BULLETIN (SB24-281)

VULNERABILITY SUMMARY FOR THE WEEK OF

30TH SEPTEMBER, 2024

Bulletin (SB24-281)
Vulnerability Summary for the Week of September 24, 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
123.chat--123.chat - Video Chat	The 123.chat - Video Chat plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 1.3.1 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 page.	2024-10-01	7.2	CVE-2024-7869 security@wordfence.com security@wordfence.com
ABCApp Creator--ABCApp Creator	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ABCApp Creator allows PHP Local File Inclusion.This issue affects ABCApp Creator: from n/a through 1.1.2.	2024-10-05	8.1	CVE-2024-44023 audit@patchstack.com
apache -- lucene	Deserialization of Untrusted Data vulnerability in Apache Lucene Replicator. This issue affects Apache Lucene's replicator module: from 4.4.0 before 9.12.0. The deprecated org.apache.lucene.replicator.http package is affected. The org.apache.lucene.replicator.nrt package is not affected. Users are recommended to upgrade to version 9.12.0, which fixes the issue. Java serialization filters (such as -Djdk.serialFilter='!*' on the commandline) can mitigate the issue on vulnerable versions without impacting functionality.	2024-09-30	8	CVE-2024-45772 security@apache.org
Apache Software Foundation--Apache Avro Java SDK	Schema parsing in the Java SDK of Apache Avro 1.11.3 and previous versions allows bad actors to execute arbitrary code. Users are recommended to upgrade to version 1.11.4 or 1.12.0, which fix this issue.	2024-10-03	7.3	CVE-2024-47561 security@apache.org
Apple--iTunes for Windows	A logic issue was addressed with improved restrictions. This issue is fixed in iTunes 12.13.3 for Windows. A local attacker may be able to elevate their privileges.	2024-10-02	8.4	CVE-2024-44193 product-security@apple.com
async-graphql--async-graphql	async-graphql is a GraphQL server library implemented in Rust. async-graphql before 7.0.10 does not limit the number of directives for a field. This can lead to Service Disruption, Resource Exhaustion, and User Experience Degradation. This vulnerability is fixed in 7.0.10.	2024-10-03	7.5	CVE-2024-47614 security-advisories@github.com security-advisories@github.com
Autodesk--Navisworks Freedom	A maliciously crafted DWFX file, when parsed in w3dtk.dll through Autodesk Navisworks, can force an Out-of-Bounds Read. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	2024-09-30	7.8	CVE-2024-7670 psirt@autodesk.com
Autodesk--Navisworks Freedom	A maliciously crafted DWFX file, when parsed in dwfcore.dll through Autodesk Navisworks, can force an Out-of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	2024-09-30	7.8	CVE-2024-7671 psirt@autodesk.com
Autodesk--Navisworks Freedom	A maliciously crafted DWF file, when parsed in dwfcore.dll through Autodesk Navisworks, can force an Out-of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	2024-09-30	7.8	CVE-2024-7672 psirt@autodesk.com
Autodesk--Navisworks Freedom	A maliciously crafted DWFX file, when parsed in w3dtk.dll through Autodesk Navisworks, can force a Heap-based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash or execute arbitrary code in the context of the current process.	2024-09-30	7.8	CVE-2024-7673 psirt@autodesk.com
Autodesk--Navisworks Freedom	A maliciously crafted DWF file, when parsed in dwfcore.dll through Autodesk Navisworks, can force a Heap-based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash or execute arbitrary code in the context of the current process.	2024-09-30	7.8	CVE-2024-7674 psirt@autodesk.com
Autodesk--Navisworks	A maliciously crafted DWF file, when parsed in w3dtk.dll through Autodesk Navisworks, can force a Use-After-Free. A malicious actor can leverage this	2024-09-30	7.8	CVE-2024-7675 psirt@autodesk.c

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Freedom	vulnerability to cause a crash or execute arbitrary code in the context of the current process.			om
AVG/Avast--Antivirus	The AVGUI.exe of AVG/Avast Antivirus before versions before 24.1 can allow a local attacker to escalate privileges via an COM hijack in a time-of-check to time-of-use (TOCTOU) when self protection is disabled.	2024-10-03	7.5	CVE-2024-5803 security@nortonlifelock.com
BannerSky--BSK Forms Blacklist	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BannerSky BSK Forms Blacklist allows Reflected XSS.This issue affects BSK Forms Blacklist: from n/a through 3.8.1.	2024-10-05	7.1	CVE-2024-47624 audit@patchstack.com
Basix--NEX-Forms Ultimate Form Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Basix NEX-Forms - Ultimate Form Builder allows Reflected XSS.This issue affects NEX-Forms - Ultimate Form Builder: from n/a through 8.7.3.	2024-10-05	7.1	CVE-2024-47389 audit@patchstack.com
Bit Apps--Bit Form Contact Form Plugin	Unrestricted Upload of File with Dangerous Type vulnerability in Bit Apps Bit Form - Contact Form Plugin allows Code Injection.This issue affects Bit Form - Contact Form Plugin: from n/a through 2.13.10.	2024-10-05	8	CVE-2024-47319 audit@patchstack.com
Bit Form--Bit Form Contact Form Plugin	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Bit Form Bit Form - Contact Form Plugin allows Stored XSS.This issue affects Bit Form - Contact Form Plugin: from n/a through 2.13.10.	2024-10-06	7.1	CVE-2024-47301 audit@patchstack.com
Booking Algorithms--BA Book Everything	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Booking Algorithms BA Book Everything allows Reflected XSS.This issue affects BA Book Everything: from n/a through 1.6.20.	2024-10-06	7.1	CVE-2024-47360 audit@patchstack.com
cagdasdag--KB Support WordPress Help Desk and Knowledge Base	The KB Support - WordPress Help Desk and Knowledge Base plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check on several functions in all versions up to, and including, 1.6.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to perform multiple administrative actions, such as replying to arbitrary tickets, updating the status of any post, deleting any post, adding notes to tickets, flagging or unflagging tickets, and adding or removing ticket participants.	2024-10-01	8.1	CVE-2024-8548 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
Canonical Ltd.--Authd	Authd PAM module before version 0.3.5 can allow broker-managed users to impersonate any other user managed by the same broker and perform any PAM operation with it, including authenticating as them.	2024-10-03	8.8	CVE-2024-9313 security@ubuntu.com security@ubuntu

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				.com
Canonical Ltd.--Juju	JUJU_CONTEXT_ID is a predictable authentication secret. On a Juju machine (non-Kubernetes) or Juju charm container (on Kubernetes), an unprivileged user in the same network namespace can connect to an abstract domain socket and guess the JUJU_CONTEXT_ID value. This gives the unprivileged user access to the same information and tools as the Juju charm.	2024-10-02	8.7	CVE-2024-7558 security@ubuntu.com security@ubuntu.com
Canonical Ltd.--Juju	Vulnerable juju introspection abstract UNIX domain socket. An abstract UNIX domain socket responsible for introspection is available without authentication locally to network namespace users. This enables denial of service attacks.	2024-10-02	7.9	CVE-2024-8038 security@ubuntu.com security@ubuntu.com
Cavok--Cavok	Cavok - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	2024-10-06	9.8	CVE-2024-45249 cna@cyber.gov.il
Chart Builder Team--Chartify	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Chart Builder Team Chartify allows Reflected XSS.This issue affects Chartify: from n/a through 2.7.6.	2024-10-06	7.1	CVE-2024-47347 audit@patchstack.com
Cisco--Cisco Data Center Network Manager	A vulnerability in the REST API and web UI of Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an authenticated, low-privileged, remote attacker to perform a command injection attack against an affected device. This vulnerability is due to improper user authorization and insufficient validation of command arguments. An attacker could exploit this vulnerability by submitting crafted commands to an affected REST API endpoint or through the web UI. A successful exploit could allow the attacker to execute arbitrary commands on the CLI of a Cisco NDFC-managed device with network-admin privileges. Note: This vulnerability does not affect Cisco NDFC when it is configured for storage area network (SAN) controller deployment.	2024-10-02	9.9	CVE-2024-20432 ykramarz@cisco.com
Cisco--Cisco Data Center Network Manager	A vulnerability in Cisco Nexus Dashboard Fabric Controller (NDFC) could allow an authenticated, remote attacker with low privileges to execute arbitrary code on an affected device. This vulnerability is due to improper path validation. An attacker could exploit this vulnerability by using the Secure Copy Protocol (SCP) to upload malicious code to an affected device using path traversal techniques. A successful exploit could allow the attacker to execute arbitrary code in a specific container with the privileges of root.	2024-10-02	8.8	CVE-2024-20449 ykramarz@cisco.com
Cisco--Cisco Meraki MX Firmware	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.	2024-10-02	8.6	CVE-2024-20498 ykramarz@cisco.com
Cisco--Cisco Meraki MX Firmware	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an	2024-10-02	8.6	CVE-2024-20499 ykramarz@cisco.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.			
