shortcode in all versions up to, and including, 0.7.0 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.	2024-03-20	6.4	CVE-2024-2474
kilbot -- woocommerce_pos	The WooCommerce POS plugin for WordPress is vulnerable to information disclosure in all versions up to, and including, 1.4.11. This is due to the plugin not properly verifying the authentication and authorization of the current user This makes it possible for authenticated attackers, with customer-level access and above, to view potentially sensitive information about other users by leveraging their order id	2024-03-20	4.3	CVE-2024-2384
kishor-23 -- food_waste_management_system	A vulnerability was found in kishor-23 Food Waste Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/admin.php. The manipulation leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257056. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-17	5.3	CVE-2024-2557
lakernote -- easyadmin	A vulnerability classified as critical has been found in lakernote EasyAdmin up to 20240315. This affects an unknown part of the file /ureport/designer/saveReportFile. The manipulation of the argument file leads to path traversal: '../filedir'. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257715.	2024-03-22	6.3	CVE-2024-2825
lakernote -- easyadmin	A vulnerability classified as problematic was found in lakernote EasyAdmin up to 20240315. This vulnerability affects unknown code of the file /ureport/designer/saveReportFile. The manipulation leads to xml external entity reference. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257716.	2024-03-22	6.3	CVE-2024-2826
lakernote -- easyadmin	A vulnerability, which was classified as critical, has been found in lakernote EasyAdmin up to 20240315. This issue affects some unknown processing of the file /ureport/designer/saveReportFile. The manipulation leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257717 was assigned to this vulnerability.	2024-03-22	6.3	CVE-2024-2827
lakernote -- easyadmin	A vulnerability, which was classified as critical, was found in lakernote EasyAdmin up to 20240315. Affected is the function thumbnail of the file src/main/java/com/laker/admin/module/sys/controller/IndexController.java. The manipulation of the argument url leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The patch is identified as 23165d8cb569048c531150f194fea39f8800b8d5. It is recommended to apply a patch to fix this issue. VDB-257718 is the identifier assigned to this vulnerability.	2024-03-22	6.3	CVE-2024-2828
latchset -- jwcrypto	JWCrypto implements JWK, JWS, and JWE specifications using python-cryptography. Prior to version 1.5.6, an attacker can cause a denial of service attack by passing in a malicious JWE Token with a high compression ratio. When the server processes this token, it will consume a lot of memory and processing time. Version 1.5.6 fixes this vulnerability by limiting the maximum token length.	2024-03-21	6.8	CVE-2024-28102
leap13 -- premium_addons_for_elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Leap13 Premium Addons for Elementor allows Stored XSS.This issue affects Premium Addons for Elementor: from n/a through 4.10.16.	2024-03-19	6.5	CVE-2024-29106

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
leevio -- happy_addons_for_elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Leevio Happy Addons for Elementor allows Stored XSS.This issue affects Happy Addons for Elementor: from n/a through 3.10.1.	2024-03-19	6.5	CVE-2024-29108
liquidpoll -- liquidpoll_-_polls,_surveys,_nps_and_feedback_reviews	The LiquidPoll - Polls, Surveys, NPS and Feedback Reviews plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.3.76 via the poller_list shortcode. This makes it possible for authenticated attackers, with contributor-level access and above, to extract information from polls that may be private.	2024-03-22	4.3	CVE-2024-2080
magenet -- website_article_monetization_by_magenet	The Website Article Monetization By MageNet plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'abp_auth_key' parameter in all versions up to, and including, 1.0.11 due to insufficient input sanitization and output escaping and a missing authorization check. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-20	6.1	CVE-2024-1379
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability, which was classified as critical, was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. This affects an unknown part of the file /admin/users.php. The manipulation of the argument user_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. The associated identifier of this vulnerability is VDB-256971. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-17	6.3	CVE-2024-2534
matt_manning -- mjm_clinic	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Matt Manning MJM Clinic.This issue affects MJM Clinic: from n/a through 1.1.22.	2024-03-19	6.5	CVE-2024-29096
matt_manning -- mjm_clinic	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Matt Manning MJM Clinic allows Stored XSS.This issue affects MJM Clinic: from n/a through 1.1.22.	2024-03-19	5.9	CVE-2024-29140
matthias-wandel -- jhead	A vulnerability was found in Matthias-Wandel jhead 3.08 and classified as critical. This issue affects the function PrintFormatNumber of the file exif.c. The manipulation leads to heap-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257711.	2024-03-22	6.3	CVE-2024-2824
mbis -- permalink_manager_pro	The Permalink Manager Lite plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ajax_save_permalink' function in all versions up to, and including, 2.4.3.1. This makes it possible for authenticated attackers, with author access and above, to modify the permalinks of arbitrary posts.	2024-03-20	5.4	CVE-2024-2538
melapress -- wp_2fa	Improper Authentication vulnerability in Melapress WP 2FA allows Authentication Bypass.This issue affects WP 2FA: from n/a through 2.2.0.	2024-03-21	5.3	CVE-2022-44595
microsoft -- microsoft_edge_(chromium-based)	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2024-03-22	4.7	CVE-2024-26247
microsoft -- microsoft_edge_(chromium-based)	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-03-22	4.3	CVE-2024-29057

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- microsoft_edge_for_android	Microsoft Edge for Android (Chromium-based) Information Disclosure Vulnerability	2024-03-21	4.3	CVE-2024-26196
moby -- moby	Moby is an open source container framework that is a key component of Docker Engine, Docker Desktop, and other distributions of container tooling or runtimes. Moby's networking implementation allows for many networks, each with their own IP address range and gateway, to be defined. This feature is frequently referred to as custom networks, as each network can have a different driver, set of parameters and thus behaviors. When creating a network, the `--internal` flag is used to designate a network as _internal_. The `internal` attribute in a docker-compose.yml file may also be used to mark a network _internal_, and other API clients may specify the `internal` parameter as well. When containers with networking are created, they are assigned unique network interfaces and IP addresses. The host serves as a router for non-internal networks, with a gateway IP that provides SNAT/DNAT to/from container IPs. Containers on an internal network may communicate between each other, but are precluded from communicating with any networks the host has access to (LAN or WAN) as no default route is configured, and firewall rules are set up to drop all outgoing traffic. Communication with the gateway IP address (and thus appropriately configured host services) is possible, and the host may communicate with any container IP directly. In addition to configuring the Linux kernel's various networking features to enable container networking, `dockerd` directly provides some services to container networks. Principal among these is serving as a resolver, enabling service discovery, and resolution of names from an upstream resolver. When a DNS request for a name that does not correspond to a container is received, the request is forwarded to the configured upstream resolver. This request is made from the container's network namespace: the level of access and routing of traffic is the same as if the request was made by the container itself. As a consequence of this design, containers solely attached to an internal network will be unable to resolve names using the upstream resolver, as the container itself is unable to communicate with that nameserver. Only the names of containers also attached to the internal network are able to be resolved. Many systems run a local forwarding DNS resolver. As the host and any containers have separate loopback devices, a consequence of the design described above is that containers are unable to resolve names from the host's configured resolver, as they cannot reach these addresses on the host loopback device. To bridge this gap, and to allow containers to properly resolve names even when a local forwarding resolver is used on a loopback address, `dockerd` detects this scenario and instead forward DNS requests from the host namework namespace. The loopback resolver then forwards the requests to its configured upstream resolvers, as expected. Because `dockerd` forwards DNS requests to the host loopback device, bypassing the container network namespace's normal routing semantics entirely, internal networks can unexpectedly forward DNS requests to an external nameserver. By registering a domain for which they control the authoritative nameservers, an attacker could arrange for a compromised container to exfiltrate data by encoding it in DNS queries that will eventually be answered by their nameservers. Docker Desktop is not affected, as Docker Desktop always runs an internal resolver on a RFC 1918 address. Moby releases 26.0.0, 25.0.4, and 23.0.11 are patched to prevent forwarding any DNS requests from internal networks. As a workaround, run containers intended to be solely attached to internal networks with a custom upstream address, which will force all upstream DNS queries to be resolved from the container's network namespace.	2024-03-20	5.9	CVE-2024-29018
moveaddons -- move_addons_for_elementor	The Move Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's infobox and button widget in all versions up to, and including, 1.2.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with	2024-03-23	6.4	CVE-2024-2131

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
n-media -- frontend_file_manager	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in N-Media Frontend File Manager.This issue affects Frontend File Manager: from n/a through 22.7.	2024-03-17	5.3	CVE-2024-25903
n/a -- 74cms	A vulnerability, which was classified as critical, has been found in 74CMS 3.28.0. Affected by this issue is the function sendCompanyLogo of the file /controller/company/Index.php#sendCompanyLogo of the component Company Logo Handler. The manipulation of the argument imgBase64 leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257060.	2024-03-17	6.3	CVE-2024-2561
n/a -- black	Versions of the package black before 24.3.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the lines_with_leading_tabs_expanded function in the strings.py file. An attacker could exploit this vulnerability by crafting a malicious input that causes a denial of service. Exploiting this vulnerability is possible when running Black on untrusted input, or if you habitually put thousands of leading tab characters in your docstrings.	2024-03-19	5.3	CVE-2024-21503
n/a -- dedecms	A vulnerability classified as problematic was found in DedeCMS 5.7. Affected by this vulnerability is an unknown functionality of the file /src/dede/baidunews.php. The manipulation of the argument filename leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257707. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	4.3	CVE-2024-2820
n/a -- dedecms	A vulnerability, which was classified as problematic, has been found in DedeCMS 5.7. Affected by this issue is some unknown functionality of the file /src/dede/friendlink_edit.php. The manipulation of the argument id leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257708. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	4.3	CVE-2024-2821
n/a -- dedecms	A vulnerability, which was classified as problematic, was found in DedeCMS 5.7. This affects an unknown part of the file /src/dede/vote_edit.php. The manipulation of the argument aid leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257709 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	4.3	CVE-2024-2822
n/a -- dedecms	A vulnerability has been found in DedeCMS 5.7 and classified as problematic. This vulnerability affects unknown code of the file /src/dede/mda_main.php. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257710 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	4.3	CVE-2024-2823
n/a -- gnutls	A flaw was found in GnuTLS. The Minerva attack is a cryptographic vulnerability that exploits deterministic behavior in systems like GnuTLS, leading to side-channel leaks. In specific scenarios, such as when using the GNUTLS_PRIVKEY_FLAG_REPRODUCIBLE flag, it can result in a noticeable step in nonce size from 513 to 512 bits, exposing a potential timing side-channel.	2024-03-21	5.3	CVE-2024-28834
n/a -- gnutls	A flaw has been discovered in GnuTLS where an application crash can be induced when attempting to verify a specially crafted .pem bundle using the "certtool --verify-chain" command.	2024-03-21	5	CVE-2024-28835

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a -- iperf	A flaw was found in iperf, a utility for testing network performance using TCP, UDP, and SCTP. A malicious or malfunctioning client can send less than the expected amount of data to the iperf server, which can cause the server to hang indefinitely waiting for the remainder or until the connection gets closed. This will prevent other connections to the server, leading to a denial of service.	2024-03-18	5.3	CVE-2023-7250
n/a -- libvirt	A flaw was found in the RPC library APIs of libvirt. The RPC server deserialization code allocates memory for arrays before the non-negative length check is performed by the C API entry points. Passing a negative length to the g_new0 function results in a crash due to the negative length being treated as a huge positive number. This flaw allows a local, unprivileged user to perform a denial of service attack by causing the libvirt daemon to crash.	2024-03-21	6.2	CVE-2024-2494
n/a -- libvirt	A NULL pointer dereference flaw was found in the udevConnectListAllInterfaces() function in libvirt. This issue can occur when detaching a host interface while at the same time collecting the list of interfaces via virConnectListAllInterfaces API. This flaw could be used to perform a denial of service attack by causing the libvirt daemon to crash.	2024-03-18	5	CVE-2024-2496
n/a -- livewire/livewire	Versions of the package livewire/livewire from 3.3.5 and before 3.4.9 are vulnerable to Cross-site Scripting (XSS) when a page uses [Url] for a property. An attacker can inject HTML code in the context of the user's browser session by crafting a malicious link and convincing the user to click on it.	2024-03-19	6.1	CVE-2024-21504
n/a -- osbuild-composer	A flaw was found in osbuild-composer. A condition can be triggered that disables GPG verification for package repositories, which can expose the build phase to a Man-in-the-Middle attack, allowing untrusted code to be installed into an image being built.	2024-03-19	6.1	CVE-2024-2307
n/a -- zhicms	A vulnerability, which was classified as critical, has been found in ZhiCms 4.0. This issue affects the function getindexdata of the file app/index/controller/mcontroller.php. The manipulation of the argument key leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-255269 was assigned to this vulnerability.	2024-03-21	6.3	CVE-2024-2015
n/a -- zhicms	A vulnerability, which was classified as critical, was found in ZhiCms 4.0. Affected is the function index of the file app/manage/controller/setcontroller.php. The manipulation of the argument sitename leads to code injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-255270 is the identifier assigned to this vulnerability.	2024-03-21	6.3	CVE-2024-2016
nasirahmed -- advanced_form_integration_-_connect_woocommerce_and_contact_form_7_to_google_sheets_and_other_platforms	The Advanced Form Integration - Connect WooCommerce and Contact Form 7 to Google Sheets and other platforms plugin for WordPress is vulnerable to SQL Injection via the 'integration_id' parameter in all versions up to, and including, 1.82.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries and subsequently 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.	2024-03-20	6.1	CVE-2024-2387
netentsec -- ns-asg_application_security_gateway	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been rated as critical. Affected by this issue is some unknown functionality of the file /protocol/firewall/addfirewall.php. The manipulation of the argument FireWallTableArray leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257282 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-19	6.3	CVE-2024-2644
netentsec -- ns-asg_application_se	A vulnerability classified as critical was found in Netentsec NS-ASG Application Security Gateway 6.3. This vulnerability affects unknown code of the file	2024-03-19	6.3	CVE-2024-2646

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
curity_gateway	/vpnweb/index.php?para=index. The manipulation of the argument check_VirtualSiteId leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257284. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
netentsec -- ns-asg_application_security_gateway	A vulnerability has been found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /protocol/iscdevicestatus/deleteonlineuser.php. The manipulation of the argument messagecontent leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257287. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-20	6.3	CVE-2024-2649
netentsec -- ns-asg_application_security_gateway	A vulnerability classified as problematic has been found in Netentsec NS-ASG Application Security Gateway 6.3. This affects an unknown part of the file /vpnweb/resetpwd/resetpwd.php. The manipulation of the argument UserId leads to improper neutralization of data within xpath expressions. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257283. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-19	4.3	CVE-2024-2645
netentsec -- ns-asg_application_security_gateway	A vulnerability, which was classified as problematic, was found in Netentsec NS-ASG Application Security Gateway 6.3. Affected is an unknown function of the file /nac/naccheck.php. The manipulation of the argument username leads to improper neutralization of data within xpath expressions. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257286 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-19	4.3	CVE-2024-2648
octoprint -- octoprint	OctoPrint provides a web interface for controlling consumer 3D printers. OctoPrint versions up until and including 1.9.3 contain a vulnerability that allows malicious admins to configure or talk a victim with administrator rights into configuring a webcam snapshot URL which when tested through the "Test" button included in the web interface will execute JavaScript code in the victims browser when attempting to render the snapshot image. An attacker who successfully talked a victim with admin rights into performing a snapshot test with such a crafted URL could use this to retrieve or modify sensitive configuration settings, interrupt prints or otherwise interact with the OctoPrint instance in a malicious way. The vulnerability is patched in version 1.10.0rc3. OctoPrint administrators are strongly advised to thoroughly vet who has admin access to their installation and what settings they modify based on instructions by strangers.	2024-03-18	4	CVE-2024-28237
openbmb -- xagent	A vulnerability was found in OpenBMB XAgent 1.0.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Privileged Mode. The manipulation leads to sandbox issue. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-255265 was assigned to this vulnerability.	2024-03-21	5.3	CVE-2024-2007
opentext -- service_management_automation_x_(smax)	Insufficient Granularity of Access Control vulnerability in OpenText™ Service Management Automation X (SMAX), OpenText™ Asset Management X (AMX) allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11; and Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11.	2024-03-19	6.5	CVE-2023-32259
opentext -- service_management_automation_x_(smax)	Misinterpretation of Input vulnerability in OpenText™ Service Management Automation X (SMAX), OpenText™ Asset Management X (AMX), and OpenText™ Hybrid Cloud Management X (HCMX) products. The vulnerability could allow Input data manipulation.This issue affects Service Management Automation X (SMAX) versions: 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05,	2024-03-19	6.5	CVE-2023-32260

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2022.11, 2023.05; Asset Management X (AMX) versions: 2021.08, 2021.11, 2022.05, 2022.11, 2023.05; and Hybrid Cloud Management X (HCMX) versions: 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11, 2023.05.			
openzeppelin -- openzeppelin-contracts	OpenZeppelin Contracts is a library for secure smart contract development. The `Base64.encode` function encodes a `bytes` input by iterating over it in chunks of 3 bytes. When this input is not a multiple of 3, the last iteration may read parts of the memory that are beyond the input buffer. The vulnerability is fixed in 5.0.2 and 4.9.6.	2024-03-21	6.5	CVE-2024-27094
osamaesh -- wp_visitor_statistics_(real_time_traffic)	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Osamaesh WP Visitor Statistics (Real Time Traffic).This issue affects WP Visitor Statistics (Real Time Traffic): from n/a through 6.9.4.	2024-03-17	5.3	CVE-2024-24867
pandaxgo -- pandax	A vulnerability, which was classified as critical, was found in PandaXGO PandaX up to 20240310. This affects the function InsertRole of the file /apps/system/services/role_menu.go. The manipulation of the argument roleKey leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257061 was assigned to this vulnerability.	2024-03-17	6.3	CVE-2024-2562
pandaxgo -- pandax	A vulnerability was found in PandaXGO PandaX up to 20240310 and classified as critical. This issue affects the function ExportUser of the file /apps/system/api/user.go. The manipulation of the argument filename leads to path traversal: '../filedir'. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257063.	2024-03-17	6.3	CVE-2024-2564
pandaxgo -- pandax	A vulnerability was found in PandaXGO PandaX up to 20240310. It has been classified as critical. Affected is an unknown function of the file /apps/system/router/upload.go of the component File Extension Handler. The manipulation of the argument file leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257064.	2024-03-17	6.3	CVE-2024-2565
pandaxgo -- pandax	A vulnerability has been found in PandaXGO PandaX up to 20240310 and classified as critical. This vulnerability affects the function DeleteImage of the file /apps/system/router/upload.go. The manipulation of the argument fileName with the input ../../../../../../../../../tmp/1.txt leads to path traversal: '../filedir'. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257062 is the identifier assigned to this vulnerability.	2024-03-17	5.4	CVE-2024-2563
pandora_fms -- pandora_fms	: Path Traversal vulnerability in Pandora FMS on all allows Path Traversal. This vulnerability allowed changing directories and creating files and downloading them outside the allowed directories. This issue affects Pandora FMS: from 700 through <776.	2024-03-19	6.7	CVE-2023-41793
pandora_fms -- pandora_fms	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pandora FMS on all allows CVE-2008-5817. This vulnerability allowed SQL changes to be made to several files in the Grafana module. This issue affects Pandora FMS: from 700 through <776.	2024-03-19	6.8	CVE-2023-44090
paul_ryley -- site_reviews	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Paul Ryley Site Reviews allows Stored XSS.This issue affects Site Reviews: from n/a through 6.11.6.	2024-03-19	5.9	CVE-2024-29095

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pdf_embedder -- pdf_embedder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PDF Embedder allows Stored XSS.This issue affects PDF Embedder: from n/a through 4.6.4.	2024-03-19	6.5	CVE-2024-29141
pepro_dev._group -- peprodev_ultimate_invoice	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Pepro Dev. Group PeproDev Ultimate Invoice.This issue affects PeproDev Ultimate Invoice: from n/a through 1.9.7.	2024-03-17	5.3	CVE-2024-25933
pickplugins -- user_profile	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PickPlugins User profile allows Stored XSS.This issue affects User profile: from n/a through 2.0.20.	2024-03-19	6.3	CVE-2024-29097
progress_software -- moveit_transfer	In Progress MOVEit Transfer versions released before 2022.0.11 (14.0.11), 2022.1.12 (14.1.12), 2023.0.9 (15.0.9), 2023.1.4 (15.1.4), a logging bypass vulnerability has been discovered. An authenticated user could manipulate a request to bypass the logging mechanism within the web application which results in user activity not being logged properly.	2024-03-20	4.3	CVE-2024-2291
python_software_foundation -- cpython	An issue was found in the CPython `zipfile` module affecting versions 3.12.2, 3.11.8, 3.10.13, 3.9.18, and 3.8.18 and prior. The zipfile module is vulnerable to "quoted-overlap" zip-bombs which exploit the zip format to create a zip-bomb with a high compression ratio. The fixed versions of CPython makes the zipfile module reject zip archives which overlap entries in the archive.	2024-03-19	6.2	CVE-2024-0450
qiskit -- qiskit-ibm-runtime	Qiskit IBM Runtime is an environment that streamlines quantum computations and provides optimal implementations of the Qiskit quantum computing SDK. Starting in version 0.1.0 and prior to version 0.21.2, deserializing json data using `qiskit_ibm_runtime.RuntimeDecoder` can lead to arbitrary code execution given a correctly formatted input string. Version 0.21.2 contains a fix for this issue.	2024-03-20	5.3	CVE-2024-29032
railmedia -- order_tip_for_woocommerce	The Order Tip for WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the export_tips_to_csv() function in all versions up to, and including, 1.3.1. This makes it possible for unauthenticated attackers to export the plugin's order fees.	2024-03-20	5.3	CVE-2024-1119
realmag777 -- bear	Missing Authorization vulnerability in realmag777 BEAR.This issue affects BEAR: from n/a through 1.1.4.	2024-03-23	4.3	CVE-2024-24835
remyb92 -- translate_wordpress_and_go_multilingual_-_weglot	The Translate WordPress and go Multilingual - Weglot plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widget/block in all versions up to, and including, 4.2.5 due to insufficient input sanitization and output escaping on user supplied attributes such as 'className'. 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.	2024-03-20	6.4	CVE-2024-2124
repute_infosystems -- armember_-_membership_plugin_content_restriction_member_levels_user_profile_&_user_signup	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Repute Infosystems ARMember - Membership Plugin, Content Restriction, Member Levels, User Profile & User signup allows Stored XSS.This issue affects ARMember - Membership Plugin, Content Restriction, Member Levels, User Profile & User signup: from n/a through 4.0.23.	2024-03-21	5.9	CVE-2024-27995

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rewardsfuel -- contests_by_rewards_fuel	The Contests by Rewards Fuel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'update_rewards_fuel_api_key' parameter in all versions up to, and including, 2.0.64 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.	2024-03-20	6.4	CVE-2024-1787
rewardsfuel -- contests_by_rewards_fuel	The Contests by Rewards Fuel plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.62. This is due to missing or incorrect nonce validation on the ajax_handler() function. This makes it possible for unauthenticated attackers to update the plugin's settings and inject malicious JavaScript via a forged request granted they can trick a site's user with the edit_posts capability into performing an action such as clicking on a link.	2024-03-20	5.4	CVE-2024-1785
rubengc -- gamipress_-_button	The GamiPress - Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'gamipress_button' shortcode in all versions up to, and including, 1.0.7 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.	2024-03-20	6.4	CVE-2024-2460
ruijie -- rg-nbs2009g-p	A vulnerability was found in Ruijie RG-NBS2009G-P up to 20240305. It has been classified as critical. Affected is an unknown function of the file /system/passwdManage.htm of the component Password Handler. The manipulation leads to improper authorization. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257280. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-19	5.3	CVE-2024-2641
saleor -- storefront	Saleor Storefront is software for building e-commerce experiences. Prior to commit 579241e75a5eb332ccf26e0bcdd54befa33f4783, when any user authenticates in the storefront, anonymous users are able to access their data. The session is leaked through cache and can be accessed by anyone. Users should upgrade to a version that incorporates commit 579241e75a5eb332ccf26e0bcdd54befa33f4783 or later to receive a patch. A possible workaround is to temporarily disable authentication by changing the usage of `createSaleorAuthClient()`.	2024-03-20	4.3	CVE-2024-29036
save_as_pdf_plugin_by_pdfcrowd -- word_replacer_pro	Missing Authorization vulnerability in Save as PDF plugin by Pdfcrowd Word Replacer Pro.This issue affects Word Replacer Pro: from n/a through 1.0.	2024-03-20	6.5	CVE-2023-52229
scrollsequence -- scrollsequence	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Scrollsequence allows Stored XSS.This issue affects Scrollsequence: from n/a through 1.5.4.	2024-03-19	6.5	CVE-2024-29118
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 plugin's 'efb_likebox' shortcode in all versions up to, and including, 6.5.4 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.	2024-03-21	6.4	CVE-2024-1278
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 Cross-Site Request Forgery in all versions up to, and including, 6.5.4. This is due to missing or incorrect nonce validation on the esf_insta_save_access_token and efbl_save_facebook_access_token functions. This makes it possible for unauthenticated attackers to connect their facebook and instagram pages to the site via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-21	5.4	CVE-2024-1213

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
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 Cross-Site Request Forgery in all versions up to, and including, 6.5.4. This is due to missing or incorrect nonce validation on the save_groups_list function. This makes it possible for unauthenticated attackers to disconnect a site's facebook or instagram page/group connection via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-21	4.3	CVE-2024-1214
sonatype -- iq_server	Path Traversal in Sonatype IQ Server from version 143 allows remote authenticated attackers to overwrite or delete files via a specially crafted request. Version 171 fixes this issue.	2024-03-21	5.4	CVE-2024-1142
sourcecodester -- complete_e-commerce_site	A vulnerability classified as critical has been found in SourceCodester Complete E-Commerce Site 1.0. Affected is an unknown function of the file /admin/users_photo.php. The manipulation of the argument photo leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257544.	2024-03-21	4.7	CVE-2024-2754
sourcecodester -- employee_task_management_system	A vulnerability has been found in SourceCodester Employee Task Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file update-employee.php. The manipulation of the argument admin_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257053 was assigned to this vulnerability.	2024-03-17	6.3	CVE-2024-2554
sourcecodester -- employee_task_management_system	A vulnerability was found in SourceCodester Employee Task Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file update-admin.php. The manipulation of the argument admin_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257054 is the identifier assigned to this vulnerability.	2024-03-17	6.3	CVE-2024-2555
sourcecodester -- employee_task_management_system	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been classified as critical. This affects an unknown part of the file attendance-info.php. The manipulation of the argument user_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. The associated identifier of this vulnerability is VDB-257055.	2024-03-17	6.3	CVE-2024-2556
sourcecodester -- file_manager_app	A vulnerability was found in SourceCodester File Manager App 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /endpoint/update-file.php. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257182 is the identifier assigned to this vulnerability.	2024-03-18	6.3	CVE-2024-2604
sourcecodester -- online_discussion_forum_site	A vulnerability was found in SourceCodester Online Discussion Forum Site 1.0. It has been classified as critical. Affected is an unknown function of the file /uupdate.php. The manipulation of the argument ima leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257388.	2024-03-20	6.3	CVE-2024-2690
sourcecodester -- simple_file_manager	A vulnerability classified as critical was found in SourceCodester Simple File Manager 1.0. This vulnerability affects unknown code. The manipulation of the argument photo leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257770 is the identifier assigned to this vulnerability.	2024-03-23	6.3	CVE-2024-2849
spring -- spring	Spring Authorization Server versions 1.0.0 - 1.0.5, 1.1.0 - 1.1.5, 1.2.0 - 1.2.2 and older unsupported versions are susceptible to a PKCE Downgrade Attack for Confidential Clients. Specifically, an application is vulnerable when a Confidential	2024-03-20	6.1	CVE-2024-22258

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Client uses PKCE for the Authorization Code Grant. An application is not vulnerable when a Public Client uses PKCE for the Authorization Code Grant.			
supercleanse -- pretty_links_-_affiliate_links_link_branding_link_tracking_&_marketing_plugin	The Pretty Links - Affiliate Links, Link Branding, Link Tracking & Marketing Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.6.3. This is due to missing or incorrect nonce validation when saving plugin settings. This makes it possible for unauthenticated attackers to change the plugin's configuration including stripe integration via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-23	4.3	CVE-2024-2326
survey_maker_team -- survey_maker	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Survey Maker team Survey Maker allows Stored XSS.This issue affects Survey Maker: from n/a through 4.0.5.	2024-03-19	5.9	CVE-2024-27996
tenda -- ac10u	A vulnerability has been found in Tenda AC10U 15.03.06.49 and classified as critical. This vulnerability affects the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257458 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-20	6.3	CVE-2024-2707
tenda -- ac15	A vulnerability was found in Tenda AC15 15.03.05.18/15.03.20_multi. It has been classified as critical. This affects the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257667. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	6.3	CVE-2024-2812
tenda -- ac15	A vulnerability classified as problematic was found in Tenda AC15 15.03.05.18. Affected by this vulnerability is the function fromSysToolReboot of the file /goform/SysToolReboot. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257671. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	4.3	CVE-2024-2816
tenda -- ac15	A vulnerability, which was classified as problematic, has been found in Tenda AC15 15.03.05.18. Affected by this issue is the function fromSysToolRestoreSet of the file /goform/SysToolRestoreSet. The manipulation leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257672. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-22	4.3	CVE-2024-2817
tenda -- ac18	A vulnerability classified as problematic has been found in Tenda AC18 15.03.05.05. Affected is the function fromSysToolReboot of the file /goform/SysToolReboot. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257058 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-17	4.3	CVE-2024-2559
tenda -- ac18	A vulnerability classified as problematic was found in Tenda AC18 15.03.05.05. Affected by this vulnerability is the function fromSysToolRestoreSet of the file /goform/SysToolRestoreSet. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257059. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-17	4.3	CVE-2024-2560

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
themefic -- tourfic	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themefic Tourfic allows Stored XSS.This issue affects Tourfic: from n/a through 2.11.8.	2024-03-19	6.5	CVE-2024-29134
themegrill -- colormag	The ColorMag theme for WordPress is vulnerable to Stored Cross-Site Scripting via a user's Display Name in all versions up to, and including, 3.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authentciated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-22	6.4	CVE-2024-2500
themelocation -- custom_woocommerce_checkout_fields_editor	The Custom WooCommerce Checkout Fields Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the save_wcfe_options function in all versions up to, and including, 1.3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-23	6.4	CVE-2024-1697
themeum -- tutor_lms_-_elearning_and_online_course_solution	The Tutor LMS - eLearning and online course solution plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the tutor_delete_announcement() function in all versions up to, and including, 2.6.1. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary posts.	2024-03-21	5.4	CVE-2024-1502
themeum -- tutor_lms_-_elearning_and_online_course_solution	The Tutor LMS - eLearning and online course solution plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.6.1. This is due to missing or incorrect nonce validation on the erase_tutor_data() function. This makes it possible for unauthenticated attackers to deactivate the plugin and erase all data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This requires the "Erase upon uninstallation" option to be enabled.	2024-03-21	4.3	CVE-2024-1503
timersys -- wp_popups	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Timersys WP Popups allows Stored XSS.This issue affects WP Popups: from n/a through 2.1.5.5.	2024-03-19	5.9	CVE-2024-29105
tobias_conrad -- builder_for_woocommerce_reviews_shortcodes_-_reviewshort	Cross-Site Request Forgery (CSRF) vulnerability in Tobias Conrad Builder for WooCommerce reviews shortcodes - ReviewShort.This issue affects Builder for WooCommerce reviews shortcodes - ReviewShort: from n/a through 1.01.3.	2024-03-19	4.3	CVE-2024-29093
visualcomposer -- visual_composer_website_builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Visualcomposer Visual Composer Website Builder allows Stored XSS.This issue affects Visual Composer Website Builder: from n/a through 45.6.0.	2024-03-19	5.9	CVE-2024-27997
w3_eden_inc -- download_manager	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in W3 Eden, Inc. Download Manager allows Stored XSS.This issue affects Download Manager: from n/a through 3.2.84.	2024-03-19	6.5	CVE-2024-29114
webtoffee -- woocommerce_pdf_invoices_packing_slips_delivery_notes_and_shipping_labels	The WooCommerce PDF Invoices, Packing Slips, Delivery Notes and Shipping Labels plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Customer Notes field in all versions up to, and including, 4.4.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected invoice for printing.	2024-03-22	6.1	CVE-2024-0957

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
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 1.6.	2024-03-19	6.5	CVE-2024-29111
wp_marketing_robot -- woocommerce_google_feed_manager	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Marketing Robot WooCommerce Google Feed Manager allows Stored XSS.This issue affects WooCommerce Google Feed Manager: from n/a through 2.2.0.	2024-03-19	5.9	CVE-2024-29112
wpbits -- wpbits_addons_for_elementor_page_builder	The WPBITS Addons For Elementor Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's heading widget in all versions up to, and including, 1.3.4.2 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 arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-20	6.4	CVE-2024-2129
wpcoder -- wp_coder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPCoder WP Coder allows Stored XSS.This issue affects WP Coder: from n/a through 3.5.	2024-03-21	5.9	CVE-2024-2578
wpdevteam -- embedpress_-_embed_pdf_google_docs_vimeo_wistia_embed_youtube_videos_audios_maps_&_embed_any_documents_in_gutenberg_&_elementor	The EmbedPress - Embed PDF, Google Docs, Vimeo, Wistia, Embed YouTube Videos, Audios, Maps & Embed Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the EmbedPress document widget in all versions up to, and including, 3.9.12 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.	2024-03-23	5.4	CVE-2024-2688
wpdevteam -- embedpress_-_embed_pdf_google_docs_vimeo_wistia_embed_youtube_videos_audios_maps_&_embed_any_documents_in_gutenberg_&_elementor	The EmbedPress - Embed PDF, Google Docs, Vimeo, Wistia, Embed YouTube Videos, Audios, Maps & Embed Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the EmbedPress widget 'embedpress_pro_twitch_theme ' attribute in all versions up to, and including, 3.9.12 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.	2024-03-23	6.4	CVE-2024-2468
wpdevteam -- essential_blocks_-_page_builder_gutenberg_blocks-patterns_&_templates	The Essential Blocks - Page Builder Gutenberg Blocks, Patterns & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 4.5.2 due to insufficient input sanitization and output escaping on user supplied attributes such as listStyle. 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.	2024-03-20	6.4	CVE-2024-2255
wpfunnels_team -- wpfunnels	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFunnels Team WPFunnels allows Stored XSS.This issue affects WPFunnels: from n/a through 3.0.6.	2024-03-21	5.9	CVE-2024-27965
wpvibes -- elementor_addon_	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPVibes Elementor Addon Elements allows Stored XSS.This issue affects Elementor Addon Elements: from n/a through 1.12.10.	2024-03-19	6.5	CVE-2024-29107

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
elements				
zaytech -- smart_online_order_for_clover	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zaytech Smart Online Order for Clover allows Stored XSS.This issue affects Smart Online Order for Clover: from n/a through 1.5.5.	2024-03-19	6.5	CVE-2024-29115
zimma_ltd. -- ticket_tailor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zimma Ltd. Ticket Tailor allows Stored XSS.This issue affects Ticket Tailor: from n/a through 1.10.	2024-03-19	6.5	CVE-2024-29104
zulip -- zulip	Zulip is an open-source team collaboration. When a user moves a Zulip message, they have the option to move all messages in the topic, move only subsequent messages as well, or move just a single message. If the user chose to just move one message, and was moving it from a public stream to a private stream, Zulip would successfully move the message, -- but active users who did not have access to the private stream, but whose client had already received the message, would continue to see the message in the public stream until they reloaded their client. Additionally, Zulip did not remove view permissions on the message from recently-active users, allowing the message to show up in the "All messages" view or in search results, but not in "Inbox" or "Recent conversations" views. While the bug has been present since moving messages between streams was first introduced in version 3.0, this option became much more common starting in Zulip 8.0, when the default option in the picker for moving the very last message in a conversation was changed. This issue is fixed in Zulip Server 8.3. No known workarounds are available.	2024-03-20	6.5	CVE-2024-27286
aio-libs -- aiosmtpd	aiosmtpd is a reimplementation of the Python stdlib smtpd.py based on asyncio. aiosmtpd is vulnerable to inbound SMTP smuggling. SMTP smuggling is a novel vulnerability based on not so novel interpretation differences of the SMTP protocol. By exploiting SMTP smuggling, an attacker may send smuggle/spoof e-mails with fake sender addresses, allowing advanced phishing attacks. This issue is also existed in other SMTP software like Postfix. With the right SMTP server constellation, an attacker can send spoofed e-mails to inbound/receiving aiosmtpd instances. This issue has been addressed in version 1.4.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-12	5.3	CVE-2024-27305
ameliabooking -- booking_for_appointments_and_events_calendar_-_amelia	The Booking for Appointments and Events Calendar - Amelia plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the date parameters in all versions up to, and including, 1.0.98 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.	2024-03-13	6.1	CVE-2024-1484
apache_software_foundation -- apache_pulsar	The vulnerability allows authenticated users with only produce or consume permissions to modify topic-level policies, such as retention, TTL, and offloading settings. These management operations should be restricted to users with the tenant admin role or super user role. This issue affects Apache Pulsar versions from 2.7.1 to 2.10.5, from 2.11.0 to 2.11.3, from 3.0.0 to 3.0.2, from 3.1.0 to 3.1.2, and 3.2.0. 2.10 Apache Pulsar users should upgrade to at least 2.10.6. 2.11 Apache Pulsar users should upgrade to at least 2.11.4. 3.0 Apache Pulsar users should upgrade to at least 3.0.3. 3.1 Apache Pulsar users should upgrade to at least 3.1.3. 3.2 Apache Pulsar users should upgrade to at least 3.2.1. Users operating versions prior to those listed above should upgrade to the aforementioned patched versions or newer versions.	2024-03-12	6.4	CVE-2024-28098
apache_software_foundation -- apache_zookeeper	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /Admin/add-admin.php. The manipulation of the argument avatar leads to unrestricted upload. The attack may be launched remotely. The exploit has been	2024-03-12	4.7	CVE-2024-2394