Cisco--Cisco Meraki MX Firmware	Multiple vulnerabilities in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. These vulnerabilities are due to insufficient validation of client-supplied parameters while establishing an SSL VPN session. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to restart, resulting in the failure of the established SSL VPN connections and forcing remote users to initiate a new VPN connection and reauthenticate. A sustained attack could prevent new SSL VPN connections from being established. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.	2024-10-02	8.6	CVE-2024-20501 ykramarz@cisco.com
Cisco--Cisco Small Business RV Series Router Firmware	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin.	2024-10-02	8.8	CVE-2024-20393 ykramarz@cisco.com
code-projects -- restaurant_reservation_system	A vulnerability was found in code-projects Restaurant Reservation System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /addcompany.php. The manipulation of the argument company leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-01	9.8	CVE-2024-9359 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
code-projects -- restaurant_reservation_system	A vulnerability was found in code-projects Restaurant Reservation System 1.0. It has been classified as critical. This affects an unknown part of the file /updatebal.php. The manipulation of the argument company leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-01	9.8	CVE-2024-9360 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
CodePeople--CP Polls	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CodePeople CP Polls allows Reflected XSS.This issue affects CP Polls: from n/a through 1.0.74.	2024-10-06	7.1	CVE-2024-47297 audit@patchstack.com
CodeRevolution--Echo RSS Feed Post Generator	The Echo RSS Feed Post Generator plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 5.4.6. This is due to the plugin not properly restricting the roles that can set during registration through the echo_check_post_header_sent() function. This makes it possible for unauthenticated attackers to register as an administrator.	2024-10-01	9.8	CVE-2024-9265 security@wordfence.com security@wordfence.com
Codezips--Online Shopping Portal	A vulnerability was found in Codezips Online Shopping Portal 1.0. It has been classified as critical. Affected is an unknown function of the file index.php. The manipulation of the argument username leads to sql	2024-10-03	7.3	CVE-2024-9460 cna@vuldb.com cna@vuldb.com cna@vuldb.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.			cna@vuldb.com
Copy Content Protection Team--Secure Copy Content Protection and Content Locking	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Copy Content Protection Team Secure Copy Content Protection and Content Locking allows Stored XSS.This issue affects Secure Copy Content Protection and Content Locking: from n/a through 4.2.3.	2024-10-06	7.1	CVE-2024-47306 audit@patchstack.com
Copyscape / Indigo Stream Technologies--Copyscape Premium	Cross-Site Request Forgery (CSRF) vulnerability in Copyscape / Indigo Stream Technologies Copyscape Premium allows Stored XSS.This issue affects Copyscape Premium: from n/a through 1.3.6.	2024-10-05	7.1	CVE-2024-47644 audit@patchstack.com
CubeWP--CubeWP Forms All-in-One Form Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CubeWP CubeWP Forms - All-in-One Form Builder allows Stored XSS.This issue affects CubeWP Forms - All-in-One Form Builder: from n/a through 1.1.1.	2024-10-06	7.1	CVE-2024-47300 audit@patchstack.com
D-Link--DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been declared as critical. This vulnerability affects the function formSetDomainFilter of the file /goform/formSetDomainFilter. The manipulation of the argument curTime leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-04	8.8	CVE-2024-9514 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. This affects the function formSetQoS of the file /goform/formSetQoS. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-04	8.8	CVE-2024-9515 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability has been found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This vulnerability affects the function formAdvanceSetup of the file /goform/formAdvanceSetup. The manipulation of the argument webpage leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-05	8.8	CVE-2024-9532 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This issue affects the function formDeviceReboot of the file /goform/formDeviceReboot. The manipulation of the argument next_page leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-05	8.8	CVE-2024-9533 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. Affected is the function formEasySetPassword of the file /goform/formEasySetPassword. The manipulation of the argument curTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-05	8.8	CVE-2024-9534 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been declared as critical. Affected by this vulnerability is the function formEasySetupWWConfig of the file /goform/formEasySetupWWConfig. The manipulation of the argument curTime leads to buffer overflow. The	2024-10-05	8.8	CVE-2024-9535 cna@vuldb.com cna@vuldb.com cna@vuldb.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attack can be launched remotely. The exploit has been disclosed to the public and may be used.			cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This issue affects the function formEasySetupWizard/formEasySetupWizard2 of the file /goform/formEasySetupWizard. The manipulation of the argument curTime leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-06	8.8	CVE-2024-9549 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. Affected is the function formLogDnsquery of the file /goform/formLogDnsquery. The manipulation of the argument curTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-06	8.8	CVE-2024-9550 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been declared as critical. Affected by this vulnerability is the function formSetWanL2TP of the file /goform/formSetWanL2TP. The manipulation of the argument webpage leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-06	8.8	CVE-2024-9551 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been rated as critical. Affected by this issue is the function formSetWanNonLogin of the file /goform/formSetWanNonLogin. The manipulation of the argument webpage leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-06	8.8	CVE-2024-9552 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability classified as critical has been found in D-Link DIR-605L 2.13B01 BETA. This affects the function formdumpeasysetup of the file /goform/formdumpeasysetup. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-06	8.8	CVE-2024-9553 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability, which was classified as critical, has been found in D-Link DIR-605L 2.13B01 BETA. Affected by this issue is the function formSetEasy_Wizard of the file /goform/formSetEasy_Wizard. The manipulation of the argument curTime leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-06	8.8	CVE-2024-9555 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability, which was classified as critical, was found in D-Link DIR-605L 2.13B01 BETA. This affects the function formSetEnableWizard of the file /goform/formSetEnableWizard. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-06	8.8	CVE-2024-9556 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability has been found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This vulnerability affects the function formSetWanPPPoE of the file /goform/formSetWanPPPoE. The manipulation of the argument webpage leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-06	8.8	CVE-2024-9557 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
D-Link--DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA and classified as critical. This issue affects the function formSetWanPPTP of the file /goform/formSetWanPPTP. The manipulation of the argument webpage leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-06	8.8	CVE-2024-9558 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01 BETA. It has been classified as critical. Affected is the function formWlanSetup of the file /goform/formWlanSetup. The manipulation of the argument webpage leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-06	8.8	CVE-2024-9559 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability classified as critical has been found in D-Link DIR-605L 2.13B01 BETA. This affects the function formSetWAN_Wizard51/formSetWAN_Wizard52. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-10-06	8.8	CVE-2024-9561 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
D-Link--DIR-605L	A vulnerability classified as critical was found in D-Link DIR-605L 2.13B01 BETA. This vulnerability affects the function formSetWizard1/formSetWizard2. The manipulation of the argument curTime leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-10-06	8.8	CVE-2024-9562 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
David Garlitz--viala	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in David Garlitz viala allows Reflected XSS.This issue affects viala: from n/a through 1.3.1.	2024-10-06	7.1	CVE-2024-44029 audit@patchstack.com
decidim--decidim	Decidim is a participatory democracy framework. The version control feature used in resources is subject to potential XSS attack through a malformed URL. This vulnerability is fixed in 0.27.8.	2024-10-01	7.1	CVE-2024-41673 security-advisories@github.com security-advisories@github.com
dejanmarkovic--Social Web Suite Social Media Auto Post, Social Media Auto Publish	The Social Web Suite - Social Media Auto Post, Social Media Auto Publish plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 4.1.11 via the download_log function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	2024-10-03	7.5	CVE-2024-8352 security@wordfence.com security@wordfence.com security@wordfence.com