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disclosed to the public and may be used. VDB-256454 is the identifier assigned to this vulnerability.			
argoproj -- argo-cd	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. "Local sync" is an Argo CD feature that allows developers to temporarily override an Application's manifests with locally-defined manifests. Use of the feature should generally be limited to highly-trusted users, since it allows the user to bypass any merge protections in git. An improper validation bug allows users who have `create` privileges but not `override` privileges to sync local manifests on app creation. All other restrictions, including AppProject restrictions are still enforced. The only restriction which is not enforced is that the manifests come from some approved git/Helm/OCI source. The bug was introduced in 1.2.0-rc1 when the local manifest sync feature was added. The bug has been patched in Argo CD versions 2.10.3, 2.9.8, and 2.8.12. Users are advised to upgrade. Users unable to upgrade may mitigate the risk of branch protection bypass by removing `applications, create` RBAC access. The only way to eliminate the issue without removing RBAC access is to upgrade to a patched version.	2024-03-13	6.4	CVE-2023-50726
ari_soft -- ari_stream_quiz	Cross-Site Request Forgery (CSRF) vulnerability in ARI Soft ARI Stream Quiz.This issue affects ARI Stream Quiz: from n/a through 1.2.32.	2024-03-16	5.4	CVE-2023-51487
artibot -- artibot_free_chat_bot_for_wordpress_websites	The ArtiBot Free Chat Bot for WordPress WebSites plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.1.6 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.	2024-03-13	4.4	CVE-2024-0449
artibot -- artibot_free_chat_bot_for_wordpress_websites	The ArtiBot Free Chat Bot for WordPress WebSites plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the artibot_update function in all versions up to, and including, 1.1.6. This makes it possible for authenticated attackers, with subscriber-level access and above, to update plugin settings.	2024-03-13	5	CVE-2024-0447
atlas_gondal -- export_media_urls	Cross-Site Request Forgery (CSRF) vulnerability in Atlas Gondal Export Media URLs.This issue affects Export Media URLs: from n/a through 1.0.	2024-03-16	4.3	CVE-2023-51510
automattic,_inc. -- crowdsignal_dashboard_-_polls,_surveys_&_more	Cross-Site Request Forgery (CSRF) vulnerability in Automattic, Inc. Crowdsignal Dashboard - Polls, Surveys & more.This issue affects Crowdsignal Dashboard - Polls, Surveys & more: from n/a through 3.0.11.	2024-03-16	5.4	CVE-2023-51489
averta -- depicter_slider	Cross-Site Request Forgery (CSRF) vulnerability in Averta Depicter Slider.This issue affects Depicter Slider: from n/a through 2.0.6.	2024-03-16	5.4	CVE-2023-51491
badger_meter -- monitool	Incorrectly limiting the path to a restricted directory vulnerability in Badger Meter Monitool that affects versions up to 4.6.3 and earlier. This vulnerability allows an authenticated attacker to retrieve any file from the device using the download-file functionality.	2024-03-12	6.5	CVE-2024-1303 cve-
badger_meter -- monitool	Cross-site scripting vulnerability in Badger Meter Monitool that affects versions up to 4.6.3 and earlier. This vulnerability allows a remote attacker to send a specially crafted javascript payload to an authenticated user and partially hijack their browser session.	2024-03-12	6.3	CVE-2024-1304 cve-

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
barrykooij -- related_posts_for_wordpress	The Related Posts for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.2.1. This is due to missing or incorrect nonce validation on the handle_create_link() function. This makes it possible for unauthenticated attackers to add related posts to other posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This ultimately makes it possible for attackers to view draft and password protected posts.	2024-03-13	5.4	CVE-2024-0592
basix -- nex-forms_-_ultimate_form_builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Basix NEX-Forms - Ultimate Form Builder allows Stored XSS.This issue affects NEX-Forms - Ultimate Form Builder: from n/a through 8.5.5.	2024-03-15	6.5	CVE-2024-25593
bdthemes -- prime_slider_-_addons_for_elementor_(revolution_of_a_slider,_hero_slider,_ecommerce_slider)	The Prime Slider - Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title_tags' attribute of the Rubix widget in all versions up to, and including, 3.13.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1507
bdthemes -- prime_slider_-_addons_for_elementor_(revolution_of_a_slider,_hero_slider,_ecommerce_slider)	The Prime Slider - Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'settings['title_tags']' attribute of the Mercury widget in all versions up to, and including, 3.13.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1508
binhnguyenplus -- ladiapp:_landing_page,_popupx,_marketing_automation,_affiliate_marketin-¦	The LadiApp plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ladiflow_save_hook() function in versions up to, and including, 4.3. This makes it possible for authenticated attackers with subscriber-level access and above to update the 'ladiflow_hook_configs' option.	2024-03-12	4.3	CVE-2023-4626
binhnguyenplus -- ladiapp:_landing_page,_popupx,_marketing_automation,_affiliate_marketing-¦	The LadiApp plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_config() function in versions up to, and including, 4.4. This makes it possible for authenticated attackers with subscriber-level access and above to update the 'ladipage_config' option.	2024-03-12	4.3	CVE-2023-4627
binhnguyenplus -- ladiapp:_landing_page,_popupx,_marketing_automation,_affiliate_marketing-¦	The LadiApp plugin for WordPress is vulnerable to Cross-Site Request Forgery due to a missing nonce check on the ladiflow_save_hook() function in versions up to, and including, 4.4. This makes it possible for unauthenticated attackers to update the 'ladiflow_hook_configs' option via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-12	4.3	CVE-2023-4628
binhnguyenplus -- ladiapp:_landing_page,_popupx,_marketing_automation,_affiliate_marketi	The LadiApp plugin for WordPress is vulnerable to Cross-Site Request Forgery due to a missing nonce check on the save_config() function in versions up to, and including, 4.3. This makes it possible for unauthenticated attackers to update the 'ladipage_config' option via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-12	4.3	CVE-2023-4629

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ng-¦				
binhnguyenplus -- ladiapp:_landing_page,_popupx,_marketing_automation,_affiliate_marketing-¦	The LadiApp plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the publish_lp() function hooked via an AJAX action in versions up to, and including, 4.4. This makes it possible for authenticated attackers with subscriber-level access and above to change the LadiPage key (a key fully controlled by the attacker), enabling them to freely create new pages, including web pages that trigger stored XSS	2024-03-12	4.3	CVE-2023-4728
binhnguyenplus -- ladiapp:_landing_page,_popupx,_marketing_automation,_affiliate_marketing-¦	The LadiApp plugin for WordPress is vulnerable to Cross-Site Request Forgery due to a missing nonce check on the publish_lp() function hooked via an AJAX action in versions up to, and including, 4.4. This makes it possible for unauthenticated attackers to change the LadiPage key (a key fully controlled by the attacker), enabling them to freely create new pages, including web pages that trigger stored XSS via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-12	4.3	CVE-2023-4729
binhnguyenplus -- ladiapp:_landing_page,_popupx,_marketing_automation,_affiliate_marketing-¦	The LadiApp plugn for WordPress is vulnerable to Cross-Site Request Forgery due to a missing nonce check on the init_endpoint() function hooked via 'init' in versions up to, and including, 4.4. This makes it possible for unauthenticated attackers to modify a variety of settings, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. An attacker can directly modify the 'ladipage_key' which enables them to create new posts on the website and inject malicious web scripts,	2024-03-12	4.3	CVE-2023-4731
bitpressadmin -- contact_form_builder_by_bit_form:_create_contact_form,_multi_step_form,_conversational_form	The Contact Form Builder Plugin: Multi Step Contact Form, Payment Form, Custom Contact Form Plugin by Bit Form plugin for WordPress is vulnerable to unauthorized modification of data due to a insufficient user validation on the bitforms_update_form_entry AJAX action in all versions up to, and including, 2.10.1. This makes it possible for unauthenticated attackers to modify form submissions.	2024-03-13	5.3	CVE-2024-1640
blossomthemes -- blossom_spa	The Blossom Spa theme for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.3.4 via generated source. This makes it possible for unauthenticated attackers to extract sensitive data including contents of password-protected or scheduled posts.	2024-03-12	5.8	CVE-2024-2107
bluecoral -- chat_bubble_-_floating_chat_with_contact_chat_icons,_messages,_telegram,_email,_sms,_call_me_back	The Chat Bubble - Floating Chat with Contact Chat Icons, Messages, Telegram, Email, SMS, Call me back plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-03-13	4.4	CVE-2024-0898
bobbingwide -- oik	The oik plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes such as bw_contact_button and bw_button shortcodes in all versions up to, and including, 4.10.0 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.	2024-03-14	6.4	CVE-2024-2256
bradwenqiang -- hr	A vulnerability was found in BradWenqiang HR 2.0. It has been rated as critical. Affected by this issue is the function selectAll of the file /bishe/register of the component Background Management. The manipulation of the argument	2024-03-15	6.3	CVE-2024-2478

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	userName leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-256886 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
brainstormforce -- elementor_header_&_footer_builder	The Elementor Header & Footer Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the flyout_layout attribute in all versions up to, and including, 1.6.24 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1237
britner -- gutenberg_blocks_by_kadence_blocks_-_page_builder_features	The Gutenberg Blocks by Kadence Blocks - Page Builder Features plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the htmlTag attribute in all versions up to, and including, 3.2.23 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1541
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 2.2.5.	2024-03-15	6.5	CVE-2024-27189
charlestsmith -- word_replacer_pro	The Word Replacer Pro plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the word_replacer_ultra() function in all versions up to, and including, 1.0. This makes it possible for unauthenticated attackers to update arbitrary content on the affected WordPress site.	2024-03-16	5.3	CVE-2024-1733
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 the LinkWrapper attribute found in several widgets in all versions up to, and including, 1.3.7.4 due to insufficient input sanitization and output escaping the user supplied attribute. 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.	2024-03-14	6.4	CVE-2024-2249
chrisbadgett -- lifterlms_-_wordpress_lms_plugin_for_elearning	The LifterLMS - WordPress LMS Plugin for eLearning plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'process_review' function in all versions up to, and including, 7.5.1. This makes it possible for unauthenticated attackers to publish an unrestricted number of reviews on the site.	2024-03-13	5.3	CVE-2024-0377
cisco -- cisco_ios_xr_software	A vulnerability in the Secure Copy Protocol (SCP) and SFTP feature of Cisco IOS XR Software could allow an authenticated, local attacker to create or overwrite files in a system directory, which could lead to a denial of service (DoS) condition. The attacker would require valid user credentials to perform this attack. This vulnerability is due to a lack of proper validation of SCP and SFTP CLI input parameters. An attacker could exploit this vulnerability by authenticating to the device and issuing SCP or SFTP CLI commands with specific parameters. A successful exploit could allow the attacker to impact the functionality of the device, which could lead to a DoS condition. The device may need to be manually rebooted to recover. Note: This vulnerability is exploitable only when a local user invokes SCP or SFTP commands at the Cisco IOS XR CLI. A local user with administrative privileges could exploit this vulnerability remotely.	2024-03-13	6.5	CVE-2024-20262
cisco -- cisco_ios_xr_softw	The Video Conferencing with Zoom plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'zoom_recordings_by_meeting' shortcode in all versions up to, and including, 4.4.4 due to insufficient input sanitization and output	2024-03-12	6.4	CVE-2024-2031

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
are	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.			
cisco -- cisco_ios_xr_software	A vulnerability in the DHCP version 4 (DHCPv4) server feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to trigger a crash of the dhcpd process, resulting in a denial of service (DoS) condition. This vulnerability exists because certain DHCPv4 messages are improperly validated when they are processed by an affected device. An attacker could exploit this vulnerability by sending a malformed DHCPv4 message to an affected device. A successful exploit could allow the attacker to cause a crash of the dhcpd process. While the dhcpd process is restarting, which may take approximately two minutes, DHCPv4 server services are unavailable on the affected device. This could temporarily prevent network access to clients that join the network during that time period and rely on the DHCPv4 server of the affected device. Notes: Only the dhcpd process crashes and eventually restarts automatically. The router does not reload. This vulnerability only applies to DHCPv4. DHCP version 6 (DHCPv6) is not affected.	2024-03-13	5.3	CVE-2024-20266
cisco -- cisco_ios_xr_software	A vulnerability in the access control list (ACL) processing on MPLS interfaces in the ingress direction of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to improper assignment of lookup keys to internal interface contexts. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to access resources behind the affected device that were supposed to be protected by a configured ACL.	2024-03-13	5.8	CVE-2024-20315
cisco -- cisco_ios_xr_software	A vulnerability in the access control list (ACL) processing on Pseudowire interfaces in the ingress direction of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to improper assignment of lookup keys to internal interface contexts. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to access resources behind the affected device that were supposed to be protected by a configured ACL.	2024-03-13	5.8	CVE-2024-20322
cisco -- cisco_ios_xr_software	A vulnerability in the UDP forwarding code of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to bypass configured management plane protection policies and access the Simple Network Management Plane (SNMP) server of an affected device. This vulnerability is due to incorrect UDP forwarding programming when using SNMP with management plane protection. An attacker could exploit this vulnerability by attempting to perform an SNMP operation using broadcast as the destination address that could be processed by an affected device that is configured with an SNMP server. A successful exploit could allow the attacker to communicate to the device on the configured SNMP ports. Although an unauthenticated attacker could send UDP datagrams to the configured SNMP port, only an authenticated user can retrieve or modify data using SNMP requests.	2024-03-13	4.3	CVE-2024-20319
citrix -- citrix_sd-wan_standard/premium_editions	Server-Side Request Forgery (SSRF) in Citrix SD-WAN Standard/Premium Editions on or after 11.4.0 and before 11.4.4.46 allows an attacker to disclose limited information from the appliance via Access to management IP.	2024-03-12	6.5	CVE-2024-2049
ckan -- ckan	A user endpoint didn't perform filtering on an incoming parameter, which was added directly to the application log. This could lead to an attacker injecting false log entries or corrupt the log file format. This has been fixed in the CKAN versions 2.9.11 and 2.10.4. Users are advised to upgrade. Users unable to upgrade should override the `/user/reset` endpoint to filter the `id` parameter in order to exclude newlines.	2024-03-13	4.3	CVE-2024-27097
cloudflare -- quiche	Cloudflare Quiche (through version 0.19.1/0.20.0) was affected by an unlimited resource allocation vulnerability causing rapid increase of memory usage of the system running quiche server or client. A remote attacker could take advantage of	2024-03-12	5.9	CVE-2024-1765

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	this vulnerability by repeatedly sending an unlimited number of 1-RTT CRYPTO frames after previously completing the QUIC handshake. Exploitation was possible for the duration of the connection which could be extended by the attacker. quiche 0.19.2 and 0.20.1 are the earliest versions containing the fix for this issue.			
codename065 -- download_manager	The Download Manager Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 3.2.85 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.	2024-03-13	6.4	CVE-2023-6954
codename065 -- download_manager	The Download Manager plugin for WordPress is vulnerable to unauthorized file download of files added via the plugin in all versions up to, and including, 3.2.84. This makes it possible for unauthenticated attackers to download files added with the plugin (even when privately published).	2024-03-13	5.3	CVE-2023-6785
codeworkweb -- cww_companion	The CWW Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Module2 widget in all versions up to, and including, 1.2.7 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.	2024-03-12	6.4	CVE-2024-2130
collizo4sky -- paid_membership_plugin,_ecommerce,_user_registration_form,_login_form,_user_profile_&_restrict_content_-_profilepress	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content - ProfilePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's [reg-select-role] shortcode in all versions up to, and including, 4.15.0 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.	2024-03-13	6.4	CVE-2024-1409
collizo4sky -- paid_membership_plugin,_ecommerce,_user_registration_form,_login_form,_user_profile_&_restrict_content_-_profilepress	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content - ProfilePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 4.15.2 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 arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1535
collizo4sky -- paid_membership_plugin,_ecommerce,_user_registration_form,_login_form,_user_profile_&_restrict_content_-_profilepress	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content - ProfilePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 4.15.1 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.	2024-03-13	6.4	CVE-2024-1806
cool_plugins -- cryptocurrency_widgets_-_price_ticker_&_coins_list	Missing Authorization vulnerability in Cool Plugins Cryptocurrency Widgets - Price Ticker & Coins List.This issue affects Cryptocurrency Widgets - Price Ticker & Coins List: from n/a through 2.6.8.	2024-03-13	4.7	CVE-2024-27953

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cozmoslabs -- paid_member_subscriptions	Cross-Site Request Forgery (CSRF) vulnerability in Cozmoslabs Paid Member Subscriptions.This issue affects Paid Member Subscriptions: from n/a through 2.10.4.	2024-03-15	4.3	CVE-2023-51522
cozyvision1 -- sms_alert_order_notifications_-_woocommerce	The SMS Alert Order Notifications - WooCommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.6.9. This is due to missing or incorrect nonce validation on the processBulkAction function. This makes it possible for unauthenticated attackers to delete pages and posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-13	4.3	CVE-2024-1489
crmperks -- database_for_contact_form_7,_wpforms,_elementor_forms	The Database for Contact Form 7, WPforms, Elementor forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.3.3 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.	2024-03-13	6.4	CVE-2024-2030
cservit -- affiliate-toolkit – WordPress Affiliate Plugin	The affiliate-toolkit - WordPress Affiliate Plugin plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the atkp_create_list() function in all versions up to, and including, 3.5.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to to perform unauthorized actions such as creating product lists.	2024-03-08	6.3	CVE-2024-1851
cyberlord92 -- page_restriction_wordpress_(wp)_-_protect_wp_pages/post	The Page Restriction WordPress (WP) - Protect WP Pages/Post plugin for WordPress is vulnerable to information disclosure in all versions up to, and including, 1.3.4. This is due to the plugin not properly restricting access to pages via the REST API when a page has been made private. This makes it possible for unauthenticated attackers to view protected pages. The vendor has decided that they will not implement REST API protection on posts and pages and the restrictions will only apply to the front-end of the site. The vendors solution was to add notices throughout the dashboard and recommends installing the WordPress REST API Authentication plugin for REST API coverage.	2024-03-13	5.3	CVE-2024-0681
david_de_boer -- paytium:_mollie_payment_forms_&_donations	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David de Boer Paytium: Mollie payment forms & donations allows Stored XSS.This issue affects Paytium: Mollie payment forms & donations: from n/a through 4.4.2.	2024-03-13	6.5	CVE-2024-25099
dell -- poweredge_bios_intel_16g	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain an Improper SMM communication buffer verification vulnerability. A local low privileged attacker could potentially exploit this vulnerability leading to out-of-bound read/writes to SMRAM.	2024-03-13	5.3	CVE-2024-0162
dell -- poweredge_bios_intel_16g	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain a TOCTOU race condition vulnerability. A local low privileged attacker could potentially exploit this vulnerability to gain access to otherwise unauthorized resources.	2024-03-13	5.3	CVE-2024-0163
devitemsllc -- ht_mega_-_absolute_addons_for_elementor	The HT Mega - Absolute Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's blocks in all versions up to, and including, 2.4.6 due to insufficient input sanitization and output escaping on the 'titleTag' 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.	2024-03-12	6.4	CVE-2024-1397
devitemsllc -- ht_mega_-	The HT Mega - Absolute Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'border_type' attribute of the Post Carousel	2024-03-12	6.4	CVE-2024-1421

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_absolute_addons_for_elementor	widget in all versions up to, and including, 2.4.4 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.			
directus -- directus	Directus is a real-time API and App dashboard for managing SQL database content. The authentication API has a `redirect` parameter that can be exploited as an open redirect vulnerability as the user tries to log in via the API URL. There's a redirect that is done after successful login via the Auth API GET request to `directus/auth/login/google?redirect=http://malicious-fishing-site.com`. While credentials don't seem to be passed to the attacker site, the user can be phished into clicking a legitimate directus site and be taken to a malicious site made to look like a an error message "Your password needs to be updated" to phish out the current password. Users who login via OAuth2 into Directus may be at risk. This issue has been addressed in version 10.10.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-12	5.4	CVE-2024-28239
discourse -- discourse	Discourse is an open source platform for community discussion. In affected versions users that are allowed to invite others can inject arbitrarily large data in parameters used in the invite route. The problem has been patched in the latest version of Discourse. Users are advised to upgrade. Users unable to upgrade should disable invites or restrict access to them using the `invite allowed groups` site setting.	2024-03-15	6.5	CVE-2024-27085
discourse -- discourse	Discourse is an open source platform for community discussion. In affected versions the endpoints for suspending users, silencing users and exporting CSV files weren't enforcing limits on the sizes of the parameters that they accept. This could lead to excessive resource consumption which could render an instance inoperable. A site could be disrupted by either a malicious moderator on the same site or a malicious staff member on another site in the same multisite cluster. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-15	6.5	CVE-2024-27100
discourse -- discourse	Discourse is an open source platform for community discussion. In affected versions an attacker can learn that a secret subcategory exists under a public category which has no public subcategories. The issue is patched in the latest stable, beta and tests-passed version of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-15	5.3	CVE-2024-24748
discourse -- discourse	Discourse is an open source platform for community discussion. Without a rate limit on the POST /uploads endpoint, it makes it easier for an attacker to carry out a DoS attack on the server since creating an upload can be a resource intensive process. Do note that the impact varies from site to site as various site settings like `max_image_size_kb`, `max_attachment_size_kb` and `max_image_megapixels` will determine the amount of resources used when creating an upload. The issue is patched in the latest stable, beta and tests-passed version of Discourse. Users are advised to upgrade. Users unable to upgrade should reduce `max_image_size_kb`, `max_attachment_size_kb` and `max_image_megapixels` as smaller uploads require less resources to process. Alternatively, `client_max_body_size` can be reduced in Nginx to prevent large uploads from reaching the server.	2024-03-15	5.3	CVE-2024-24827
discourse -- discourse	Discourse is an open source platform for community discussion. In affected versions an attacker can learn that secret categories exist when they have backgrounds set. The issue is patched in the latest stable, beta and tests-passed version of Discourse. Users are advised to upgrade. Users unable to upgrade should temporarily remove category backgrounds.	2024-03-15	5.3	CVE-2024-28242
doofinder -- doofinder_for_wo	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Doofinder Doofinder for WooCommerce allows Stored XSS.This issue affects Doofinder for WooCommerce: from n/a through 2.1.8.	2024-03-15	5.9	CVE-2024-25596

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ocommerce				
dreamer -- cms	A vulnerability, which was classified as problematic, was found in Dreamer CMS 4.1.3. Affected is an unknown function of the file /admin/menu/toEdit. The manipulation of the argument id leads to cross-site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-256314 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-10	4.3	CVE-2024-2354
droitthemes -- droit_elementor_addons_-_widgets,_blocks,_templates_library_for_elementor_builder	The Droit Elementor Addons - Widgets, Blocks, Templates Library For Elementor Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 3.1.5 due to insufficient input sanitization and output escaping on user supplied attributes such as URL. 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.	2024-03-13	5.4	CVE-2024-2252
edge22 -- generateblocks	The GenerateBlocks plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.8.2 via Query Loop. This makes it possible for authenticated attackers, with contributor access and above, to see contents of posts and pages in draft or private status as well as those with scheduled publication dates.	2024-03-13	4.3	CVE-2024-1452
edge22 -- wp_show_posts	The WP Show Posts plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.1.4 via the wpsp_display function. This makes it possible for authenticated attackers with contributor access and above to view the contents of draft, trash, future, private and pending posts and pages.	2024-03-13	5.3	CVE-2024-1479
elementinvader -- elementinvader_addons_for_elementor	The ElementInvader Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the button link in the EliSlider in all versions up to, and including, 1.2.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-16	6.4	CVE-2024-2308
elementor -- elementor_pro	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Elementor Pro.This issue affects Elementor Pro: from n/a through 3.19.2.	2024-03-16	6.5	CVE-2024-23523
exafunction -- codeium-chrome	codeium-chrome is an open source code completion plugin for the chrome web browser. The service worker of the codeium-chrome extension doesn't check the sender when receiving an external message. This allows an attacker to host a website that will steal the user's Codeium api-key, and thus impersonate the user on the backend autocomplete server. This issue has not been addressed. Users are advised to monitor the usage of their API key.	2024-03-11	6.5	CVE-2024-28120
expresstech -- quiz_and_survey_master	Cross-Site Request Forgery (CSRF) vulnerability in ExpressTech Quiz And Survey Master. This issue affects Quiz And Survey Master: from n/a through 8.1.18.	2024-03-16	5.4	CVE-2023-51521
file_manager -- file_manager_pro	The File Manager Pro plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tb' parameter in all versions up to, and including, 8.3.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-03-13	6.1	CVE-2023-7015

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fluid-cloudnative -- fluid	Fluid is an open source Kubernetes-native Distributed Dataset Orchestrator and Accelerator for data-intensive applications. An OS command injection vulnerability within the Fluid project's JuicefsRuntime can potentially allow an authenticated user, who has the authority to create or update the K8s CRD Dataset/JuicefsRuntime, to execute arbitrary OS commands within the juicefs related containers. This could lead to unauthorized access, modification or deletion of data. Users who're using versions < 0.9.3 with JuicefsRuntime should upgrade to v0.9.3.	2024-03-15	4	CVE-2023-51699
follow-redirects -- follow-redirects	follow-redirects is an open source, drop-in replacement for Node's `http` and `https` modules that automatically follows redirects. In affected versions follow-redirects only clears authorization header during cross-domain redirect, but keep the proxy-authentication header which contains credentials too. This vulnerability may lead to credentials leak, but has been addressed in version 1.15.6. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-14	6.5	CVE-2024-28849
formfacade -- formfacade	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FormFacade allows Stored XSS.This issue affects FormFacade: from n/a through 1.0.0.	2024-03-15	6.5	CVE-2024-25934
fortinet -- fortimanager	A use of externally-controlled format string vulnerability [CWE-134] in Fortinet FortiManager version 7.4.0 through 7.4.1, version 7.2.0 through 7.2.3 and before 7.0.10, Fortinet FortiAnalyzer version 7.4.0 through 7.4.1, version 7.2.0 through 7.2.3 and before 7.0.10, Fortinet FortiAnalyzer-BigData before 7.2.5 and Fortinet FortiPortal version 6.0 all versions and version 5.3 all versions allows a privileged attacker to execute unauthorized code or commands via specially crafted command arguments.	2024-03-12	6.7	CVE-2023-41842
fortinet -- fortiportal	An improper authorization vulnerability [CWE-285] in FortiPortal version 7.2.0, and versions 7.0.6 and below reports may allow a user to download other organizations reports via modification in the request payload.	2024-03-12	4.3	CVE-2024-21761
fortinet -- fortiproxy	An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiOS version 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.1 through 7.0.13, 6.4.7 through 6.4.14, and FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 SSL-VPN may allow an authenticated attacker to gain access to another user's bookmark via URL manipulation.	2024-03-12	4.3	CVE-2024-23112
fortra -- filecatalyst	Improper URL validation leads to path traversal in FileCatalyst Direct 3.8.8 and earlier allowing an encoded payload to cause the web server to return files located outside of the web root which may lead to data leakage.	2024-03-13	5.3	CVE-2024-25154
fortra -- goanywhere_mft	A path traversal vulnerability exists in GoAnywhere MFT prior to 7.4.2 which allows attackers to circumvent endpoint-specific permission checks in the GoAnywhere Admin and Web Clients.	2024-03-14	6.5	CVE-2024-25156
frenify -- categorify_-_wordpress_media_library_category_&_file_manager	The Categorify plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the categorifyAjaxAddCategory function in all versions up to, and including, 1.0.7.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to add categories.	2024-03-13	4.3	CVE-2024-0385
friendlyelec -- friendlywrt	Cryptographic key vulnerability encoded in the FriendlyWrt firmware affecting version 2022-11-16.51b3d35. This vulnerability could allow an attacker to compromise the confidentiality and integrity of encrypted data.	2024-03-15	5.2	CVE-2024-2495 cve-
friendsofsymfony1 -- symfony1	Symfony1 is a community fork of symfony 1.4 with DIC, form enhancements, latest Swiftmailer, better performance, composer compatible and PHP 8 support. Symfony 1 has a gadget chain due to vulnerable Swift Mailer dependency that would enable an attacker to get remote code execution if a developer unserialize user input in his project. This vulnerability present no direct threat but is a vector	2024-03-15	5	CVE-2024-28859

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	that will enable remote code execution if a developper deserialize user untrusted data. Symfony 1 depends on Swift Mailer which is bundled by default in vendor directory in the default installation since 1.3.0. Swift Mailer classes implement some `__destruct()` methods. These methods are called when php destroys the object in memory. However, it is possible to include any object type in `$this->_keys` to make PHP access to another array/object properties than intended by the developer. In particular, it is possible to abuse the array access which is triggered on foreach($this->_keys ...) for any class implementing ArrayAccess interface. This may allow an attacker to execute any PHP command which leads to remote code execution. This issue has been addressed in version 1.5.18. Users are advised to upgrade. There are no known workarounds for this vulnerability.			
gacjie -- server	A vulnerability, which was classified as critical, was found in Gacjie Server up to 1.0. This affects the function index of the file /app/admin/controller/Upload.php. The manipulation of the argument file leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256503.	2024-03-12	5.4	CVE-2024-2406
geminilabs -- site_reviews	The Site Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the user display name in all versions up to, and including, 6.11.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-2293
gonahkar -- custom_fields_shortcode	The Custom fields shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's cf shortcode in all versions up to, and including, 0.1 due to insufficient input sanitization and output escaping on user supplied custom post meta values. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2023-6809
gpriday -- siteorigin_widgets_bundle	The SiteOrigin Widgets Bundle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several parameters in all versions up to, and including, 1.58.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Affected parameters include: $instance['fonts']['title_options']['tag'], $headline_tag, $sub_headline_tag, $feature['icon'].	2024-03-13	6.4	CVE-2024-1723
hammadh -- play.ht_-_make_your_blog_posts_accessible_with_text_to_speech_audio	The Play.ht - Make Your Blog Posts Accessible With Text to Speech Audio plugin for WordPress is vulnerable to unauthorized access of functionality due to a missing capability check on several functions in all versions up to, and including, 3.6.4. This makes it possible for authenticated attackers, with subscriber access or higher, to delete, retrieve, or modify post metadata, retrieve posts contents of protected posts, modify conversion data and delete article audio.	2024-03-13	5.4	CVE-2024-0828
hammadh -- play.ht_-_make_your_blog_posts_accessible_with_text_to_speech_audio	The Play.ht - Make Your Blog Posts Accessible With Text to Speech Audio plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.6.4. This is due to missing or incorrect nonce validation on several functions. This makes it possible for unauthenticated attackers to invoke those functions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-13	4.3	CVE-2024-0827
heimavista -- rpage	The disabling function of the user registration page for Heimavista Rpage and Epage is not properly implemented, allowing remote attackers to complete user registration on sites where user registration is supposed to be disabled.	2024-03-13	5.3	CVE-2024-2412 twcert@cert.org.tw

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hiroaki_miyashita -- custom_field_template	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hiroaki Miyashita Custom Field Template allows Stored XSS.This issue affects Custom Field Template: from n/a through 2.6.	2024-03-15	6.5	CVE-2024-25919
hitachi -- cosminexus_component_container	Insertion of Sensitive Information into Log File vulnerability in Hitachi Cosminexus Component Container allows local users to gain sensitive information.This issue affects Cosminexus Component Container: from 11-30 before 11-30-05, from 11-20 through 11-20-*, from 11-10 through 11-10-*, from 11-00 before 11-00-12, All versions of V8 and V9.	2024-03-12	5.6	CVE-2023-6814
htplugins -- ht_easy_ga4_-_google_analytics_wordpress_plugin	The HT Easy GA4 - Google Analytics WordPress Plugin plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the login() function in all versions up to, and including, 1.1.5. This makes it possible for unauthenticated attackers to update the email associated through the plugin with GA4.	2024-03-13	5.3	CVE-2024-1176
ibm -- host_access_transformation_services	IBM Host Access Transformation Services (HATS) 9.6 through 9.6.1.4 and 9.7 through 9.7.0.3 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 210989.	2024-03-15	6.2	CVE-2021-38938
ibm -- integration_bus_for_z/os	IBM Integration Bus for z/OS 10.1 through 10.1.0.3 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. IBM X-Force ID: 284564.	2024-03-14	4.5	CVE-2024-27265
ibm -- maximo_application_suite_-_maximo_mobile_for_eam	IBM Maximo Application Suite - Maximo Mobile for EAM 8.10 and 8.11 could disclose sensitive information to a local user. IBM X-Force ID: 266875.	2024-03-13	5.1	CVE-2023-43043
ibm -- maximo_asset_management	IBM Maximo Application Suite 7.6.1.3 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 262192.	2024-03-13	6.4	CVE-2023-38723
ibm -- secure_proxy	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 270973.	2024-03-15	6.1	CVE-2023-47162
ibm -- secure_proxy	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 270974.	2024-03-15	6.1	CVE-2023-47699
ibm -- secure_proxy	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 269692.	2024-03-15	5.4	CVE-2023-46182
ibm -- secure_proxy	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 could allow an attacker to overwrite a log message under specific conditions. IBM X-Force ID: 270598.	2024-03-15	5.9	CVE-2023-47147
ibm -- secure_proxy	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 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	2024-03-15	4.3	CVE-2023-46179

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 269683.			
ibm -- secure_proxy	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 269686.	2024-03-15	4	CVE-2023-46181
ibm -- sterling_partner_engagement_manager	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 250421.	2024-03-13	5.4	CVE-2023-28517
icopydoc -- yml_for_yandex_market	The YML for Yandex Market plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the feed_id parameter in all versions up to, and including, 4.2.3 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.	2024-03-13	6.1	CVE-2024-1365
intoxstudio -- restrict_user_access_-_ultimate_membership_&_content_protection	The Restrict User Access - Ultimate Membership & Content Protection plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 2.5 via API. This makes it possible for unauthenticated attackers to obtain the contents of posts and pages via API.	2024-03-13	5.3	CVE-2024-0687
joseph_c_dolson -- my_calendar	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Joseph C Dolson My Calendar allows Stored XSS.This issue affects My Calendar: from n/a through 3.4.23.	2024-03-15	6.5	CVE-2024-25916
justinbusa -- beaver_builder_-_wordpress_page_builder	The Beaver Builder - WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the button link parameter in all versions up to, and including, 2.7.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor access or higher to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-0896
justinbusa -- beaver_builder_-_wordpress_page_builder	The Beaver Builder - WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the image URL parameter in all versions up to, and including, 2.7.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-0897
justinbusa -- beaver_builder_-_wordpress_page_builder	The Beaver Builder - WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the audio widget 'link_url' parameter in all versions up to, and including, 2.7.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1074
justinbusa -- beaver_builder_-_wordpress_page_builder	The Beaver Builder - WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the via the heading tag in all versions up to, and including, 2.7.4.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1080
justinbusa -- beaver_builder_-	The Beaver Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Icon Widget 'fl_builder_data[node_preview][link]' and	2024-03-13	5.4	CVE-2024-0871