Delta Electronics--DIAEnergie	Delta Electronics DIAEnergie is vulnerable to an SQL injection in the script AM_RegReport.aspx. An unauthenticated attacker may be able to exploit this issue to obtain records contained in the targeted product.	2024-10-03	9.8	CVE-2024-43699 ics-cert@hq.dhs.gov ics-cert@hq.dhs.gov
Delta Electronics--DIAEnergie	Delta Electronics DIAEnergie is vulnerable to an SQL injection in the script Handler_CFG.ashx. An authenticated attacker may be able to exploit this issue to cause delay in the targeted product.	2024-10-03	8.8	CVE-2024-42417 ics-cert@hq.dhs.gov ics-

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				cert@hq.dhs.gov
Diebold Nixdorf--Vynamic View prior to v5.9.5	Diebold Nixdorf - CWE-427: Uncontrolled Search Path Element	2024-10-06	7.3	CVE-2024-45246 cna@cyber.gov.il
Diebold Nixdorf--Vynamic View prior	Diebold Nixdorf - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	2024-10-06	7.8	CVE-2024-45245 cna@cyber.gov.il
elabftw--elabftw	eLabFTW is an open source electronic lab notebook for research labs. In the context of eLabFTW, an administrator is a user account with certain privileges to manage users and content in their assigned team/teams. A user may be an administrator in one team and a regular user in another. The vulnerability allows a regular user to become administrator of a team where they are a member, under a reasonable configuration. Additionally, in eLabFTW versions subsequent to v5.0.0, the vulnerability may allow an initially unauthenticated user to gain administrative privileges over an arbitrary team. The vulnerability does not affect system administrator status. Users should upgrade to version 5.1.0. System administrators are advised to turn off local user registration, saml_team_create and not allow administrators to import users into teams, unless strictly required.	2024-10-01	8.6	CVE-2024-25632 security-advisories@github.com
elabftw--elabftw	eLabFTW is an open source electronic lab notebook for research labs. An incorrect permission check has been found that could allow an authenticated user to access several kinds of otherwise restricted information. If anonymous access is allowed (something disabled by default), this extends to anyone. Users are advised to upgrade to at least version 5.1.0. System administrators can disable anonymous access in the System configuration panel.	2024-10-01	7.5	CVE-2024-45408 security-advisories@github.com
Elsight--Halo version 11.7.1.5	Elsight - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	2024-10-06	9.8	CVE-2024-45251 cna@cyber.gov.il
Elsight--Halo version 11.7.1.5	Elsight - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	2024-10-06	9.8	CVE-2024-45252 cna@cyber.gov.il
Esri--Portal	There is a local file inclusion vulnerability in Esri Portal for ArcGIS 11.2. 11.1, 11.0 and 10.9.1 that may allow a remote, unauthenticated attacker to craft a URL that could potentially disclose sensitive configuration information by reading internal files.	2024-10-04	7.5	CVE-2024-38040 psirt@esri.com
Ex-Themes--WP Timeline Vertical and Horizontal timeline plugin	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ex-Themes WP Timeline - Vertical and Horizontal timeline plugin allows PHP Local File Inclusion.This issue affects WP Timeline - Vertical and Horizontal timeline plugin: from n/a through 3.6.7.	2024-10-05	8.1	CVE-2024-47323 audit@patchstack.com
Ex-Themes--WP Timeline Vertical and Horizontal timeline plugin	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ex-Themes WP Timeline - Vertical and Horizontal timeline plugin allows Reflected XSS.This issue affects WP Timeline - Vertical and Horizontal timeline plugin: from n/a through 3.6.7.	2024-10-06	7.1	CVE-2024-47322 audit@patchstack.com
Ex-Themes--WP Timeline Vertical and Horizontal timeline plugin	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Ex-Themes WP Timeline - Vertical and Horizontal timeline plugin allows PHP Local File Inclusion.This issue affects WP Timeline - Vertical and Horizontal timeline plugin: from n/a through 3.6.7.	2024-10-05	7.5	CVE-2024-47324 audit@patchstack.com
Eyal Fitoussi--GEO my WordPress	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Eyal Fitoussi GEO my WordPress allows Reflected XSS.This issue affects GEO my WordPress: from n/a through 4.5.0.3.	2024-10-06	7.1	CVE-2024-47327 audit@patchstack.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eyecix--JobSearch	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in eyecix JobSearch allows Reflected XSS.This issue affects JobSearch: from n/a through 2.5.9.	2024-10-05	7.1	CVE-2024-47394 audit@patchstack.com
Foxit--Foxit Reader	A use-after-free vulnerability exists in the way Foxit Reade 2024.1.0.23997 handles a checkbox field object. A specially crafted Javascript code inside a malicious PDF document can trigger this vulnerability, which can lead to memory corruption and result in arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled.	2024-10-02	8.8	CVE-2024-28888 talos-cna@cisco.com talos-cna@cisco.com
GNOME Project--G Structured File Library (libgsf)	An integer overflow vulnerability exists in the Compound Document Binary File format parser of the GNOME Project G Structured File Library (libgsf) version v1.14.52. A specially crafted file can result in an integer overflow when processing the directory from the file that allows for an out-of-bounds index to be used when reading and writing to an array. This can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	2024-10-03	8.4	CVE-2024-36474 talos-cna@cisco.com talos-cna@cisco.com
GNOME Project--G Structured File Library (libgsf)	An integer overflow vulnerability exists in the Compound Document Binary File format parser of v1.14.52 of the GNOME Project G Structured File Library (libgsf). A specially crafted file can result in an integer overflow that allows for a heap-based buffer overflow when processing the sector allocation table. This can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	2024-10-03	8.4	CVE-2024-42415 talos-cna@cisco.com talos-cna@cisco.com
Google--Android	According to the researcher: "The TLS connections are encrypted against tampering or eavesdropping. However, the application does not validate the server certificate properly while initializing the TLS connection. This allows for a network attacker to intercept the connection and read the data. The attacker could the either send the client a malicious response, or forward the (possibly modified) data to the real server."	2024-10-02	9.8	CVE-2024-44097 dsap-vuln-management@google.com
hahncgdev--WP Easy Gallery WordPress Gallery Plugin	The WP Easy Gallery - WordPress Gallery Plugin plugin for WordPress is vulnerable to time-based SQL Injection via the 'key' parameter in all versions up to, and including, 4.8.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-10-01	8.8	CVE-2024-9018 security@wordfence.com security@wordfence.com security@wordfence.com
HP, Inc.--HP One Agent Software	A potential security vulnerability has been identified in the HP One Agent for certain HP PC products, which might allow for escalation of privilege. HP is releasing software updates to mitigate this potential vulnerability.	2024-10-02	8	CVE-2024-8733 hp-security-alert@hp.com
idurar--idurar-erp-crm	IDURAR is open source ERP CRM accounting invoicing software. The vulnerability exists in the corePublicRouter.js file. Using the reference usage here, it is identified that the public endpoint is accessible to an unauthenticated user. The user's input is directly appended to the join statement without additional checks. This allows an attacker to send URL encoded malicious payload. The directory structure can be escaped to read system files by adding an encoded string (payload) at subpath location.	2024-10-04	7.5	CVE-2024-47769 security-advisories@github.com security-advisories@github.com
ILLID--Share This Image	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ILLID Share This Image allows Reflected XSS.This issue affects Share This Image: from n/a through 2.01.	2024-10-06	7.1	CVE-2024-47326 audit@patchstack.com
Innate Images LLC--VR Calendar	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Innate Images LLC VR Calendar allows PHP Local File Inclusion.This issue affects VR Calendar: from n/a through 2.4.0.	2024-10-05	7.5	CVE-2024-44013 audit@patchstack.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Istmo Plugins--Instant Chat Floating Button for WordPress Websites	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Istmo Plugins Instant Chat Floating Button for WordPress Websites allows PHP Local File Inclusion.This issue affects Instant Chat Floating Button for WordPress Websites: from n/a through 1.0.5.	2024-10-05	7.5	CVE-2024-44018 audit@patchstack.com
James Ward--WP Mail Catcher	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in James Ward WP Mail Catcher allows Reflected XSS.This issue affects WP Mail Catcher: from n/a through 2.1.9.	2024-10-06	7.1	CVE-2024-47339 audit@patchstack.com
Jenkins Project--Jenkins OpenId Connect Authentication Plugin	Jenkins OpenId Connect Authentication Plugin 4.354.v321ce67a_1de8 and earlier does not check the `aud` (Audience) claim of an ID Token, allowing attackers to subvert the authentication flow, potentially gaining administrator access to Jenkins.	2024-10-02	8.1	CVE-2024-47806 jenkinsci-cert@googlegroups.com
Jenkins Project--Jenkins OpenId Connect Authentication Plugin	Jenkins OpenId Connect Authentication Plugin 4.354.v321ce67a_1de8 and earlier does not check the `iss` (Issuer) claim of an ID Token, allowing attackers to subvert the authentication flow, potentially gaining administrator access to Jenkins.	2024-10-02	8.1	CVE-2024-47807 jenkinsci-cert@googlegroups.com