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_wordpress_page_builder	'fl_builder_data[settings][link_target]' parameters in all versions up to, and including, 2.7.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
justinbusa -- beaver_builder_-_wordpress_page_builder	The Beaver Builder - WordPress Page Builder plugin for WordPress is vulnerable to DOM-Based Reflected Cross-Site Scripting via a 'playground.wordpress.net' parameter in all versions up to, and including, 2.7.4.2 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.	2024-03-13	5.4	CVE-2024-1038
kbjohnson90 -- user_shortcodes_plus	The User Shortcodes Plus plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.0.2 via the user_meta shortcode due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with contributor-level access and above, to retrieve potentially sensitive user meta.	2024-03-13	5.3	CVE-2023-6969
korenix -- jeti/o_6550	Information exposure vulnerability in Korenix JetI/O 6550 affecting firmware version F208 Build:0817. The SNMP protocol uses plaintext to transfer data, allowing an attacker to intercept traffic and retrieve credentials.	2024-03-12	6.2	CVE-2024-2371 cve-
leap13 -- premium_addons_for_elementor	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Link Wrapper functionality in all versions up to, and including, 4.10.17 due to insufficient input sanitization and output escaping on user supplied links. 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.	2024-03-13	6.4	CVE-2024-0326
leap13 -- premium_addons_for_elementor	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Image Settings URL of the Banner, Team Members, and Image Scroll widgets in all versions up to, and including, 4.10.21 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.	2024-03-13	6.4	CVE-2024-1680
livemesh -- elementor_addons_by_livemesh	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Livemesh Elementor Addons by Livemesh allows Stored XSS.This issue affects Elementor Addons by Livemesh: from n/a through 8.3.5.	2024-03-14	6.5	CVE-2024-27986
livemesh -- livemesh_addons_for_elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Livemesh Livemesh Addons for Elementor allows Stored XSS.This issue affects Livemesh Addons for Elementor: from n/a through 8.3.	2024-03-15	6.5	CVE-2024-25598
livemesh -- wpbakery_page_builder_addons_by_livemesh	The WPBakery Page Builder Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'per_line_mobile' shortcode in all versions up to, and including, 3.8.1 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.	2024-03-13	6.4	CVE-2024-2079
logitech -- logi_tune	Improper Control of Dynamically-Managed Code Resources vulnerability in Logitech Logi Tune on MacOS allows Local Code Inclusion.	2024-03-15	4.4	CVE-2024-2537
magesh-k21 -- online-college-event-hall-	A vulnerability, which was classified as critical, was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. This affects an unknown part of the file home.php. The manipulation of the argument id leads to sql injection. It is possible	2024-03-16	6.3	CVE-2024-2516

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
reservation-system	to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256953 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as critical. This vulnerability affects unknown code of the file book_history.php. The manipulation of the argument del_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-256954 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	6.3	CVE-2024-2517
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/bookdate.php. The manipulation of the argument room_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256957 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	6.3	CVE-2024-2520
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability classified as critical has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. This affects an unknown part of the file /admin/booktime.php. The manipulation of the argument room_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. The associated identifier of this vulnerability is VDB-256959. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	6.3	CVE-2024-2522
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability, which was classified as critical, has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. This issue affects some unknown processing of the file /admin/receipt.php. The manipulation of the argument room_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256961 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	6.3	CVE-2024-2524
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/rooms.php. The manipulation of the argument room_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256964. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	6.3	CVE-2024-2527
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/update-rooms.php. The manipulation of the argument room_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. The identifier VDB-256965 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	6.3	CVE-2024-2528
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/rooms.php. The manipulation leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-256966 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	6.3	CVE-2024-2529

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability classified as critical has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected is an unknown function of the file /admin/update-rooms.php. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256968. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	6.3	CVE-2024-2531
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability classified as critical was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/update-users.php. The 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. The identifier VDB-256969 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	6.3	CVE-2024-2532
mainwp -- mainwp_dashboard_-_wordpress_manager_for_multiple_websites_maintenance	The MainWP Dashboard - WordPress Manager for Multiple Websites Maintenance plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.6.0.1. This is due to missing or incorrect nonce validation on the 'posting_bulk' function. This makes it possible for unauthenticated attackers to delete arbitrary posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-13	4.3	CVE-2024-1642
mattermost -- mattermost	Mattermost Jira plugin versions shipped with Mattermost versions 8.1.x before 8.1.10, 9.2.x before 9.2.6, 9.3.x before 9.3.2, and 9.4.x before 9.4.3 fail to escape user-controlled outputs when generating HTML pages, which allows an attacker to perform reflected cross-site scripting attacks against the users of the Mattermost server.	2024-03-15	6.1	CVE-2024-2445
mattermost -- mattermost	Mattermost versions 8.1.x before 8.1.10, 9.2.x before 9.2.6, 9.3.x before 9.3.2, and 9.4.x before 9.4.3 fail to limit the number of @-mentions processed per message, allowing an authenticated attacker to crash the client applications of other users via large, crafted messages.	2024-03-15	4.3	CVE-2024-2446
mattermost -- mattermost_mobile	A vulnerability was found in RaspAP raspap-webgui 3.0.9 and classified as critical. This issue affects some unknown processing of the file includes/provider.php of the component HTTP POST Request Handler. The manipulation of the argument country leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256919. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-15	4.7	CVE-2024-2497
mdp -- rotp	The Ruby One Time Password library (ROTP) is an open source library for generating and validating one time passwords. Affected versions had overly permissive default permissions. Users should patch to version 6.3.0. Users unable to patch may correct file permissions after installation.	2024-03-16	5.3	CVE-2024-28862
metagauss -- eventprime_-_events_calendar,_bookings_and_tickets	The EventPrime - Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the get_attendees_email_by_event_id() 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 to retrieve the attendees list for any event.	2024-03-13	5.3	CVE-2024-1126
metagauss -- eventprime_-_events_calendar,_bookings_and_tickets	The EventPrime - Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to payment bypass in all versions up to, and including, 3.4.2. This is due to the plugin allowing unauthenticated users to update the status of order payments. This makes it possible for unauthenticated attackers to book events for free.	2024-03-13	5.3	CVE-2024-1321

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
metagauss -- eventprime_-_events_calendar,_bookings_and_tickets	The EventPrime - Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the booking_export_all() 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 retrieve all event booking which can contain PII.	2024-03-13	4.3	CVE-2024-1127
mha_sistemas -- armhazena	A vulnerability classified as critical was found in MHA Sistemas arMHAzena 9.6.0.0. This vulnerability affects unknown code of the component Executa Page. The manipulation of the argument Companhia/Planta/Agente de/Agente até leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256888. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-15	6.3	CVE-2024-2480
microsoft -- intune_company_portal_for_android	Microsoft Intune Linux Agent Elevation of Privilege Vulnerability	2024-03-12	6.6	CVE-2024-26201
microsoft -- microsoft_edge_(chromium-based)	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2024-03-14	4.7	CVE-2024-26163
microsoft -- microsoft_teams_for_android	Microsoft Teams for Android Information Disclosure Vulnerability	2024-03-12	5	CVE-2024-21448
microsoft -- windows_10_version_1809	Windows USB Hub Driver Remote Code Execution Vulnerability	2024-03-12	6.8	CVE-2024-21429
microsoft -- windows_10_version_1809	Windows Hyper-V Denial of Service Vulnerability	2024-03-12	5.5	CVE-2024-21408
microsoft -- windows_10_version_1809	Windows USB Attached SCSI (UAS) Protocol Remote Code Execution Vulnerability	2024-03-12	5.7	CVE-2024-21430
microsoft -- windows_10_version_1809	Windows Kernel Information Disclosure Vulnerability	2024-03-12	5.5	CVE-2024-26174
microsoft -- windows_10_version_1809	Windows Kernel Information Disclosure Vulnerability	2024-03-12	5.5	CVE-2024-26177
microsoft -- windows_10_version_1809	Windows Kernel Denial of Service Vulnerability	2024-03-12	5.5	CVE-2024-26181
microsoft -- windows_11_versi	Windows Compressed Folder Tampering Vulnerability	2024-03-12	6.5	CVE-2024-26185

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
on_22h2				
microsoft -- windows_11_version_22h2	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability	2024-03-12	5.5	CVE-2024-26160
microsoft -- windows_defender_antimalware_platform	Microsoft Defender Security Feature Bypass Vulnerability	2024-03-12	5.5	CVE-2024-20671
microsoft -- windows_server_2019	Windows Standards-Based Storage Management Service Denial of Service Vulnerability	2024-03-12	6.5	CVE-2024-26197
movistar_ -- router_movistar_4g	Cross-Site Request Forgery vulnerability in Movistar's 4G router affecting version ES_WLD71-T1_v2.0.201820. This vulnerability allows an attacker to force an end user to execute unwanted actions in a web application in which they are currently authenticated.	2024-03-13	6.5	CVE-2024-2416 cve-
mra13 -- simple_membership	The Simple Membership plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Display Name' parameter in all versions up to, and including, 4.4.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This vulnerability requires social engineering to successfully exploit, and the impact would be very limited due to the attacker requiring a user to login as the user with the injected payload for execution.	2024-03-13	4.7	CVE-2024-1985
msaari -- relevanssi_-_a_better_search	The Relevanssi - A Better Search plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the relevanssi_export_log_check() function in all versions up to, and including, 4.22.0. This makes it possible for unauthenticated attackers to export the query log data. The vendor has indicated that they may look into adding a capability check for proper authorization control, however, this vulnerability is theoretically patched as is.	2024-03-13	5.3	CVE-2024-1380
n/a -- 1panel	A vulnerability, which was classified as critical, has been found in 1Panel up to 1.10.1-lts. Affected by this issue is the function baseApi.UpdateDeviceSwap of the file /api/v1/toolbox/device/update/swap. The manipulation of the argument Path with the input 123123123\nopen -a Calculator leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-256304.	2024-03-10	6.3	CVE-2024-2352
n/a -- 3rd_and_4th_generation_intel(r)_xeon(r)_processors_when_using_intel(r)_sgx_or_intel(r)_tdx	Protection mechanism failure in some 3rd and 4th Generation Intel(R) Xeon(R) Processors when using Intel(R) SGX or Intel(R) TDX may allow a privileged user to potentially enable escalation of privilege via local access.	2024-03-14	6.1	CVE-2023-22655

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a -- intel(r)_atom(r)_processors	Information exposure through microarchitectural state after transient execution from some register files for some Intel(R) Atom(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	2024-03-14	6.5	CVE-2023-28746
n/a -- intel(r)_csme_installer_software	Incorrect default permissions in some Intel(R) CSME installer software before version 2328.5.5.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-03-14	6.7	CVE-2023-28389
n/a -- intel(r)_csme_installer_software	Improper input validation in the Intel(R) CSME installer software before version 2328.5.5.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-03-14	6.7	CVE-2023-32633
n/a -- intel(r)_processors	Protection mechanism failure of bus lock regulator for some Intel(R) Processors may allow an unauthenticated user to potentially enable denial of service via network access.	2024-03-14	6.5	CVE-2023-39368
n/a -- intel(r)_processors	Non-transparent sharing of return predictor targets between contexts in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.	2024-03-14	5.5	CVE-2023-38575
n/a -- intel(r)_sps_firmware_versions	Uncontrolled resource consumption for some Intel(R) SPS firmware versions may allow a privileged user to potentially enable denial of service via network access.	2024-03-14	6.8	CVE-2023-35191
n/a -- intel(r)_xeon(r)_d_processors_with_intel(r)_sgx	Incorrect calculation in microcode keying mechanism for some Intel(R) Xeon(R) D Processors with Intel(R) SGX may allow a privileged user to potentially enable information disclosure via local access.	2024-03-14	5.3	CVE-2023-43490
n/a -- libvirt	An off-by-one error flaw was found in the udevListInterfacesByStatus() function in libvirt when the number of interfaces exceeds the size of the `names` array. This issue can be reproduced by sending specially crafted data to the libvirt daemon, allowing an unprivileged client to perform a denial of service attack by causing the libvirt daemon to crash.	2024-03-11	5.5	CVE-2024-1441
n/a -- openstack-designate	An access-control flaw was found in the OpenStack Designate component where private configuration information including access keys to BIND were improperly made world readable. A malicious attacker with access to any container could exploit this flaw to access sensitive information.	2024-03-15	6.6	CVE-2023-6725
n/a -- ovn	A flaw was found in the Open Virtual Network (OVN). In OVN clusters where BFD is used between hypervisors for high availability, an attacker can inject specially crafted BFD packets from inside unprivileged workloads, including virtual machines or containers, that can trigger a denial of service.	2024-03-12	6.5	CVE-2024-2182
ndijkstra -- mollie_forms	The Mollie Forms plugin for WordPress is vulnerable to unauthorized post or page duplication due to a missing capability check on the duplicateForm function in all versions up to, and including, 2.6.3. This makes it possible for authenticated attackers, with subscriber access or higher, to duplicate arbitrary posts and pages.	2024-03-11	4.3	CVE-2024-1400
ndijkstra -- mollie_forms	The Mollie Forms plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the exportRegistrations function in all versions up to, and including, 2.6.3. This makes it possible for authenticated attackers, with subscriber access or higher, to export payment data collected by this plugin.	2024-03-11	4.3	CVE-2024-1645
netweblogic -- events_manager_-	The Events Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 6.4.6.4 due to	2024-03-13	4.4	CVE-2024-0614

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_calendar,_bookings,_tickets,_and_more!	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.			
newsletter2go -- newsletter2go	The Newsletter2Go plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'style' parameter in all versions up to, and including, 4.0.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-12	6.4	CVE-2024-1328
nik00726 -- team_circle_image_slider_with_lightbox	The Team Circle Image Slider With Lightbox plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing or incorrect nonce validation on the circle_thumbnail_slider_with_lightbox_image_management_func() function. This makes it possible for unauthenticated attackers to edit image data which can be used to inject malicious JavaScript, along with deleting images, and uploading malicious files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-03-13	5.3	CVE-2015-10130
nixos -- nix	Nix is a package manager for Linux and other Unix systems. A fixed-output derivations on Linux can send file descriptors to files in the Nix store to another program running on the host (or another fixed-output derivation) via Unix domain sockets in the abstract namespace. This allows to modify the output of the derivation, after Nix has registered the path as "valid" and immutable in the Nix database. In particular, this allows the output of fixed-output derivations to be modified from their expected content. This issue has been addressed in versions 2.3.18 2.18.2 2.19.4 and 2.20.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-11	6.3	CVE-2024-27297
nmedia -- comments_extra_fields_for_post,pages_and_cpt	The Comments Extra Fields For Post,Pages and CPT plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 5.0. This is due to missing or incorrect capability checks on several ajax actions. This makes it possible for authenticated attackers, with subscriber access or higher, to invoke those actions. As a result, they may modify comment form fields and update plugin settings.	2024-03-13	4.3	CVE-2024-0829
nmedia -- comments_extra_fields_for_post,pages_and_cpt	The Comments Extra Fields For Post,Pages and CPT plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.0. This is due to missing or incorrect nonce validation on several ajax actions. This makes it possible for unauthenticated attackers to invoke those actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. As a result, they may modify comment form fields and update plugin settings.	2024-03-13	4.3	CVE-2024-0830
openolat -- openolat	OpenOlat is an open source web-based e-learning platform for teaching, learning, assessment and communication. By manually manipulating http requests when using the draw.io integration it is possible to read arbitrary files as the configured system user and SSRF. The problem is fixed in version 18.1.6 and 18.2.2. It is advised to upgrade to the latest version of 18.1.x or 18.2.x. Users unable to upgrade may work around this issue by disabling the Draw.io module or the entire REST API which will secure the system.	2024-03-11	4.6	CVE-2024-28198
opentext -- vertica_management_console	Certain functionality in OpenText Vertica Management console might be prone to bypass via crafted requests. The vulnerability would affect one of Vertica's authentication functionalities by allowing specially crafted requests and sequences. This issue impacts the following Vertica Management Console versions: 10.x 11.1.1-24 or lower 12.0.4-18 or lower Please upgrade to one of the following Vertica Management Console versions: 10.x to upgrade to latest versions from below. 11.1.1-25 12.0.4-19 23.x 24.x	2024-03-15	5	CVE-2023-7248

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
opentext--exceed_turbo_x	HTML injection in OpenText™ Exceed Turbo X affecting version 12.5.1. The vulnerability could result in Cross site scripting.	2024-03-13	6.4	CVE-2023-38536
opentextâ„¢ --exceed_turbo_x	Use of Hard-coded Cryptographic Key vulnerability in OpenText™ Exceed Turbo X affecting versions 12.5.1 and 12.5.2. The vulnerability could compromise the cryptographic keys.	2024-03-13	4.7	CVE-2023-38535
palantir --com.palantir.acme.gaia:gaia	One of Gotham Gaia services was found to be vulnerable to a stored cross-site scripting (XSS) vulnerability that could have allowed an attacker to bypass CSP and get a persistent cross site scripting payload on the stack.	2024-03-12	6.8	CVE-2023-30968
palo_alto_networks --globalprotect_app	An issue in the Palo Alto Networks GlobalProtect app enables a non-privileged user to disable the GlobalProtect app in configurations that allow a user to disable GlobalProtect with a passcode.	2024-03-13	5.5	CVE-2024-2431
palo_alto_networks --globalprotect_app	A privilege escalation (PE) vulnerability in the Palo Alto Networks GlobalProtect app on Windows devices enables a local user to execute programs with elevated privileges. However, execution requires that the local user is able to successfully exploit a race condition.	2024-03-13	4.5	CVE-2024-2432
palo_alto_networks -- pan-os	An improper authorization vulnerability in Palo Alto Networks Panorama software enables an authenticated read-only administrator to upload files using the web interface and completely fill one of the disk partitions with those uploaded files, which prevents the ability to log into the web interface or to download PAN-OS, WildFire, and content images. This issue affects only the web interface of the management plane; the dataplane is unaffected.	2024-03-13	4.3	CVE-2024-2433
papercut --papercut_ng,_papercut_mf	This is a reflected cross site scripting vulnerability in the PaperCut NG/MF application server. An attacker can exploit this weakness by crafting a malicious URL that contains a script. When an unsuspecting user clicks on this malicious link, it could potentially lead to limited loss of confidentiality, integrity or availability.	2024-03-14	6.3	CVE-2024-1883
papercut --papercut_ng,_papercut_mf	This is a Server-Side Request Forgery (SSRF) vulnerability in the PaperCut NG/MF server-side module that allows an attacker to induce the server-side application to make HTTP requests to an arbitrary domain of the attacker's choosing.	2024-03-14	6.5	CVE-2024-1884
papercut --papercut_ng,_papercut_mf	This vulnerability potentially allows unauthorized enumeration of information from the embedded device APIs. An attacker must already have existing knowledge of some combination of valid usernames, device names and an internal system key. For such an attack to be successful the system must be in a specific runtime state.	2024-03-14	4.8	CVE-2024-1223
pawaryogesh1989 --bulk_edit_post_titles	The Bulk Edit Post Titles plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the bulkUpdatePostTitles function in all versions up to, and including, 5.0.0. This makes it possible for authenticated attackers, with subscriber access and above, to modify the titles of arbitrary posts.	2024-03-13	4.3	CVE-2024-0369
peering-manager --peering-manager	Peering Manager is a BGP session management tool. Affected versions of Peering Manager are subject to a potential stored Cross-Site Scripting (XSS) attack in the `name` attribute of AS or Platform. The XSS triggers on a routers detail page. Adversaries are able to execute arbitrary JavaScript code with the permission of a victim. XSS attacks are often used to steal credentials or login tokens of other users. This issue has been addressed in version 1.8.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-12	6.1	CVE-2024-28112
phoenix_contact --charx_sec-3000	An unauthenticated remote attacker can upload a arbitrary script file due to improper input validation. The upload destination is fixed and is write only.	2024-03-12	5.3	CVE-2024-25994

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
phoenix_contact -- charx_sec-3000	An unauthenticated remote attacker can perform a remote code execution due to an origin validation error. The access is limited to the service user.	2024-03-12	5.3	CVE-2024-25996
phoenix_contact -- charx_sec-3000	An unauthenticated remote attacker can perform a log injection due to improper input validation. Only a certain log file is affected.	2024-03-12	5.3	CVE-2024-25997
phoenix_contact -- charx_sec-3000	An unauthenticated remote attacker can read memory out of bounds due to improper input validation in the MQTT stack. The brute force attack is not always successful because of memory randomization.	2024-03-12	5.9	CVE-2024-26000
phoenix_contact -- charx_sec-3000	An unauthenticated remote attacker can gain service level privileges through an incomplete cleanup during service restart after a DoS.	2024-03-12	4.8	CVE-2024-26005
pinterest -- querybook	Querybook is a Big Data Querying UI, combining collocated table metadata and a simple notebook interface. Querybook's datadocs functionality works by using a Websocket Server. The client talks to this WSS whenever updating/deleting/reading any cells as well as for watching the live status of query executions. Currently the CORS setting allows all origins, which could result in cross-site websocket hijacking and allow attackers to read/edit/remove datadocs of the user. This issue has been addressed in version 3.32.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-14	5.6	CVE-2024-28251
postalserver -- postal	Postal is an open source SMTP server. Postal versions less than 3.0.0 are vulnerable to SMTP Smuggling attacks which may allow incoming e-mails to be spoofed. This, in conjunction with a cooperative outgoing SMTP service, would allow for an incoming e-mail to be received by Postal addressed from a server that a user has 'authorised' to send mail on their behalf but were not the genuine author of the e-mail. Postal is not affected for sending outgoing e-mails as email is re-encoded with `<CR><LF>` line endings when transmitted over SMTP. This issue has been addressed and users should upgrade to Postal v3.0.0 or higher. Once upgraded, Postal will only accept End of DATA sequences which are explicitly `<CR><LF>.<CR><LF>`. If a non-compliant sequence is detected it will be logged to the SMTP server log. There are no workarounds for this issue.	2024-03-11	5.3	CVE-2024-27938
premium_addons_for_elementor -- premium_addons_pro_for_elementor	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's IHover widget link in all versions up to, and including, 2.9.12 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.	2024-03-13	6.4	CVE-2024-1996
premium_addons_for_elementor -- premium_addons_pro_for_elementor	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'premium_fbchat_app_id' parameter of the Messenger Chat Widget in all versions up to, and including, 2.9.12 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.	2024-03-13	6.4	CVE-2024-1997
premium_addons_for_elementor -- premium_addons_pro_for_elementor	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'navigation_dots' parameter of the Multi Scroll Widget in all versions up to, and including, 2.9.12 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.	2024-03-13	6.4	CVE-2024-2000
premium_addons_for_elementor -- premium_addons_	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Global Badge module in all versions up to, and including, 2.9.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject	2024-03-13	6.4	CVE-2024-2237

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pro_for_elementor	arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
premium_addons_for_elementor -- premium_addons_pro_for_elementor	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Custom Mouse Cursor module in all versions up to, and including, 2.9.12 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.	2024-03-13	6.4	CVE-2024-2238
premium_addons_for_elementor -- premium_addons_pro_for_elementor	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Premium Magic Scroll module in all versions up to, and including, 2.9.12 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.	2024-03-13	6.4	CVE-2024-2239
premium_addons_for_elementor -- premium_addons_pro_for_elementor	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 4.10.23 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.	2024-03-15	6.4	CVE-2024-2399
qnap -- qts	An injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later	2024-03-08	6.5	CVE-2024-21900
radgeek -- feedwordpress	The FeedWordPress plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2022.0222 due to missing validation on the user controlled 'guid' key. This makes it possible for unauthenticated attackers to view draft posts that may contain sensitive information.	2024-03-13	5.3	CVE-2024-0839
rayhanduitku -- duitku_payment_gateway	The Duitku Payment Gateway plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the check_duitku_response function in all versions up to, and including, 2.11.4. This makes it possible for unauthenticated attackers to change the payment status of orders to failed.	2024-03-13	5.3	CVE-2024-0631
realmag777 -- husky_-_products_filter_for_woocommerce_(formerly_woof)	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 HUSKY - Products Filter for WooCommerce (formerly WOOF).This issue affects HUSKY - Products Filter for WooCommerce (formerly WOOF): from n/a through 1.3.4.3.	2024-03-15	4.3	CVE-2023-50861
realmag777 -- husky_-_products_filter_professional_for_woocommerce	The HUSKY - Products Filter for WooCommerce Professional plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'woof' shortcode in all versions up to, and including, 1.3.5.1 due to insufficient input sanitization and output escaping on user supplied attributes such as 'swoof_slug'. 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.	2024-03-15	6.4	CVE-2024-1796
rednao -- woocommerce_pdf_invoice_builder	Cross-Site Request Forgery (CSRF) vulnerability in RedNao WooCommerce PDF Invoice Builder.This issue affects WooCommerce PDF Invoice Builder: from n/a through 1.2.101.	2024-03-16	5.4	CVE-2023-51486

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rejetto_ -- http_file_server_	An open redirect vulnerability, the exploitation of which could allow an attacker to create a custom URL and redirect a legitimate page to a malicious site.	2024-03-12	6.5	CVE-2024-1227 cve-
rocket_elements -- split_test_for_elementor	Cross-Site Request Forgery (CSRF) vulnerability in Rocket Elements Split Test For Elementor.This issue affects Split Test For Elementor: from n/a through 1.6.9.	2024-03-16	4.3	CVE-2023-51407
rogierlankhorst -- burst_statistics_-_privacy-friendly_analytics_for_wordpress	The Burst Statistics - Privacy-Friendly Analytics for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'burst_total_pageviews_count' custom meta field in all versions up to, and including, 1.5.6.1 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. Note that this exploit only functions if the victim has the 'Show Toolbar when viewing site' option enabled in their profile.	2024-03-13	6.4	CVE-2024-1894
sap_se -- netweaver_(wsrm)	Under certain conditions SAP NetWeaver WSRM - version 7.50, allows an attacker to access information which would otherwise be restricted, causing low impact on Confidentiality with no impact on Integrity and Availability of the application.	2024-03-12	5.3	CVE-2024-25644
sap_se -- sap_abap_platform	Due to missing authorization check, attacker with business user account in SAP ABAP Platform - version 758, 795, can change the privacy setting of job templates from shared to private. As a result, the selected template would only be accessible to the owner.	2024-03-12	4.3	CVE-2024-27900
sap_se -- sap_fiori_front_end_server	SAP Fiori Front End Server - version 605, allows altering of approver details on the read-only field when sending leave request information. This could lead to creation of request with incorrect approver causing low impact on Confidentiality and Integrity with no impact on Availability of the application.	2024-03-12	4.6	CVE-2024-22133
sap_se -- sap_netweaver_(enterprise_portal)	Under certain condition SAP NetWeaver (Enterprise Portal) - version 7.50 allows an attacker to access information which would otherwise be restricted causing low impact on confidentiality of the application and with no impact on Integrity and Availability of the application.	2024-03-12	5.3	CVE-2024-25645
sap_se -- sap_netweaver_as_abap_applications_based_on_sapgui_for_html_(webgui)	Applications based on SAP GUI for HTML in SAP NetWeaver AS ABAP - versions 7.89, 7.93, do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. A successful attack can allow a malicious attacker to access and modify data through their ability to execute code in a user's browser. There is no impact on the availability of the system	2024-03-12	5.4	CVE-2024-27902
sap_se -- sap_netweaver_process_integration_(support_web_pages)	Under certain conditions, Support Web Pages of SAP NetWeaver Process Integration (PI) - versions 7.50, allows an attacker to access information which would otherwise be restricted, causing low impact on Confidentiality with no impact on Integrity and Availability of the application.	2024-03-12	5.3	CVE-2024-28163
sewpafly -- post_thumbnail_editor	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Sewpafly Post Thumbnail Editor.This issue affects Post Thumbnail Editor: from n/a through 2.4.8.	2024-03-16	5.3	CVE-2024-24845
shapedplugin -- easy_accordion_-_best_accordion_faq_plugin_for_wor	The Easy Accordion - Best Accordion FAQ Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'accordion_content_source' attribute in all versions up to, and including, 2.3.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject	2024-03-13	6.4	CVE-2024-1363

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dpress	arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
siemens -- sentron_7km_pac3120_ac/dc	A vulnerability has been identified in SENTRON 7KM PAC3120 AC/DC (7KM3120-0BA01-1DA0) (All versions >= V3.2.3 < V3.3.0 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...)), SENTRON 7KM PAC3120 DC (7KM3120-1BA01-1EA0) (All versions >= V3.2.3 < V3.3.0 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...)), SENTRON 7KM PAC3220 AC/DC (7KM3220-0BA01-1DA0) (All versions >= V3.2.3 < V3.3.0 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...)), SENTRON 7KM PAC3220 DC (7KM3220-1BA01-1EA0) (All versions >= V3.2.3 < V3.3.0 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...)). The read out protection of the internal flash of affected devices was not properly set at the end of the manufacturing process. An attacker with physical access to the device could read out the data.	2024-03-12	4.6	CVE-2024-21483
siemens -- siveillance_control	A vulnerability has been identified in Siveillance Control (All versions >= V2.8 < V3.1.1). The affected product does not properly check the list of access groups that are assigned to an individual user. This could enable a locally logged on user to gain write privileges for objects where they only have read privileges.	2024-03-12	5.5	CVE-2023-45793
sirv.com -- sirv	Missing Authorization vulnerability in sirv.Com Sirv.This issue affects Sirv: from n/a through 7.1.2.	2024-03-15	5.4	CVE-2023-50898
skyhigh -- skyhigh_client_proxy	A malicious insider can bypass the existing policy of Skyhigh Client Proxy without a valid release code.	2024-03-14	5.5	CVE-2024-0311
skyhigh -- skyhigh_client_proxy	A malicious insider can uninstall Skyhigh Client Proxy without a valid uninstall password.	2024-03-14	5.5	CVE-2024-0312
skyhigh -- skyhigh_client_proxy	A malicious insider exploiting this vulnerability can circumvent existing security controls put in place by the organization. On the contrary, if the victim is legitimately using the temporary bypass to reach out to the Internet for retrieving application and system updates, a remote device could target it and undo the bypass, thereby denying the victim access to the update service, causing it to fail.	2024-03-14	5.5	CVE-2024-0313
snowflakedb -- snowflake-hive-metastore-connector	The Snowflake Hive metastore connector provides an easy way to query Hive-managed data via Snowflake. Snowflake Hive MetaStore Connector has addressed a potential elevation of privilege vulnerability in a `helper script` for the Hive MetaStore Connector. A malicious insider without admin privileges could, in theory, use the script to download content from a Microsoft domain to the local system and replace the valid content with malicious code. If the attacker then also had local access to the same system where the maliciously modified script is run, they could attempt to manipulate users into executing the attacker-controlled helper script, potentially gaining elevated privileges to the local system. The vulnerability in the script was patched on February 09, 2024, without a version bump to the Connector. User who use the helper script are strongly advised to use the latest version as soon as possible. Users unable to upgrade should avoid using the helper script.	2024-03-15	4	CVE-2024-28851
softaculous -- backuply_-_backup,_restore,_migrate_and_clone	The Backuply - Backup, Restore, Migrate and Clone plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.2.7 via the backup_name parameter in the backuply_download_backup function. This makes it possible for attackers to have an account with only activate_plugins capability to access arbitrary files on the server, which can contain sensitive information. This only impacts sites hosted on Windows servers.	2024-03-16	4.9	CVE-2024-2294

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
soundcloud_inc.,_lawrie_malen -- soundcloud_shortcode	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SoundCloud Inc., Lawrie Malen SoundCloud Shortcode allows Stored XSS.This issue affects SoundCloud Shortcode: from n/a through 4.0.1.	2024-03-15	6.5	CVE-2024-25936
sourcecodester -- best_pos_management_system	A vulnerability was found in SourceCodester Best POS Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /view_order.php. The 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. The identifier VDB-256705 was assigned to this vulnerability.	2024-03-13	6.3	CVE-2024-2418
sourcecodester -- crud_without_page_reload	A vulnerability was found in SourceCodester CRUD without Page Reload 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file add_user.php. The manipulation of the argument city leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256453 was assigned to this vulnerability.	2024-03-12	6.3	CVE-2024-2393
stylemix -- masterstudy_lms_wordpress_plugin_-_for_online_courses_and_education	The MasterStudy LMS WordPress Plugin - for Online Courses and Education plugin for WordPress is vulnerable to Information Exposure in versions up to, and including, 3.2.10. This can allow unauthenticated attackers to extract sensitive data including all registered user's username and email addresses which can be used to help perform future attacks.	2024-03-13	5.3	CVE-2024-2106
subratamal -- terawallet_-_best_woocommerce_wallet_system_with_cashback_rewards,_partial_payment,_wallet_refunds	The TeraWallet - Best WooCommerce Wallet System With Cashback Rewards, Partial Payment, Wallet Refunds plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the terawallet_export_user_search() function in all versions up to, and including, 1.4.10. This makes it possible for authenticated attackers, with subscriber-level access and above, to export a list of registered users and their emails.	2024-03-13	4.3	CVE-2024-1690
surya2developer -- hostel_management_service	A vulnerability, which was classified as problematic, has been found in Surya2Developer Hostel Management Service 1.0. This issue affects some unknown processing of the file /change-password.php of the component Password Change Handler. The manipulation of the argument oldpassword leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256889 was assigned to this vulnerability.	2024-03-15	4.3	CVE-2024-2483
surya2developer -- hostel_management_system	A vulnerability, which was classified as critical, was found in Surya2Developer Hostel Management System 1.0. Affected is an unknown function of the file /admin/manage-students.php. The manipulation of the argument del leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-256890 is the identifier assigned to this vulnerability.	2024-03-15	6.5	CVE-2024-2481
svenl77 -- post_form_-_registration_form_-_profile_form_for_user_profiles_-_frontend_content_forms_for_user_s	The Post Form - Registration Form - Profile Form for User Profiles - Frontend Content Forms for User Submissions (UGC) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the buddyforms_new_page function in all versions up to, and including, 2.8.7. This makes it possible for authenticated attackers, with subscriber access or higher, to create pages with arbitrary titles. These pages are published.	2024-03-13	4.3	CVE-2024-1158

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ubmissions_(ugc)				
sysbasics -- customize_my_account_for_woocommerce	Cross-Site Request Forgery (CSRF) vulnerability in SysBasics Customize My Account for WooCommerce.This issue affects Customize My Account for WooCommerce: from n/a through 1.8.3.	2024-03-15	4.3	CVE-2023-51369
takayukister -- contact_form_7	The Contact Form 7 plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'active-tab' parameter in all versions up to, and including, 5.9 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.	2024-03-13	6.1	CVE-2024-2242
techfyd -- sky_addons_for_elementor_(free_templates_library,_live_copy,_animations,_post_grid,_post_carousel,_particles,_sliders,_chart,_blogs)	The Sky Addons for Elementor (Free Templates Library, Live Copy, Animations, Post Grid, Post Carousel, Particles, Sliders, Chart) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the wrapper link URL value in all versions up to, and including, 2.4.0 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.	2024-03-13	6.4	CVE-2024-2286
techjewel -- contact_form_plugin_by_fluent_forms_for_quiz,_survey,_and_drag_&_drop_wp_form_builder	The Fluent Forms plugin for WordPress by Fluent Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 5.1.9 due to insufficient input sanitization and output escaping. This makes it possible for attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The exploitation level depends on who is granted the right to create forms by an administrator. This level can be as low as contributor, but by default is admin.	2024-03-13	4.9	CVE-2023-6957
thedark -- auto_affiliate_links	The Auto Affiliate Links plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the aalAddLink function in all versions up to, and including, 6.4.3. This makes it possible for authenticated attackers, with subscriber access or higher, to add arbitrary links to posts.	2024-03-13	4.3	CVE-2024-1843
themefusecom -- brizy_-_page_builder	The Brizy - Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Countdown URL parameter in all versions up to, and including, 2.4.40 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1291
themefusecom -- brizy_-_page_builder	The Brizy - Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the embedded media custom block in all versions up to, and including, 2.4.40 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1293
themefusecom -- brizy_-_page_builder	The Brizy - Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's block upload in all versions up to, and including, 2.4.40 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.	2024-03-13	6.4	CVE-2024-1296