JTEKT ELECTRONICS CORPORATION--Kostac PLC Programming Software (Former name: Koyo PLC Programming Software)	Out-of-bounds write vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC Programming Software) Version 1.6.14.0 and earlier. Having a user open a specially crafted project file which was saved using Kostac PLC Programming Software Version 1.6.9.0 and earlier may cause a denial-of-service (DoS) condition, arbitrary code execution, and/or information disclosure because the issues exist in parsing of KPP project files.	2024-10-03	7.8	CVE-2024-47134 vultures@jpcert.or.jp vultures@jpcert.or.jp vultures@jpcert.or.jp
JTEKT ELECTRONICS CORPORATION--Kostac PLC Programming Software (Former name: Koyo PLC Programming Software)	Stack-based buffer overflow vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC Programming Software) Version 1.6.14.0 and earlier. Having a user open a specially crafted project file which was saved using Kostac PLC Programming Software Version 1.6.9.0 and earlier may cause a denial-of-service (DoS) condition, arbitrary code execution, and/or information disclosure because the issues exist in parsing of KPP project files.	2024-10-03	7.8	CVE-2024-47135 vultures@jpcert.or.jp vultures@jpcert.or.jp vultures@jpcert.or.jp
JTEKT ELECTRONICS CORPORATION--Kostac PLC Programming Software (Former name: Koyo PLC Programming Software)	Out-of-bounds read vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC Programming Software) Version 1.6.14.0 and earlier. Having a user open a specially crafted project file which was saved using Kostac PLC Programming Software Version 1.6.9.0 and earlier may cause a denial-of-service (DoS) condition, arbitrary code execution, and/or information disclosure because the issues exist in parsing of KPP project files.	2024-10-03	7.8	CVE-2024-47136 vultures@jpcert.or.jp vultures@jpcert.or.jp vultures@jpcert.or.jp
Lester GaMerZ Chan--WP-DownloadManag	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Lester 'GaMerZ' Chan WP-DownloadManager allows Reflected XSS.This issue affects WP-DownloadManager: from n/a through 1.68.8.	2024-10-06	7.1	CVE-2024-47341 audit@patchstack.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
er				
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Alert Transports" feature allows authenticated users to inject arbitrary JavaScript through the "Details" section (which contains multiple fields depending on which transport is selected at that moment). This vulnerability can lead to the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and allowing unauthorized actions. This vulnerability is fixed in 24.9.0.	2024-10-01	7.5	CVE-2024-47523 security-advisories@github.com security-advisories@github.com security-advisories@github.com
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. User with Admin role can create a Device Groups, the application did not properly sanitize the user input in the Device Groups name, when user see the detail of the Device Group, if java script code is inside the name of the Device Groups, its will be trigger. This vulnerability is fixed in 24.9.0.	2024-10-01	7.2	CVE-2024-47524 security-advisories@github.com security-advisories@github.com
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Alert Rules" feature allows authenticated users to inject arbitrary JavaScript through the "Title" field. This vulnerability can lead to the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and allowing unauthorized actions. This vulnerability is fixed in 24.9.0.	2024-10-01	7.5	CVE-2024-47525 security-advisories@github.com security-advisories@github.com security-advisories@github.com
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Device Dependencies" feature allows authenticated users to inject arbitrary JavaScript through the device name ("hostname" parameter). This vulnerability can lead to the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and allowing unauthorized actions. This vulnerability is fixed in 24.9.0.	2024-10-01	7.5	CVE-2024-47527 security-advisories@github.com security-advisories@github.com
Linear--eMerge e3-Series	The Linear eMerge e3-Series through version 1.00-07 is vulnerable to an OS command injection vulnerability. A remote and unauthenticated attacker can execute arbitrary OS commands via the login_id parameter when invoking the forgot_password functionality over HTTP.	2024-10-02	9.8	CVE-2024-9441 disclosure@vulncheck.com disclosure@vulncheck.com
LiteSpeed Technologies--LiteSpeed Cache	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LiteSpeed Technologies LiteSpeed Cache allows Stored XSS.This issue affects LiteSpeed Cache: from n/a through 6.5.0.2.	2024-10-05	7.1	CVE-2024-47374 audit@patchstack.com
Mark Steadman--Podiant	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Mark Steadman Podiant allows PHP Local File Inclusion.This issue affects Podiant: from n/a through 1.1.	2024-10-05	7.5	CVE-2024-44016 audit@patchstack.com
Martin Greenwood--WPSPX	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Martin Greenwood WPSPX allows PHP Local File Inclusion.This issue affects WPSPX: from n/a through 1.0.2.	2024-10-05	7.5	CVE-2024-44034 audit@patchstack.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Mestres do WP--Checkout Mestres WP	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Mestres do WP Checkout Mestres WP allows PHP Local File Inclusion.This issue affects Checkout Mestres WP: from n/a through 8.6.	2024-10-02	7.2	CVE-2024-44030 audit@patchstack.com
MinHyeong Lim--MH Board	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in MinHyeong Lim MH Board allows PHP Local File Inclusion.This issue affects MH Board: from n/a through 1.3.2.1.	2024-10-02	7.5	CVE-2024-44017 audit@patchstack.com
Mozilla--Firefox	A compromised content process could have allowed for the arbitrary loading of cross-origin pages. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	9.8	CVE-2024-9392 security@mozilla.org security@mozilla.org security@mozilla.org security@mozilla.org security@mozilla.org security@mozilla.org security@mozilla.org
Mozilla--Firefox	Memory safety bugs present in Firefox 130, Firefox ESR 115.15, Firefox ESR 128.2, and Thunderbird 128.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	9.8	CVE-2024-9401 security@mozilla.org security@mozilla.org security@mozilla.org security@mozilla.org security@mozilla.org security@mozilla.org
Mozilla--Firefox	Memory safety bugs present in Firefox 130, Firefox ESR 128.2, and Thunderbird 128.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	9.8	CVE-2024-9402 security@mozilla.org security@mozilla.org security@mozilla.org security@mozilla.org security@mozilla.org
Mozilla--Firefox	It is currently unknown if this issue is exploitable but a condition may arise where the structured clone of certain objects could lead to memory corruption. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	8.8	CVE-2024-9396 security@mozilla.org security@mozilla.org security@mozilla.org security@mozilla.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				security@mozilla.org
Mozilla--Firefox	A potential memory corruption vulnerability could be triggered if an attacker had the ability to trigger an OOM at a specific moment during JIT compilation. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	2024-10-01	8.8	CVE-2024-9400 security@mozilla.org security@mozilla.org security@mozilla.org security@mozilla.org security@mozilla.org
Mozilla--Firefox	Memory safety bugs present in Firefox 130. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 131 and Thunderbird < 131.	2024-10-01	7.3	CVE-2024-9403 security@mozilla.org security@mozilla.org security@mozilla.org
Multi-DNC--Multi-DNC	Multi-DNC - CWE-35: Path Traversal: '.../...//'	2024-10-06	7.5	CVE-2024-45248 cna@cyber.gov.il
n/a--n/a	An issue was discovered in Atos Eviden iCare 2.7.1 through 2.7.11. The application exposes a web interface locally. In the worst-case scenario, if the application is remotely accessible, it allows an attacker to execute arbitrary commands with system privilege on the endpoint hosting the application, without any authentication.	2024-09-30	10	CVE-2024-42017 cve@mitre.org cve@mitre.org
n/a--n/a	The WebDAV service in Infinera TNMS (Transcend Network Management System) 19.10.3 allows a low-privileged remote attacker to conduct unauthorized file operations, because of execution with unnecessary privileges.	2024-10-01	9	CVE-2024-25660 cve@mitre.org
n/a--n/a	A vulnerability in Kaiten version 57.131.12 and earlier allows attackers to bypass the PIN code authentication mechanism. The application requires users to input a 6-digit PIN code sent to their email for authorization after entering their login credentials. However, the request limiting mechanism can be easily bypassed, enabling attackers to perform a brute force attack to guess the correct PIN and gain unauthorized access to the application.	2024-10-01	9.8	CVE-2024-41276 cve@mitre.org cve@mitre.org
n/a--n/a	A vulnerability in the legacy chat component of Mitel MiContact Center Business through 10.1.0.4 could allow an unauthenticated attacker to conduct an unauthorized access attack due to inadequate access control checks. A successful exploit requires user interaction and could allow an attacker to access sensitive information and send unauthorized messages during an active chat session.	2024-10-01	9.1	CVE-2024-42514 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	FileSender before 2.49 allows server-side template injection (SSTI) for retrieving credentials.	2024-10-02	9.8	CVE-2024-45186 cve@mitre.org
n/a--n/a	Sourcecodester Online Medicine Ordering System 1.0 is vulnerable to Incorrect Access Control. There is a lack of authorization checks for admin operations. Specifically, an attacker can perform admin-level actions without possessing a valid session token. The application does not verify whether the user is logged in as an admin or even check for a session token at all.	2024-09-30	9.8	CVE-2024-46293 cve@mitre.org