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
themefusion -- avada_|_website_builder_for_wordpress_&_woocommerce	The Avada | Website Builder For WordPress & WooCommerce theme for WordPress is vulnerable to Sensitive Information Exposure in versions up to and including 7.11.5 via the form entries page. This makes it possible for authenticated attackers, with contributor access and above, to view the contents of all form submissions, including fields that are obfuscated (such as the contact form's "password" field).	2024-03-13	6.5	CVE-2024-1668
themegrill -- maintenance_page	The Maintenance Page plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the subscribe_download function hooked via AJAX action in all versions up to, and including, 1.0.8. This makes it possible for authenticated attackers, with subscriber access or higher, to download a csv containing subscriber emails.	2024-03-13	5.3	CVE-2024-1370
themegrill -- maintenance_page	The Maintenance Page plugin for WordPress is vulnerable to Basic Information Exposure in all versions up to, and including, 1.0.8 via the REST API. This makes it possible for unauthenticated attackers to view post titles and content when the site is in maintenance mode.	2024-03-13	5.3	CVE-2024-1462
themeisle -- orbit_fox_by_themeisle	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form widget addr2_width attribute in all versions up to, and including, 2.10.30 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1497
themeisle -- orbit_fox_by_themeisle	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Pricing Table widget in the $settings['title_tags'] parameter in all versions up to, and including, 2.10.30 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1499
themeisle -- orbit_fox_by_themeisle	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Registration Form widget in all versions up to, and including, 2.10.32 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.	2024-03-13	6.4	CVE-2024-2126
themencode_llc -- tnc_pdf_viewer	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeNcode LLC TNC PDF viewer allows Stored XSS.This issue affects TNC PDF viewer: from n/a through 2.8.0.	2024-03-13	6.5	CVE-2024-25097
themisle -- otter_blocks_pro_-_gutenberg_blocks,_page_builder_for_gutenberg_editor_&_fse	The Otter Blocks - Gutenberg Blocks, Page Builder for Gutenberg Editor & FSE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the contact form file field CSS metabox in all versions up to, and including, 2.6.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1684
themisle -- otter_blocks_pro_-_gutenberg_blocks,_page_builder_for_gutenberg_editor_&_fse	The Otter Blocks - Gutenberg Blocks, Page Builder for Gutenberg Editor & FSE PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via file upload form, which allows SVG uploads, in all versions up to, and including, 2.6.3 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. Note that the patch in 2.6.4 allows SVG uploads but the uploaded SVG files are sanitized.	2024-03-13	6.1	CVE-2024-1691
tibco_software_inc. -- tibco_activespaces	The Proxy and Client components of TIBCO Software Inc.'s TIBCO ActiveSpaces - Enterprise Edition contain a vulnerability that theoretically allows an Active Spaces client to passively observe data traffic to other clients. Affected releases are TIBCO	2024-03-12	4.3	CVE-2024-1137

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_-_enterprise_edition	Software Inc.'s TIBCO ActiveSpaces - Enterprise Edition: versions 4.4.0 through 4.9.0.			
timstrifler -- exclusive_addons_for_elementor	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via data attribute in all versions up to, and including, 2.6.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1234
timstrifler -- exclusive_addons_for_elementor	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Countdown Timer widget in all versions up to, and including, 2.6.9 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.	2024-03-13	6.4	CVE-2024-1413
timstrifler -- exclusive_addons_for_elementor	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Call To Action widget in all versions up to, and including, 2.6.9 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.	2024-03-13	6.4	CVE-2024-1414
timstrifler -- exclusive_addons_for_elementor	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Covid-19 Stats Widget in all versions up to, and including, 2.6.9 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.	2024-03-13	6.4	CVE-2024-2028
turtlepod -- f(x)_private_site	The f(x) Private Site plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.2.1 via the API. This makes it possible for unauthenticated attackers to obtain page and post contents of a site protected with this plugin.	2024-03-12	5.3	CVE-2024-0906
vantage6 -- vantage6	vantage6 is an open source framework built to enable, manage and deploy privacy enhancing technologies like Federated Learning and Multi-Party Computation. Much like GHSA-45gq-q4xh-cp53, it is possible to find which usernames exist in vantage6 by calling the API routes `/recover/lost` and `/2fa/lost`. These routes send emails to users if they have lost their password or MFA token. This issue has been addressed in commit `aecfd6d0e` and is expected to ship in subsequent releases. Users are advised to upgrade as soon as a new release is available. There are no known workarounds for this vulnerability.	2024-03-14	5.3	CVE-2024-24770
vantage6 -- vantage6	vantage6 is an open source framework built to enable, manage and deploy privacy enhancing technologies like Federated Learning and Multi-Party Computation. The vantage6 server has no restrictions on CORS settings. It should be possible for people to set the allowed origins of the server. The impact is limited because v6 does not use session cookies. This issue has been addressed in commit `70bb4e1d8` and is expected to ship in subsequent releases. Users are advised to upgrade as soon as a new release is available. There are no known workarounds for this vulnerability.	2024-03-14	4.2	CVE-2024-23823
vantage6 -- vantage6-ui	vantage6-UI is the official user interface for the vantage6 server. In affected versions a number of security headers are not set. This issue has been addressed in commit `68dfa6614` which is expected to be included in future releases. Users are advised to upgrade when a new release is made. While an upgrade path is not available users may modify the docker image build to insert the headers into nginx.	2024-03-14	5.4	CVE-2024-24562

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
visualcomposer -- visual_composer_website_builder,_landing_page_builder,_custom_theme_builder,_maintenance_mode_&_coming_soon_pages	The Visual Composer Website Builder, Landing Page Builder, Custom Theme Builder, Maintenance Mode & Coming Soon Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's custom fields in all versions up to, and including, 45.6.0 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.	2024-03-13	6.4	CVE-2023-6880
wago -- controller_bacnet/ip	An unauthenticated remote attacker can use an XSS attack due to improper neutralization of input during web page generation. User interaction is required. This leads to a limited impact of confidentiality and integrity but no impact of availability.	2024-03-13	5.4	CVE-2018-25090
wbw -- product_table_by_wbw	Cross Site Request Forgery (CSRF) vulnerability in WBW Product Table by WBW.This issue affects Product Table by WBW: from n/a through 1.8.6.	2024-03-16	4.3	CVE-2023-51512
webtechstreet -- elementor_addon_elements	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'icon_align' attribute of the Content Switcher widget in all versions up to, and including, 1.12.12 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.	2024-03-13	6.4	CVE-2024-1393
webtechstreet -- elementor_addon_elements	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'eae_custom_overlay_switcher' attribute of the Thumbnail Slider widget in all versions up to, and including, 1.12.12 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.	2024-03-13	6.4	CVE-2024-1391
webtechstreet -- elementor_addon_elements	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button1_icon' attribute of the Dual Button widget in all versions up to, and including, 1.12.12 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.	2024-03-13	6.4	CVE-2024-1392
webtechstreet -- elementor_addon_elements	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the modal popup widget's effect setting in all versions up to, and including, 1.12.12 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.	2024-03-13	6.4	CVE-2024-1422
wokamoto -- simple_tweet	The Simple Tweet plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Tweet this text value in all versions up to, and including, 1.4.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-0700
wpchill -- simple_restrict	The Simple Restrict plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.2.6 via the REST API. This makes it possible for authenticated attackers to bypass the plugin's restrictions to extract post titles and content	2024-03-13	5.3	CVE-2024-1083
wpdatatables -- wpdatatables_-_wordpress_data_	The wpDataTables - WordPress Data Table, Dynamic Tables & Table Charts Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'A' parameter in all versions up to, and including, 3.4.2.2 due to insufficient input	2024-03-13	6.1	CVE-2024-0591

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
table,_dynamic_tables_&_table_charts_plugin	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.			
wpdevteam -- essential_addons_for_elementor_-_best_elementor_templates,_widgets,_kits_&_woocommerce_builders	The Essential Addons for Elementor - Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Data Table widget in all versions up to, and including, 5.9.9 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.	2024-03-13	6.4	CVE-2024-1537
wpdevteam -- essential_blocks_-_page_builder_gutenberg_blocks,_patterns_&_templates	The Essential Blocks - Page Builder Gutenberg Blocks, Patterns & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the blockId parameter in all versions up to, and including, 4.5.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-13	6.4	CVE-2024-1854
wpeventmanager -- wp_event_manager_-_events_calendar,_registrations,_sell_tickets_with_woocommerce	The WP Event Manager - Events Calendar, Registrations, Sell Tickets with WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the plugin parameter in all versions up to, and including, 3.1.41 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.	2024-03-13	6.1	CVE-2024-0976
wpgmaps -- wp_go_maps_(formerly_wp_google_maps)	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpgmza' shortcode in all versions up to, and including, 9.0.32 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.	2024-03-13	6.4	CVE-2024-1582
wpgmaps -- wp_go_maps_(formerly_wp_google_maps)	The WP Go Maps for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 9.0.32 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.	2024-03-13	4.4	CVE-2023-4839
wpmu_dev -- broken_link_checker	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPMU DEV Broken Link Checker allows Stored XSS.This issue affects Broken Link Checker: from n/a through 2.2.3.	2024-03-15	5.9	CVE-2024-25592
wpswings -- ultimate_gift_cards_for_woocommerce_-_create,_redeem_&_manage_digital_gift_certificates_with_personalized	The Ultimate Gift Cards for WooCommerce - Create, Redeem & Manage Digital Gift Certificates with Personalized Templates plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.6.6 via the wps_wgm_preview_email_template(). This makes it possible for unauthenticated attackers to read password protected and draft posts that may contain sensitive data.	2024-03-16	5.3	CVE-2024-1857

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
_templates				
wpvividplugins -- wpvivid_backup_for_mainwp	The WPvivid Backup for MainWP plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 0.9.32 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.	2024-03-13	6.1	CVE-2024-1383
wpwax -- legal_pages	Cross-Site Request Forgery (CSRF), Incorrect Authorization vulnerability in wpWax Legal Pages.This issue affects Legal Pages: from n/a through 1.3.7.	2024-03-15	4.3	CVE-2023-50886
xpeedstudio -- elementskit_elementor_addons	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the blog post read more button in all versions up to, and including, 3.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-03-16	6.4	CVE-2024-1239
xpeedstudio -- elementskit_elementor_addons	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Image Accordion widget in all versions up to, and including, 3.0.5 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.	2024-03-16	6.4	CVE-2024-2042
xpeedstudio -- elementskit_elementor_addons	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the progress bar element attributes in all versions up to, and including, 3.0.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This primarily affects multi-site installations and installations where unfiltered_html has been disabled.	2024-03-16	5.5	CVE-2023-6525
xpeedstudio -- metform_elementor_contact_form_builder	The Metform Elementor Contact Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 3.8.3 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.	2024-03-13	6.4	CVE-2024-1585
xpeedstudio -- wp_social_login_and_register_social_counter	The Wp Social Login and Register Social Counter plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the /wp_social/v1/ REST API endpoint in all versions up to, and including, 3.0.0. This makes it possible for unauthenticated attackers to enable and disable certain providers for the social share and login features.	2024-03-13	6.5	CVE-2024-1763
yonifre -- maspik_-_spam_blacklist	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in yonifre Maspik - Spam Blacklist allows Stored XSS.This issue affects Maspik - Spam Blacklist: from n/a through 0.10.6.	2024-03-13	5.9	CVE-2024-25101
yooooomi -- your_spotify	your_spotify is an open source, self hosted Spotify tracking dashboard. YourSpotify version <1.8.0 allows users to create a public token in the settings, which can be used to provide guest-level access to the information of that specific user in YourSpotify. The /me API endpoint discloses Spotify API access and refresh tokens to guest users. Attackers with access to a public token for guest access to YourSpotify can therefore obtain access to Spotify API tokens of YourSpotify users. As a consequence, attackers may extract profile information, information about listening habits, playlists and other information from the corresponding Spotify profile. In addition, the attacker can pause and resume playback in the Spotify app	2024-03-13	6.5	CVE-2024-28193

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	at will. This issue has been resolved in version 1.8.0. Users are advised to upgrade. There are no known workarounds for this issue.			
yooooomi -- your_spotify	your_spotify is an open source, self hosted Spotify tracking dashboard. YourSpotify version < 1.9.0 does not prevent other pages from displaying it in an iframe and is thus vulnerable to clickjacking. Clickjacking can be used to trick an existing user of YourSpotify to trigger actions, such as allowing signup of other users or deleting the current user account. Clickjacking works by opening the target application in an invisible iframe on an attacker-controlled site and luring a victim to visit the attacker page and interacting with it. By positioning elements over the invisible iframe, a victim can be tricked into triggering malicious or destructive actions in the invisible iframe, while they think they interact with a totally different site altogether. When a victim visits an attacker-controlled site while they are logged into YourSpotify, they can be tricked into performing actions on their YourSpotify instance without their knowledge. These actions include allowing signup of other users or deleting the current user account, resulting in a high impact to the integrity of YourSpotify. This issue has been addressed in version 1.9.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-13	6.5	CVE-2024-28196
yooooomi -- your_spotify	your_spotify is an open source, self hosted Spotify tracking dashboard. YourSpotify version <1.8.0 is vulnerable to NoSQL injection in the public access token processing logic. Attackers can fully bypass the public token authentication mechanism, regardless if a public token has been generated before or not, without any user interaction or prerequisite knowledge. This vulnerability allows an attacker to fully bypass the public token authentication mechanism, regardless if a public token has been generated before or not, without any user interaction or prerequisite knowledge. This issue has been addressed in version 1.8.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-13	5.3	CVE-2024-28192
zemana -- antilogger	Zemana AntiLogger v2.74.204.664 is vulnerable to a Memory Information Leak vulnerability by triggering the 0x80002020 IOCTL code of the zam64.sys and zamguard64.sys drivers	2024-03-15	5.5	CVE-2024-2180
zemana -- antilogger	Zemana AntiLogger v2.74.204.664 is vulnerable to a Denial of Service (DoS) vulnerability by triggering the 0x80002004 and 0x80002010 IOCTL codes of the zam64.sys and zamguard64.sys drivers.	2024-03-15	5.5	CVE-2024-2204
zemena -- antilogger	Zemana AntiLogger v2.74.204.664 is vulnerable to an Arbitrary Process Termination vulnerability by triggering the 0x80002048 IOCTL code of the zam64.sys and zamguard64.sys drivers.	2024-03-14	5.5	CVE-2024-1853
zoom_video_communications,_inc. -- zoom_rooms_client_for_windows	Race condition in the installer for Zoom Rooms Client for Windows before version 5.17.5 may allow an authenticated user to conduct a denial of service via local access.	2024-03-13	5.3	CVE-2024-24692

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ampache -- ampache	Ampache is a web based audio/video streaming application and file manager. Stored Cross Site Scripting (XSS) vulnerability in ampache before v6.3.1 allows a remote attacker to execute code via a crafted payload to serval parameters in the post request of /preferences.php?action=admin_update_preferences. This vulnerability is fixed in 6.3.1.	2024-03-27	3.9	CVE-2024-28853
awesomestcode -- livebot	A vulnerability was found in AwesomestCode LiveBot. It has been classified as problematic. Affected is the function parseSend of the file js/parseMessage.js. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. Upgrading to version 0.1 is able to address this issue. The name of the patch is 57505527f838d1e46e8f93d567ba552a30185bfa. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-257784.	2024-03-25	3.5	CVE-2020-36826
bdtask -- multi-store_inventory_management_system	A vulnerability was found in Bdtask Multi-Store Inventory Management System up to 20240320. It has been classified as problematic. Affected is an unknown function of the component Page Title Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-258198 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	2.4	CVE-2024-2996
bdtask -- multi-store_inventory_management_system	A vulnerability was found in Bdtask Multi-Store Inventory Management System up to 20240320. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument Category Name/Model Name/Brand Name/Unit Name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258199. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	2.4	CVE-2024-2997
bdtask -- multi-store_inventory_management_system	A vulnerability was found in Bdtask Multi-Store Inventory Management System up to 20240320. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Store Update Page. The manipulation of the argument Store Name/Store Address leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258200. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-27	2.4	CVE-2024-2998
campcodes -- online_examination_system	A vulnerability classified as problematic has been found in Campcodes Online Examination System 1.0. Affected is an unknown function of the file /adminpanel/admin/facebox_modal/updateExaminee.php. The manipulation of the argument id leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-258030 is the identifier assigned to this vulnerability.	2024-03-27	3.5	CVE-2024-2939
campcodes -- online_examination_system	A vulnerability classified as problematic was found in Campcodes Online Examination System 1.0. Affected by this vulnerability is an unknown functionality of the file /adminpanel/admin/facebox_modal/updateCourse.php. The manipulation of the argument id leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258031.	2024-03-27	3.5	CVE-2024-2940
code-projects -- online_book_system	A vulnerability was found in code-projects Online Book System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /Product.php. The manipulation of the argument value leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-258206 is the identifier assigned to this vulnerability.	2024-03-27	3.5	CVE-2024-3004

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
easycorp -- easyadmin	A vulnerability was found in EasyCorp EasyAdmin up to 4.8.9. It has been declared as problematic. Affected by this vulnerability is the function Autocomplete of the file assets/js/autocomplete.js of the component Autocomplete. The manipulation of the argument item leads to cross site scripting. The attack can be launched remotely. Upgrading to version 4.8.10 is able to address this issue. The identifier of the patch is 127436e4c3f56276d548070f99e61b7234200a11. It is recommended to upgrade the affected component. The identifier VDB-258613 was assigned to this vulnerability.	2024-03-29	3.5	CVE-2024-3081
hcl_software -- bigfix_platform	An administrative user of WebReports may perform a Server Side Request Forgery (SSRF) exploit through SMTP configuration options.	2024-03-28	3.5	CVE-2023-45705
hcl_software -- bigfix_platform	The console may experience a service interruption when processing file names with invalid characters.	2024-03-28	3.5	CVE-2023-45715
hcl_software -- bigfix_platform	An administrative user of WebReports may perform a Cross Site Scripting (XSS) and/or Man in the Middle (MITM) exploit through SAML configuration.	2024-03-28	2	CVE-2023-45706
ibm -- common_cryptographic_architecture	Under certain conditions, RSA operations performed by IBM Common Cryptographic Architecture (CCA) 7.0.0 through 7.5.36 may exhibit non-constant-time behavior. This could allow a remote attacker to obtain sensitive information using a timing-based attack. IBM X-Force ID: 257676.	2024-03-26	3.7	CVE-2023-33855
molongui -- molongui	Authorization Bypass Through User-Controlled Key vulnerability in Molongui.This issue affects Molongui: from n/a through 4.7.7.	2024-03-29	2.7	CVE-2024-30507
nautobot -- nautobot	Nautobot is a Network Source of Truth and Network Automation Platform. A number of Nautobot URL endpoints were found to be improperly accessible to unauthenticated (anonymous) users. These endpoints will not disclose any Nautobot data to an unauthenticated user unless the Nautobot configuration variable EXEMPT_VIEW_PERMISSIONS is changed from its default value (an empty list) to permit access to specific data by unauthenticated users. This vulnerability is fixed in 1.6.16 and 2.1.9.	2024-03-26	3.7	CVE-2024-29199
phpgurukul -- emergency_ambulance_hiring_portal	A vulnerability was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/add-ambulance.php of the component Add Ambulance Page. The manipulation of the argument Ambulance Reg No/Driver Name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-258683.	2024-03-30	2.4	CVE-2024-3090
phpgurukul -- emergency_ambulance_hiring_portal	A vulnerability was found in PHPGurukul Emergency Ambulance Hiring Portal 1.0. It has been classified as problematic. Affected is an unknown function of the file /admin/search.php of the component Search Request Page. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-258684.	2024-03-30	2.4	CVE-2024-3091
sourcecodester -- todo_list_in_kanban_board	A vulnerability, which was classified as problematic, has been found in SourceCodester Todo List in Kanban Board 1.0. Affected by this issue is some unknown functionality of the component Add ToDo. The manipulation of the argument Todo leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-258014 is the identifier assigned to this vulnerability.	2024-03-27	3.5	CVE-2024-2935