n/a--n/a	An issue was discovered in Infinera hiT 7300 5.60.50. Cleartext storage of sensitive password in firmware update packages allows attackers to access various appliance services via hardcoded credentials.	2024-09-30	8.8	CVE-2024-28809 cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	An issue was discovered in Infinera hiT 7300 5.60.50. A hidden SSH service (on the local management network interface) with hardcoded credentials allows attackers to access the appliance operating system (with highest privileges) via an SSH connection.	2024-09-30	8.8	CVE-2024-28812 cve@mitre.org
n/a--n/a	An issue was discovered in Infinera hiT 7300 5.60.50. Undocumented privileged functions in the @CT management application allow an attacker to activate remote SSH access to the appliance via an unexpected network interface.	2024-09-30	8.4	CVE-2024-28813 cve@mitre.org
n/a--n/a	FlatPress CMS v1.3.1 1.3 was discovered to use insecure methods to store authentication data via the cookie's component.	2024-10-02	8.1	CVE-2024-41290 cve@mitre.org
n/a--n/a	A stack-based Buffer Overflow vulnerability in DrayTek Vigor310 devices through 4.3.2.6 allows a remote attacker to execute arbitrary code via a long query string to the cgi-bin/ipfedr.cgi component.	2024-10-03	8	CVE-2024-41586 cve@mitre.org cve@mitre.org
n/a--n/a	DrayTek Vigor310 devices through 4.3.2.6 use unencrypted HTTP for authentication requests.	2024-10-03	8.8	CVE-2024-41589 cve@mitre.org cve@mitre.org
n/a--n/a	DrayTek Vigor3910 devices through 4.3.2.6 have a stack-based overflow when processing query string parameters because GetCGI mishandles extraneous ampersand characters and long key-value pairs.	2024-10-03	8	CVE-2024-41592 cve@mitre.org cve@mitre.org
n/a--n/a	DrayTek Vigor310 devices through 4.3.2.6 allow a remote attacker to change settings or cause a denial of service via .cgi pages because of missing bounds checks on read and write operations.	2024-10-03	8	CVE-2024-41595 cve@mitre.org cve@mitre.org
n/a--n/a	Buffer Overflow vulnerabilities exist in DrayTek Vigor310 devices through 4.3.2.6 (in the Vigor management UI) because of improper retrieval and handling of the CGI form parameters.	2024-10-03	8	CVE-2024-41596 cve@mitre.org cve@mitre.org
n/a--n/a	Scriptcase v9.10.023 and before is vulnerable to Remote Code Execution (RCE) via the nm_zip function.	2024-10-01	8	CVE-2024-46080 cve@mitre.org
n/a--n/a	Scriptcase 9.10.023 and before is vulnerable to Remote Code Execution (RCE) via the nm_unzip function.	2024-10-01	8	CVE-2024-46084 cve@mitre.org cve@mitre.org
n/a--n/a	PIX-LINK LV-WR22 RE3002-P1-01_V117.0 is vulnerable to Improper Access Control. The TELNET service is enabled with weak credentials for a root-level account, without the possibility of changing them.	2024-09-30	8.8	CVE-2024-46280 cve@mitre.org
n/a--n/a	TP-Link WR941ND V6 has a stack overflow vulnerability in the ssid parameter in /userRpm/popupSiteSurveyRpm.htm.	2024-09-30	8	CVE-2024-46313 cve@mitre.org
n/a--n/a	OS4ED openSIS-Classic v9.1 was discovered to contain a SQL injection vulnerability via a crafted payload.	2024-10-02	8.8	CVE-2024-46626 cve@mitre.org
n/a--n/a	In Infinera TNMS (Transcend Network Management System) 19.10.3, an insecure default configuration of the internal SFTP server on Linux servers allows remote attacker to access files and directories outside the SFTP user home directory.	2024-10-01	7.2	CVE-2024-25659 cve@mitre.org
n/a--n/a	In Infinera TNMS (Transcend Network Management System) 19.10.3, cleartext storage of sensitive information in memory of the desktop application TNMS Client allows guest OS administrators to obtain various users' passwords by reading memory dumps of the desktop application.	2024-10-01	7.7	CVE-2024-25661 cve@mitre.org
n/a--n/a	An issue in the _readFileSync function of Simple-Spellchecker v1.0.2 allows attackers to read arbitrary files via a directory traversal.	2024-09-30	7.5	CVE-2024-46503 cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				cve@mitre.org
n/a--n/a	ESAFENET CDG v5 was discovered to contain a SQL injection vulnerability via the id parameter in the NavigationAjax interface	2024-09-30	7.6	CVE-2024-46510 cve@mitre.org
n/a--n/a	LoadZilla LLC LoadLogic v1.4.3 was discovered to contain insecure permissions vulnerability which allows a remote attacker to execute arbitrary code via the LogicLoadEc2DeployLambda and CredsGenFunction function.	2024-09-30	7.5	CVE-2024-46511 cve@mitre.org
n/a--n/a	An issue in the TP-Link MQTT Broker and API gateway of TP-Link Kasa KP125M v1.0.3 allows attackers to establish connections by impersonating devices owned by other users.	2024-09-30	7.6	CVE-2024-46549 cve@mitre.org
n/a--n/a	CUPS cups-browsed before 2.5b1 will send an HTTP POST request to an arbitrary destination and port in response to a single IPP UDP packet requesting a printer to be added, a different vulnerability than CVE-2024-47176. (The request is meant to probe the new printer but can be used to create DDoS amplification attacks.)	2024-10-04	7.5	CVE-2024-47850 cve@mitre.org cve@mitre.org
n/a--uplot	Versions of the package uplot before 1.6.31 are vulnerable to Prototype Pollution via the uplot.assign function due to missing check if the attribute resolves to the object prototype.	2024-10-01	8.2	CVE-2024-21489 report@snyk.io report@snyk.io report@snyk.io
Nicejob--NiceJob	Cross-Site Request Forgery (CSRF) vulnerability in Nicejob NiceJob allows Stored XSS.This issue affects NiceJob: from n/a before 3.6.5.	2024-10-06	7.1	CVE-2024-44028 audit@patchstack.com
NuGet--NuGetGallery	NuGet Gallery is a package repository that powers nuget.org. The NuGetGallery has a security vulnerability in its handling of HTML element attributes, which allows an attacker to execute arbitrary HTML or Javascript code in a victim's browser.	2024-10-01	8.2	CVE-2024-47604 security-advisories@github.com security-advisories@github.com security-advisories@github.com
Optigo Networks--ONS-S8 Spectra Aggregation Switch	The web service for ONS-S8 - Spectra Aggregation Switch includes functions which do not properly validate user input, allowing an attacker to traverse directories, bypass authentication, and execute remote code.	2024-10-03	9.8	CVE-2024-41925 ics-cert@hq.dhs.gov
Optigo Networks--ONS-S8 Spectra Aggregation Switch	The web server for ONS-S8 - Spectra Aggregation Switch includes an incomplete authentication process, which can lead to an attacker authenticating without a password.	2024-10-03	9.1	CVE-2024-45367 ics-cert@hq.dhs.gov
parse-community--parse-server	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. If the Parse Server option allowCustomObjectId: true is set, an attacker that is allowed to create a new user can set a custom object ID for that new user that exploits the vulnerability and acquires privileges of a specific role. This vulnerability is fixed in 6.5.9 and 7.3.0.	2024-10-04	8.1	CVE-2024-47183 security-advisories@github.com security-advisories@github.com security-advisories@github.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				security-advisories@github.com security-advisories@github.com
planet -- gs-4210-24p2s_firmware	Certain switch models from PLANET Technology have a Hard-coded community string in the SNMPv1 service, allowing unauthorized remote attackers to use this community string to access the SNMPv1 service with read-write privileges.	2024-09-30	9.8	CVE-2024-8450 twcert@cert.org.tw twcert@cert.org.tw
planet -- gs-4210-24p2s_firmware	Certain switch models from PLANET Technology lack proper access control in firmware upload and download functionality, allowing unauthenticated remote attackers to download and upload firmware and system configurations, ultimately gaining full control of the devices.	2024-09-30	9.8	CVE-2024-8456 twcert@cert.org.tw twcert@cert.org.tw
planet -- gs-4210-24p2s_firmware	Certain switch models from PLANET Technology have a hard-coded credential in the specific command-line interface, allowing remote attackers with regular privilege to log in with this credential and obtain a Linux root shell.	2024-09-30	8.8	CVE-2024-8448 twcert@cert.org.tw twcert@cert.org.tw
planet -- gs-4210-24p2s_firmware	Certain switch models from PLANET Technology have a web application that is vulnerable to Cross-Site Request Forgery (CSRF). An unauthenticated remote attacker can trick a user into visiting a malicious website, allowing the attacker to impersonate the user and perform actions on their behalf, such as creating accounts.	2024-09-30	8.8	CVE-2024-8458 twcert@cert.org.tw twcert@cert.org.tw
planet -- gs-4210-24p2s_firmware	Certain switch models from PLANET Technology have an SSH service that improperly handles insufficiently authenticated connection requests, allowing unauthorized remote attackers to exploit this weakness to occupy connection slots and prevent legitimate users from accessing the SSH service.	2024-09-30	7.5	CVE-2024-8451 twcert@cert.org.tw twcert@cert.org.tw
planet -- gs-4210-24p2s_firmware	Certain switch models from PLANET Technology only support obsolete algorithms for authentication protocol and encryption protocol in the SNMPv3 service, allowing attackers to obtain plaintext SNMPv3 credentials potentially.	2024-09-30	7.5	CVE-2024-8452 twcert@cert.org.tw twcert@cert.org.tw
planet -- gs-4210-24p2s_firmware	The swctrl service is used to detect and remotely manage PLANET Technology devices. Certain switch models have a Denial-of-Service vulnerability in the swctrl service, allowing unauthenticated remote attackers to send crafted packets that can crash the service.	2024-09-30	7.5	CVE-2024-8454 twcert@cert.org.tw twcert@cert.org.tw
PowerDNS -- Recursor	An attacker can publish a zone containing specific Resource Record Sets. Repeatedly processing and caching results for these sets can lead to a denial of service.	2024-10-03	7.5	CVE-2024-25590 security@open-xchange.com
randygaul -- cute_png	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_load_png_mem() function at cute_png.h.	2024-10-01	7.8	CVE-2024-46258 cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				cve@mitre.org
randygaul -- cute_png	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_unfilter() function at cute_png.h.	2024-10-01	7.8	CVE-2024-46259 cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org
randygaul -- cute_png	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_make32() function at cute_png.h.	2024-10-01	7.8	CVE-2024-46261 cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org
randygaul -- cute_png	cute_png v1.05 was discovered to contain a stack overflow via the cp_dynamic() function at cute_png.h.	2024-10-01	7.8	CVE-2024-46263 cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org
randygaul -- cute_png	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_find() function at cute_png.h.	2024-10-01	7.8	CVE-2024-46264 cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org
randygaul -- cute_png	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_block() function at cute_png.h.	2024-10-01	7.8	CVE-2024-46267 cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org
randygaul -- cute_png	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_stored() function at cute_png.h.	2024-10-01	7.8	CVE-2024-46274 cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org
randygaul -- cute_png	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_chunk() function at cute_png.h.	2024-10-01	7.8	CVE-2024-46276 cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org
rankmath--Rank Math SEO AI SEO Tools to Dominate SEO Rankings	The Rank Math SEO - AI SEO Tools to Dominate SEO Rankings plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.0.228 via deserialization of untrusted input 'set_redirections' function. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target system, it could	2024-10-05	7.2	CVE-2024-9314 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfe

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.			nce.com
RedefiningTheWeb--WordPress & WooCommerce Affiliate Program	The WordPress & WooCommerce Affiliate Program plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 8.4.1. This is due to the rtwwwap_login_request_callback() function not properly validating a user's identity prior to authenticating them to the site. This makes it possible for unauthenticated attackers to log in as any user, including administrators, granted they have access to the administrator's email.	2024-10-01	9.8	CVE-2024-9289 security@wordfence.com security@wordfence.com
Robokassa--Robokassa payment gateway for Woocommerce	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Robokassa Robokassa payment gateway for Woocommerce allows Reflected XSS.This issue affects Robokassa payment gateway for Woocommerce: from n/a through 1.6.1.	2024-10-05	7.1	CVE-2024-47395 audit@patchstack.com
Sale php scripts--Web Directory Free	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Sale php scripts Web Directory Free allows Reflected XSS.This issue affects Web Directory Free: from n/a through 1.7.3.	2024-10-05	7.1	CVE-2024-47379 audit@patchstack.com
Schneider Elektronik--Series 700	An unauthenticated remote attacker may use a missing authentication for critical function vulnerability to reboot or erase the affected devices resulting in data loss and/or a DoS.	2024-10-02	9.1	CVE-2024-35293 info@cert.vde.com
SEIKO EPSON CORPORATION--Web Config	Insecure initial password configuration issue in SEIKO EPSON Web Config allows a remote unauthenticated attacker to set an arbitrary password and operate the device with an administrative privilege. As for the details of the affected versions, see the information provided by the vendor under [References].	2024-10-01	8.1	CVE-2024-47295 vultures@jpcert.or.jp vultures@jpcert.or.jp
SliceWP--SliceWP	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SliceWP allows Reflected XSS.This issue affects SliceWP: from n/a through 1.1.18.	2024-10-05	7.1	CVE-2024-47388 audit@patchstack.com
Sophos--Sophos Intercept X	A local privilege escalation vulnerability in Sophos Intercept X for Windows with Central Device Encryption 2024.2.0 and older allows writing of arbitrary files.	2024-10-02	8.8	CVE-2024-8885 security-alert@sophos.com
Team Tangible--Loops & Logic	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Team Tangible Loops & Logic allows Reflected XSS.This issue affects Loops & Logic: from n/a through 4.1.4.	2024-10-06	7.1	CVE-2024-47333 audit@patchstack.com
Tenable--Nessus Network Monitor	A stored cross site scripting vulnerability exists in Nessus Network Monitor where an authenticated, privileged local attacker could inject arbitrary code into the NNM UI via the local CLI.	2024-09-30	8.4	CVE-2024-9158 vulnreport@tenable.com
thimpress--WP Hotel Booking	The WP Hotel Booking plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the update_review() function in all versions up to, and including, 2.1.2. 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.	2024-10-02	8.8	CVE-2024-7855 security@wordfence.com security@wordfence.com security@wordfence.com
Tribulant--Newsletters	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tribulant Newsletters allows Reflected XSS.This issue affects Newsletters: from n/a through 4.9.9.1.	2024-10-06	7.1	CVE-2024-47346 audit@patchstack.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ultrapressorg--Empowerment	The Empowerment theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.0.2 via deserialization of untrusted input. 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 software. 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.	2024-10-01	8.8	CVE-2024-7433 security@wordfence.com security@wordfence.com
ultrapressorg--UltraPress	The UltraPress theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.2.1 via deserialization of untrusted input. 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 software. 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.	2024-10-01	8.8	CVE-2024-7434 security@wordfence.com security@wordfence.com
ultrapressorg--Unseen Blog	The Unseen Blog theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.0.0 via deserialization of untrusted input. 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 software. 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.	2024-10-01	8.8	CVE-2024-7432 security@wordfence.com security@wordfence.com
Unknown--Cost Calculator Builder	The Cost Calculator Builder WordPress plugin before 3.2.29 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as Admin.	2024-09-30	7.2	CVE-2024-8379 contact@wpscan.com
Unknown--Migration, Backup, Staging	The Migration, Backup, Staging WordPress plugin before 0.9.106 does not use sufficient randomness in the filename that is created when generating a backup, which could be bruteforced by attackers to leak sensitive information about said backups.	2024-10-02	7.5	CVE-2024-7315 contact@wpscan.com
Unlimited Elements--Unlimited Elements For Elementor (Free Widgets, Addons, Templates)	Improper Neutralization of Input During Web Page Generation (XSS or '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 1.5.121.	2024-10-06	7.1	CVE-2024-45454 audit@patchstack.com
Users Control--Users Control	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Users Control allows PHP Local File Inclusion.This issue affects Users Control: from n/a through 1.0.16.	2024-10-05	7.5	CVE-2024-44015 audit@patchstack.com
vCita--Online Booking & Scheduling Calendar for WordPress by vcita	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in vCita Online Booking & Scheduling Calendar for WordPress by vcita allows Reflected XSS.This issue affects Online Booking & Scheduling Calendar for WordPress by vcita: from n/a through 4.4.6.	2024-10-05	7.1	CVE-2024-47638 audit@patchstack.com
Veertu--Anka Build	A privilege escalation vulnerability exists in the Veertu Anka Build 1.42.0. The vulnerability occurs during Anka node agent update. A low privilege user can trigger the update action which can result in unexpected elevation of privilege.	2024-10-03	7.8	CVE-2024-39755 talos-cna@cisco.com
Veertu--Anka Build	A directory traversal vulnerability exists in the archive download functionality of Veertu Anka Build 1.42.0. A specially crafted HTTP request	2024-10-03	7.5	CVE-2024-41163 talos-

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	can lead to a disclosure of arbitrary files. An attacker can make an unauthenticated HTTP request to exploit this vulnerability.			cna@cisco.com
Veertu--Anka Build	A directory traversal vulnerability exists in the log files download functionality of Veertu Anka Build 1.42.0. A specially crafted HTTP request can result in a disclosure of arbitrary files. An attacker can make an unauthenticated HTTP request to trigger this vulnerability.	2024-10-03	7.5	CVE-2024-41922 talos-cna@cisco.com
Vmaxstudio--Vmax Project Manager	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Vmaxstudio Vmax Project Manager allows PHP Local File Inclusion, Code Injection.This issue affects Vmax Project Manager: from n/a through 1.0.	2024-10-05	9.6	CVE-2024-44014 audit@patchstack.com
WaspThemes--YellowPencil Visual CSS Style Editor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WaspThemes YellowPencil Visual CSS Style Editor allows Reflected XSS.This issue affects YellowPencil Visual CSS Style Editor: from n/a through 7.6.4.	2024-10-06	7.1	CVE-2024-47348 audit@patchstack.com
WP Compress--WP Compress Image Optimizer [All-In-One]	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Compress WP Compress - Image Optimizer [All-In-One] allows Reflected XSS.This issue affects WP Compress - Image Optimizer [All-In-One]: from n/a through 6.20.13.	2024-10-05	7.1	CVE-2024-47384 audit@patchstack.com