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
thorsten -- phpmyfaq	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. There is a Path Traversal vulnerability in Attachments that allows attackers with admin rights to upload malicious files to other locations of the web root. This vulnerability is fixed in 3.2.6.	2024-03-26	3.8	CVE-2024-29196
xpdf -- xpdf	Out-of-bounds array write in Xpdf 4.05 and earlier, triggered by negative object number in indirect reference in the input PDF file.	2024-03-26	2.9	CVE-2024-2971
adobe -- adobe_experience_manager	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2024-03-18	3.4	CVE-2024-26051
campcodes -- complete_online_dj_booking_system	A vulnerability was found in Campcodes Complete Online DJ Booking System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/user-search.php. The manipulation of the argument searchdata leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257468.	2024-03-20	3.5	CVE-2024-2715
campcodes -- complete_online_dj_booking_system	A vulnerability was found in Campcodes Complete Online DJ Booking System 1.0. It has been classified as problematic. This affects an unknown part of the file /admin/contactus.php. The manipulation of the argument email leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257469 was assigned to this vulnerability.	2024-03-20	3.5	CVE-2024-2716
campcodes -- complete_online_dj_booking_system	A vulnerability was found in Campcodes Complete Online DJ Booking System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/booking-search.php. The manipulation of the argument searchdata leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257470 is the identifier assigned to this vulnerability.	2024-03-20	3.5	CVE-2024-2717
campcodes -- complete_online_dj_booking_system	A vulnerability was found in Campcodes Complete Online DJ Booking System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/booking-bwdates-reports-details.php. The manipulation of the argument fromdate leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257471.	2024-03-20	3.5	CVE-2024-2718
campcodes -- complete_online_dj_booking_system	A vulnerability classified as problematic has been found in Campcodes Complete Online DJ Booking System 1.0. Affected is an unknown function of the file /admin/admin-profile.php. The manipulation of the argument adminname leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257472.	2024-03-20	3.5	CVE-2024-2719
campcodes -- complete_online_dj_booking_system	A vulnerability classified as problematic was found in Campcodes Complete Online DJ Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/aboutus.php. The manipulation of the argument pagetitle leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257473 was assigned to this vulnerability.	2024-03-20	3.5	CVE-2024-2720
campcodes -- online_job_finder_system	A vulnerability was found in Campcodes Online Job Finder System 1.0. It has been classified as problematic. This affects an unknown part of the file /admin/vacancy/index.php. The manipulation of the argument view leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257379.	2024-03-20	3.5	CVE-2024-2679

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
campcodes -- online_job_finder_system	A vulnerability was found in Campcodes Online Job Finder System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/user/index.php. The manipulation of the argument view leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257380.	2024-03-20	3.5	CVE-2024-2680
campcodes -- online_job_finder_system	A vulnerability was found in Campcodes Online Job Finder System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/employee/index.php. The manipulation of the argument view leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257381 was assigned to this vulnerability.	2024-03-20	3.5	CVE-2024-2681
campcodes -- online_job_finder_system	A vulnerability classified as problematic has been found in Campcodes Online Job Finder System 1.0. Affected is an unknown function of the file /admin/employee/controller.php. The manipulation of the argument EMPLOYEEID leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257382 is the identifier assigned to this vulnerability.	2024-03-20	3.5	CVE-2024-2682
campcodes -- online_job_finder_system	A vulnerability classified as problematic was found in Campcodes Online Job Finder System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/company/index.php. The manipulation of the argument view leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257383.	2024-03-20	3.5	CVE-2024-2683
campcodes -- online_job_finder_system	A vulnerability, which was classified as problematic, has been found in Campcodes Online Job Finder System 1.0. Affected by this issue is some unknown functionality of the file /admin/category/index.php. The manipulation of the argument view leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257384.	2024-03-20	3.5	CVE-2024-2684
campcodes -- online_job_finder_system	A vulnerability, which was classified as problematic, was found in Campcodes Online Job Finder System 1.0. This affects an unknown part of the file /admin/applicants/index.php. The manipulation of the argument view leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257385 was assigned to this vulnerability.	2024-03-20	3.5	CVE-2024-2685
campcodes -- online_job_finder_system	A vulnerability has been found in Campcodes Online Job Finder System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/applicants/controller.php. The manipulation of the argument JOBREGID leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257386 is the identifier assigned to this vulnerability.	2024-03-20	3.5	CVE-2024-2686
campcodes -- online_marriage_registration_system	A vulnerability classified as problematic has been found in Campcodes Online Marriage Registration System 1.0. This affects an unknown part of the file /user/search.php. The manipulation of the argument searchdata leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257607.	2024-03-21	3.5	CVE-2024-2773
campcodes -- online_marriage_registration_system	A vulnerability, which was classified as problematic, has been found in Campcodes Online Marriage Registration System 1.0. This issue affects some unknown processing of the file /user/user-profile.php. The manipulation of the argument lname leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257609 was assigned to this vulnerability.	2024-03-21	3.5	CVE-2024-2775

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
campcodes -- online_marriage_registration_system	A vulnerability was found in Campcodes Online Marriage Registration System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/search.php. The manipulation of the argument searchdata leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257612.	2024-03-22	3.5	CVE-2024-2778
campcodes -- online_marriage_registration_system	A vulnerability was found in Campcodes Online Marriage Registration System 1.0. It has been classified as problematic. This affects an unknown part of the file /admin/application-bwdates-reports-details.php. The manipulation of the argument fromdate leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257613 was assigned to this vulnerability.	2024-03-22	3.5	CVE-2024-2779
campcodes -- online_marriage_registration_system	A vulnerability was found in Campcodes Online Marriage Registration System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/admin-profile.php. The manipulation of the argument adminname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257614 is the identifier assigned to this vulnerability.	2024-03-22	3.5	CVE-2024-2780
campcodes -- online_shopping_system	A vulnerability classified as problematic was found in Campcodes Online Shopping System 1.0. This vulnerability affects unknown code of the file /offersmail.php. The manipulation of the argument email leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257752.	2024-03-23	3.5	CVE-2024-2832
checkmk_gmbh -- checkmk	Invocation of the sqlplus command with sensitive information in the command line in the mk_oracle Checkmk agent plugin before Checkmk 2.3.0b4 (beta), 2.2.0p24, 2.1.0p41 and 2.0.0 (EOL) allows the extraction of this information from the process list.	2024-03-22	3.8	CVE-2024-1742
clickhouse -- clickhouse	ClickHouse is an open-source column-oriented database management system. A bug exists in the cloud ClickHouse offering prior to version 24.0.2.54535 and in github.com/clickhouse/clickhouse version 23.1. Query caching bypasses the role based access controls and the policies being enforced on roles. In affected versions, the query cache only respects separate users, however this is not documented and not expected behavior. People relying on ClickHouse roles can have their access control lists bypassed if they are using query caching. Attackers who have control of a role could guess queries and see data they shouldn't have access to. Version 24.1 of ClickHouse and version 24.0.2.54535 of ClickHouse Cloud contain a patch for this issue. Based on the documentation, role based access control should be enforced regardless if query caching is enabled or not.	2024-03-18	2.4	CVE-2024-22412
ibm -- security_verify_directory	IBM Security Verify Directory 10.0.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 228507.	2024-03-22	2.7	CVE-2022-32756
ilicmiljan -- secure-props	SecureProps is a PHP library designed to simplify the encryption and decryption of property data in objects. A vulnerability in SecureProps version 1.2.0 and 1.2.1 involves a regex failing to detect tags during decryption of encrypted data. This occurs when the encrypted data has been encoded with `NullEncoder` and passed to `TagAwareCipher`, and contains special characters such as `\n`. As a result, the decryption process is skipped since the tags are not detected. This causes the encrypted data to be returned in plain format. The vulnerability affects users who implement `TagAwareCipher` with any base cipher that has `NullEncoder` (not default). The patch for the issue has been released. Users are advised to update to version 1.2.2. As a workaround, one may use the default `Base64Encoder` with the base cipher decorated with `TagAwareCipher` to prevent special characters in the encrypted string from interfering with regex tag detection logic. This workaround is	2024-03-18	2.6	CVE-2024-28864

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	safe but may involve double encoding since `TagAwareCipher` uses `NullEncoder` by default.			
kaspersky -- kaspersky_password_manager_for_windows	Kaspersky has fixed a security issue in Kaspersky Password Manager (KPM) for Windows that allowed a local user to recover the auto-filled credentials from a memory dump when the KPM extension for Google Chrome is used. To exploit the issue, an attacker must trick a user into visiting a login form of a website with the saved credentials, and the KPM extension must autofill these credentials. The attacker must then launch a malware module to steal those specific credentials.	2024-03-22	2.2	CVE-2023-23349
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/users.php. The manipulation of the argument id leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256972. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-17	3.5	CVE-2024-2535
sourcecodester -- product_review_rating_system	A vulnerability, which was classified as problematic, was found in SourceCodester Product Review Rating System 1.0. Affected is an unknown function of the component Rate Product Handler. The manipulation of the argument Your Name/Comment leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257052.	2024-03-17	3.5	CVE-2024-2553
umbraco -- umbraco-cms	Umbraco is an ASP.NET content management system. Umbraco 10 prior to 10.8.4 with access to the native login screen is vulnerable to a possible user enumeration attack. This issue was fixed in version 10.8.5. As a workaround, one may disable the native login screen by exclusively using external logins.	2024-03-20	3.7	CVE-2024-28868
bpftrace -- bpftrace	If kernel headers need to be extracted, bpftrace will attempt to load them from a temporary directory. An unprivileged attacker could use this to force bcc to load compromised linux headers. Linux distributions which provide kernel headers by default are not affected by default.	2024-03-10	2.8	CVE-2024-2313
cloudflare -- quiche	Cloudflare quiche was discovered to be vulnerable to unbounded storage of information related to connection ID retirement, which could lead to excessive resource consumption. Each QUIC connection possesses a set of connection Identifiers (IDs); see RFC 9000 Section 5.1 https://datatracker.ietf.org/doc/html/rfc9000#section-5.1 . Endpoints declare the number of active connection IDs they are willing to support using the active_connection_id_limit transport parameter. The peer can create new IDs using a NEW_CONNECTION_ID frame but must stay within the active ID limit. This is done by retirement of old IDs, the endpoint sends NEW_CONNECTION_ID includes a value in the retire_prior_to field, which elicits a RETIRE_CONNECTION_ID frame as confirmation. An unauthenticated remote attacker can exploit the vulnerability by sending NEW_CONNECTION_ID frames and manipulating the connection (e.g. by restricting the peer's congestion window size) so that RETIRE_CONNECTION_ID frames can only be sent at a slower rate than they are received, leading to storage of information related to connection IDs in an unbounded queue. Quiche versions 0.19.2 and 0.20.1 are the earliest to address this problem. There is no workaround for affected versions.	2024-03-12	3.7	CVE-2024-1410
collaboraonline -- online	Collabora Online is a collaborative online office suite based on LibreOffice technology. Each document in Collabora Online is opened by a separate "Kit" instance in a different "jail" with a unique directory "jailID" name. For security reasons, this directory name is randomly generated and should not be given out to the client. In affected versions of Collabora Online it is possible to use the CELL() function, with the "filename" argument, in the spreadsheet component to get a path which includes this JailID. The impact of this vulnerability in its own is low because it requires to be chained with another vulnerability. Users should upgrade	2024-03-11	2.6	CVE-2024-25114

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to Collabora Online 23.05.9; Collabora Online 22.05.22; Collabora Online 21.11.10 or higher. There are no known workarounds for this vulnerability.			
dell -- poweredge_platform	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain an improper parameter initialization vulnerability. A local low privileged attacker could potentially exploit this vulnerability to read the contents of non-SMM stack memory.	2024-03-13	3.8	CVE-2024-0154
dell -- poweredge_platform	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain an improper parameter initialization vulnerability. A local low privileged attacker could potentially exploit this vulnerability to read the contents of non-SMM stack memory.	2024-03-13	3.8	CVE-2024-0173
directus -- directus	Directus is a real-time API and App dashboard for managing SQL database content. When reaching the /files page, a JWT is passed via GET request. Inclusion of session tokens in URLs poses a security risk as URLs are often logged in various places (e.g., web server logs, browser history). Attackers gaining access to these logs may hijack active user sessions, leading to unauthorized access to sensitive information or actions on behalf of the user. This issue has been addressed in version 10.10.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-12	2.3	CVE-2024-28238
discourse -- discourse	A vulnerability has been found in Surya2Developer Hostel Management Service 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /check_availability.php of the component HTTP POST Request Handler. The manipulation of the argument oldpassword leads to observable response discrepancy. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256891.	2024-03-15	3.7	CVE-2024-2482
ibm -- maximo_application_suite	IBM Maximo Application Suite 8.10, 8.11 and IBM Maximo Asset Management 7.6.1.3 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 255075.	2024-03-13	3.7	CVE-2023-32335
iovisor -- bpf_compiler_collection	If kernel headers need to be extracted, bcc will attempt to load them from a temporary directory. An unprivileged attacker could use this to force bcc to load compromised linux headers. Linux distributions which provide kernel headers by default are not affected by default.	2024-03-10	2.8	CVE-2024-2314
keerti1924 -- secret-coder-php-project	A vulnerability has been found in keerti1924 Secret-Coder-PHP-Project 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /secret_coder.sql. The manipulation leads to inclusion of sensitive information in source code. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256315. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-10	3.7	CVE-2024-2355
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability, which was classified as problematic, has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected by this issue is some unknown functionality of the file home.php. The manipulation of the argument id leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256952. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	3.5	CVE-2024-2515
magesh-k21 -- online-college-event-hall-	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as problematic. This issue affects some unknown processing of the file book_history.php. The manipulation of the argument id leads to cross site scripting. The attack may be initiated remotely. The exploit has been	2024-03-16	3.5	CVE-2024-2518

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
reservation-system	disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256955. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been classified as problematic. Affected is an unknown function of the file navbar.php. The manipulation of the argument id leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256956. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	3.5	CVE-2024-2519
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/bookdate.php. The manipulation of the argument id leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-256958 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	3.5	CVE-2024-2521
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability classified as problematic was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. This vulnerability affects unknown code of the file /admin/booktime.php. The manipulation of the argument id leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256960. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	3.5	CVE-2024-2523
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability, which was classified as problematic, was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected is an unknown function of the file /admin/receipt.php. The manipulation of the argument id leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-256962 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	3.5	CVE-2024-2525
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/rooms.php. The manipulation of the argument id leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256963. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	3.5	CVE-2024-2526
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/update-rooms.php. The manipulation of the argument id leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256967. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	3.5	CVE-2024-2530
magesh-k21 -- online-college-event-hall-reservation-system	A vulnerability, which was classified as problematic, has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected by this issue is some unknown functionality of the file /admin/update-users.php. The manipulation of the argument id leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-256970 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-16	3.5	CVE-2024-2533

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mattermost -- mattermost	Resource Exhaustion in Mattermost Server versions 8.1.x before 8.1.10 fails to limit the size of the payload that can be read and parsed allowing an attacker to send a very large email payload and crash the server.	2024-03-15	3.1	CVE-2024-28053
mattermost -- mattermost_mobile	Uncontrolled Resource Consumption in Mattermost Mobile versions before 2.13.0 fails to limit the size of the code block that will be processed by the syntax highlighter, allowing an attacker to send a very large code block and crash the mobile app.	2024-03-15	3.5	CVE-2024-24975
mha_sistemas -- armhazena	A vulnerability classified as problematic has been found in MHA Sistemas arMHAzena 9.6.0.0. This affects an unknown part of the component Cadastro Page. The manipulation of the argument Query leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256887. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-15	3.5	CVE-2024-2479
microsoft -- microsoft_edge_for_android	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2024-03-14	3.9	CVE-2024-26246
n/a -- eve-ng	A vulnerability was found in EVE-NG 5.0.1-13 and classified as problematic. Affected by this issue is some unknown functionality of the component Lab Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-256442 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-03-12	2.4	CVE-2024-2391
n/a -- intel(r)_local_manageability_service_software	Insertion of sensitive information into log file for some Intel(R) Local Manageability Service software before version 2316.5.1.2 may allow an authenticated user to potentially enable information disclosure via local access.	2024-03-14	3.3	CVE-2023-27502
n/a -- musicshelf	A vulnerability classified as problematic has been found in Musicshelf 1.0/1.1 on Android. Affected is an unknown function of the file androidmanifest.xml of the component Backup Handler. The manipulation leads to exposure of backup file to an unauthorized control sphere. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256320.	2024-03-10	1.8	CVE-2024-2364
n/a -- musicshelf	A vulnerability classified as problematic was found in Musicshelf 1.0/1.1 on Android. Affected by this vulnerability is an unknown functionality of the file io\fabric\sdk\android\services\network\PinningTrustManager.java of the component SHA-1 Handler. The manipulation leads to password hash with insufficient computational effort. It is possible to launch the attack on the physical device. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-256321 was assigned to this vulnerability.	2024-03-11	1.6	CVE-2024-2365
n/a -- quarkus	A vulnerability was found in Quarkus. In certain conditions related to the CI process, git credentials could be inadvertently published, which could put the git repository at risk.	2024-03-13	3.5	CVE-2024-1979
papercut -- papercut_ng,_papercut_mf	This vulnerability potentially allows files on a PaperCut NG/MF server to be exposed using a specifically formed payload against the impacted API endpoint. The attacker must carry out some reconnaissance to gain knowledge of a system token. This CVE only affects Linux and macOS PaperCut NG/MF servers.	2024-03-14	3.1	CVE-2024-1221

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
peering-manager -- peering-manager	Peering Manager is a BGP session management tool. In Peering Manager <=1.8.2, it is possible to redirect users to an arbitrary page using a crafted url. As a result users can be redirected to an unexpected location. This issue has been addressed in version 1.8.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-03-12	3.5	CVE-2024-28113