WP Extended--The Ultimate WordPress Toolkit WP Extended	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Extended The Ultimate WordPress Toolkit - WP Extended allows Reflected XSS.This issue affects The Ultimate WordPress Toolkit - WP Extended: from n/a through 3.0.8.	2024-10-05	7.1	CVE-2024-47386 audit@patchstack.com
WP Lab--WP-Lister Lite for eBay	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Lab WP-Lister Lite for eBay allows Reflected XSS.This issue affects WP-Lister Lite for eBay: from n/a through 3.6.3.	2024-10-05	7.1	CVE-2024-47380 audit@patchstack.com
WP Ticket Ultra--WP Ticket Ultra Help Desk & Support Plugin	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WP Ticket Ultra WP Ticket Ultra Help Desk & Support Plugin allows PHP Local File Inclusion.This issue affects WP Ticket Ultra Help Desk & Support Plugin: from n/a through 1.0.5.	2024-10-05	7.5	CVE-2024-44011 audit@patchstack.com
WPCOM--WPCOM Member	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPCOM WPCOM Member allows Reflected XSS.This issue affects WPCOM Member: from n/a through 1.5.4.	2024-10-05	7.1	CVE-2024-47378 audit@patchstack.com
wpdev33--WP Newsletter Subscription	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in wpdev33 WP Newsletter Subscription allows PHP Local File Inclusion.This issue affects WP Newsletter Subscription: from n/a through 1.1.	2024-10-05	7.5	CVE-2024-44012 audit@patchstack.com
WPExpertsio--WPExperts Square For GiveWP	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPExpertsio WPExperts Square For GiveWP allows SQL Injection.This issue affects WPExperts Square For GiveWP: from n/a through 1.3.	2024-10-06	7.6	CVE-2024-47338 audit@patchstack.com
WPMobile.App--WPMobile.App	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPMobile.App allows Reflected XSS.This issue affects WPMobile.App: from n/a through 11.50.	2024-10-06	7.1	CVE-2024-47349 audit@patchstack.com
wpmudev--Broken Link Checker	The Broken Link Checker plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg in /app/admin-notices/features/class-view.php without appropriate escaping on the URL in all versions up to, and including, 2.4.0. 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.	2024-10-01	7.1	CVE-2024-8981 security@wordfence.com security@wordfence.com security@wordfe

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				nce.com
WPWeb--Social Auto Poster	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPWeb Social Auto Poster allows Reflected XSS.This issue affects Social Auto Poster: from n/a through 5.3.15.	2024-10-05	7.1	CVE-2024-47369 audit@patchstack.com
WS Form--WS Form LITE	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WS Form WS Form LITE allows Stored XSS.This issue affects WS Form LITE: from n/a through 1.9.238.	2024-10-06	7.1	CVE-2024-47320 audit@patchstack.com
xunhuweb--Wechat Social login QQ	The Wechat Social login plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.3.0. This is due to insufficient verification on the user being supplied during the social login. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the user id. This is only exploitable if the app secret is not set, so it has a default empty value.	2024-10-01	9.8	CVE-2024-9106 security@wordfence.com security@wordfence.com
xunhuweb--Wechat Social login QQ	The Wechat Social login plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the 'convert_remoteimage_to_local' function in versions up to, and including, 1.3.0. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-10-01	9.8	CVE-2024-9108 security@wordfence.com security@wordfence.com
Xylus Themes--WP Bulk Delete	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Xylus Themes WP Bulk Delete allows Reflected XSS.This issue affects WP Bulk Delete: from n/a through 1.3.1.	2024-10-06	7.1	CVE-2024-47352 audit@patchstack.com
YITH--YITH WooCommerce Ajax Search	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in YITH YITH WooCommerce Ajax Search allows SQL Injection.This issue affects YITH WooCommerce Ajax Search: from n/a through 2.8.0.	2024-10-06	9.3	CVE-2024-47350 audit@patchstack.com
YITH--YITH WooCommerce Product Add-Ons	Improper Neutralization of Input During Web Page Generation (XSS or '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 4.13.0.	2024-10-06	7.1	CVE-2024-47367 audit@patchstack.com
zimbra -- collaboration	The postjournal service in Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1 sometimes allows unauthenticated users to execute commands.	2024-10-02	9.8	CVE-2024-45519 cve@mitre.org cve@mitre.org
apache -- seata	Deserialization of Untrusted Data vulnerability in Apache Seata. When developers disable authentication on the Seata-Server and do not use the Seata client SDK dependencies, they may construct uncontrolled serialized malicious requests by directly sending bytecode based on the Seata private protocol. This issue affects Apache Seata: 2.0.0, from 1.0.0 through 1.8.0. Users are recommended to upgrade to version 2.1.0/1.8.1, which fixes the issue.	2024-09-16	9.8	CVE-2024-22399 security@apache.org
Apple--iOS and iPadOS	This issue was addressed through improved state management. This issue is fixed in iOS 18 and iPadOS 18. A remote attacker may be able to cause a denial-of-service.	2024-09-17	7.5	CVE-2024-27874 product-security@apple.com
Apple--iOS and iPadOS	The issue was addressed with improved bounds checks. This issue is fixed in iOS 17.7 and iPadOS 17.7, iOS 18 and iPadOS 18. An attacker may be able to cause unexpected app termination.	2024-09-17	7.5	CVE-2024-27879 product-security@apple.com product-security@apple.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Apple--iOS and iPadOS	This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 18 and iPadOS 18. An attacker may be able to see recent photos without authentication in Assistive Access.	2024-09-17	7.5	CVE-2024-40852 product-security@apple.com
Apple--iOS and iPadOS	This issue was addressed through improved state management. This issue is fixed in iOS 18 and iPadOS 18. An app may gain unauthorized access to Local Network.	2024-09-17	7.7	CVE-2024-44147 product-security@apple.com
Apple--macOS	A race condition was addressed with improved locking. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, iOS 18 and iPadOS 18, macOS Sonoma 14.7, macOS Sequoia 15. Unpacking a maliciously crafted archive may allow an attacker to write arbitrary files.	2024-09-17	8.1	CVE-2024-27876 product-security@apple.com product-security@apple.com product-security@apple.com product-security@apple.com product-security@apple.com
Apple--macOS	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sequoia 15. An app may be able to break out of its sandbox.	2024-09-17	8.4	CVE-2024-44132 product-security@apple.com
Apple--macOS	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.7, visionOS 2, iOS 18 and iPadOS 18, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to overwrite arbitrary files.	2024-09-17	8.1	CVE-2024-44167 product-security@apple.com product-security@apple.com product-security@apple.com product-security@apple.com
Apple--macOS	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, macOS Sonoma 14.7, tvOS 18. An app may be able to cause unexpected system termination.	2024-09-17	8.1	CVE-2024-44169 product-security@apple.com product-security@apple.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				product-security@apple.com product-security@apple.com product-security@apple.com product-security@apple.com product-security@apple.com product-security@apple.com
Apple--macOS	The issue was addressed with improved checks. This issue is fixed in iOS 18 and iPadOS 18, macOS Sequoia 15. An app may be able to record the screen without an indicator.	2024-09-17	7.5	CVE-2024-27869 product-security@apple.com product-security@apple.com
Apple--macOS	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted video file may lead to unexpected app termination.	2024-09-17	7.8	CVE-2024-40841 product-security@apple.com product-security@apple.com
Apple--macOS	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15. An app may be able to gain root privileges.	2024-09-17	7.8	CVE-2024-40861 product-security@apple.com
Apple--macOS	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted texture may lead to unexpected app termination.	2024-09-17	7.8	CVE-2024-44160 product-security@apple.com product-security@apple.com product-security@apple.com
Apple--Xcode	A privacy issue was addressed by removing sensitive data. This issue is fixed in Xcode 16. An attacker may be able to determine the Apple ID of the owner of the computer.	2024-09-17	7.5	CVE-2024-40862 product-security@apple.com
best_online_news_portal_project --	A vulnerability classified as critical was found in SourceCodester Best Online News Portal 1.0. This vulnerability affects unknown code of the file /news-details.php of the component Comment Section. The manipulation	2024-09-19	9.8	CVE-2024-9008 cna@vuldb.com cna@vuldb.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
best_online_news_portal	of the argument name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.			cna@vuldb.com cna@vuldb.com cna@vuldb.com
Brave--Android Browser	In Brave Android prior to v1.67.116, domains in the Brave Shields popup are elided from the right instead of the left, which may lead to domain confusion.	2024-09-18	7.5	CVE-2024-37406 support@hackerone.com
Canonical Ltd.--Anbox Cloud	Anbox Management Service, in versions 1.17.0 through 1.23.0, does not validate the TLS certificate provided to it by the Anbox Stream Agent. An attacker must be able to machine-in-the-middle the Anbox Stream Agent from within an internal network before they can attempt to take advantage of this.	2024-09-18	7.5	CVE-2024-8287 security@ubuntu.com security@ubuntu.com security@ubuntu.com
Cellopoint--Secure Email Gateway	Secure Email Gateway from Cellopoint has Buffer Overflow Vulnerability in authentication process. Remote unauthenticated attackers can send crafted packets to crash the process, thereby bypassing authentication and obtaining system administrator privileges.	2024-09-20	9.8	CVE-2024-9043 twcert@cert.org.tw twcert@cert.org.tw
CIRCUTOR--CIRCUTOR Q-SMT	CIRCUTOR Q-SMT in its firmware version 1.0.4, could be affected by a denial of service (DoS) attack if an attacker with access to the web service bypasses the authentication mechanisms on the login page, allowing the attacker to use all the functionalities implemented at web level that allow interacting with the device.	2024-09-18	10	CVE-2024-8887 cve-coordination@incibe.es
CIRCUTOR--CIRCUTOR Q-SMT	An attacker with access to the network where CIRCUTOR Q-SMT is located in its firmware version 1.0.4, could steal the tokens used on the web, since these have no expiration date to access the web application without restrictions. Token theft can originate from different methods such as network captures, locally stored web information, etc.	2024-09-18	10	CVE-2024-8888 cve-coordination@incibe.es
CIRCUTOR--CIRCUTOR Q-SMT	An attacker with access to the network where the CIRCUTOR Q-SMT is located in its firmware version 1.0.4, could obtain legitimate credentials or steal sessions due to the fact that the device only implements the HTTP protocol. This fact prevents a secure communication channel from being established.	2024-09-18	8	CVE-2024-8890 cve-coordination@incibe.es
CIRCUTOR--CIRCUTOR TCP2RS+	Vulnerability in CIRCUTOR TCP2RS+ firmware version 1.3b, which could allow an attacker to modify any configuration value, even if the device has the user/password authentication option enabled, without authentication by sending packets through the UDP protocol and port 2000, deconfiguring the device and thus disabling its use. This equipment is at the end of its useful life cycle.	2024-09-18	9.3	CVE-2024-8889 cve-coordination@incibe.es
code-projects--Blood Bank Management System	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/login.php of the component Admin Login. The manipulation of the argument username/password leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-09-20	7.3	CVE-2024-9035 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
code-projects--Hospital Management System	A vulnerability, which was classified as critical, was found in code-projects Hospital Management System 1.0. This affects an unknown part of the file check_availability.php. The manipulation of the argument 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.	2024-09-17	7.3	CVE-2024-8944 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
code-projects--Patient Record	A vulnerability was found in code-projects Patient Record Management System 1.0 and classified as critical. Affected by this issue is some	2024-09-20	7.3	CVE-2024-9034 cna@vuldb.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	unknown functionality of the file login.php. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.			cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
code-projects--Restaurant Reservation System	A vulnerability was found in code-projects Restaurant Reservation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file index.php. The manipulation of the argument date leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions sid as affected paramater which is incorrect.	2024-09-22	7.3	CVE-2024-9085 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
code-projects--Student Record System	A vulnerability has been found in code-projects Student Record System 1.0 and classified as critical. This vulnerability affects unknown code of the file /course.php. The manipulation of the argument coursename leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-09-22	7.3	CVE-2024-9078 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
code-projects--Student Record System	A vulnerability was found in code-projects Student Record System 1.0 and classified as critical. This issue affects some unknown processing of the file /marks.php. The manipulation of the argument coursename leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-09-22	7.3	CVE-2024-9079 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
code-projects--Student Record System	A vulnerability was found in code-projects Student Record System 1.0. It has been classified as critical. Affected is an unknown function of the file /pincode-verification.php. The manipulation of the argument pincode leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-09-22	7.3	CVE-2024-9080 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
code-projects--Vehicle Management	A vulnerability, which was classified as critical, was found in code-projects Vehicle Management 1.0. This affects an unknown part of the file /edit1.php. The manipulation of the argument sno leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-09-22	7.3	CVE-2024-9087 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Codezips--Internal Marks Calculation	A vulnerability classified as critical has been found in Codezips Internal Marks Calculation 1.0. Affected is an unknown function of the file index.php. The manipulation of the argument tid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-09-20	7.3	CVE-2024-9037 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
contao--contao	Contao is an Open Source CMS. In affected versions a back end user with access to the file manager can upload malicious files and execute them on the server. Users are advised to update to Contao 4.13.49, 5.3.15 or 5.4.3. Users unable to update are advised to configure their web server so it does not execute PHP files and other scripts in the Contao file upload directory.	2024-09-17	8.3	CVE-2024-45398 security-advisories@github.com security-advisories@github.com
cure53--DOMPurify	DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTML, MathML and SVG. It has been discovered that malicious HTML using special nesting techniques can bypass the depth checking added to DOMPurify in recent releases. It was also possible to use Prototype Pollution to weaken the depth check. This renders dompurify unable to	2024-09-16	7.3	CVE-2024-45801 security-advisories@github.com security-

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	avoid cross site scripting (XSS) attacks. This issue has been addressed in versions 2.5.4 and 3.1.3 of DOMPurify. All users are advised to upgrade. There are no known workarounds for this vulnerability.			advisories@github.com security-advisories@github.com
Dassault Systmes--3DSwymer	A stored Cross-site Scripting (XSS) vulnerability affecting 3DSwym in 3DSwymer from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session.	2024-09-19	8.7	CVE-2024-7737 3DS.Information-Security@3ds.com
Dassault Systmes--ENOVIA Collaborative Industry Innovator	A reflected Cross-site Scripting (XSS) vulnerability affecting ENOVIA Collaborative Industry Innovator from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session.	2024-09-19	8.7	CVE-2024-7736 3DS.Information-Security@3ds.com
dlink -- covr-x1870_firmware	Certain models of D-Link wireless routers contain hidden functionality. By sending specific packets to the web service, the attacker can forcibly enable the telnet service and log in using hard-coded credentials. The telnet service enabled through this method can only be accessed from within the same local network as the device.	2024-09-16	8.8	CVE-2024-45696 twcert@cert.org.tw twcert@cert.org.tw
dlink -- dir-x4860_firmware	The web service of certain models of D-Link wireless routers contains a Stack-based Buffer Overflow vulnerability, which allows unauthenticated remote attackers to exploit this vulnerability to execute arbitrary code on the device.	2024-09-16	9.8	CVE-2024-45695 twcert@cert.org.tw twcert@cert.org.tw
dlink -- dir-x4860_firmware	Certain models of D-Link wireless routers have a hidden functionality where the telnet service is enabled when the WAN port is plugged in. Unauthorized remote attackers can log in and execute OS commands using hard-coded credentials.	2024-09-16	9.8	CVE-2024-45697 twcert@cert.org.tw twcert@cert.org.tw
dlink -- dir-x4860_firmware	Certain models of D-Link wireless routers do not properly validate user input in the telnet service, allowing unauthenticated remote attackers to use hard-coded credentials to log into telnet and inject arbitrary OS commands, which can then be executed on the device.	2024-09-16	9.8	CVE-2024-45698 twcert@cert.org.tw twcert@cert.org.tw
dlink -- dir-x5460_firmware	The web service of certain models of D-Link wireless routers contains a Stack-based Buffer Overflow vulnerability, which allows unauthenticated remote attackers to exploit this vulnerability to execute arbitrary code on the device.	2024-09-16	9.8	CVE-2024-45694 twcert@cert.org.tw twcert@cert.org.tw
dragonflyoss--Dragonfly2	Dragonfly is an open source P2P-based file distribution and image acceleration system. It is hosted by the Cloud Native Computing Foundation (CNCF) as an Incubating Level Project. Dragonfly uses JWT to verify user. However, the secret key for JWT, "Secret Key", is hard coded, which leads to authentication bypass. An attacker can perform any action as a user with admin privileges. This issue has been addressed in release version 2.0.9. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-19	9.8	CVE-2023-27584 security-advisories@github.com security-advisories@github.com
Eliz Software--Panel	Files or Directories Accessible to External Parties vulnerability in Eliz Software Panel allows Collect Data from Common Resource Locations.This issue affects Panel: before v2.3.24.	2024-09-18	7.5	CVE-2024-6878 iletisim@usom.g

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				ov.tr
envoyproxy--envoy	Envoy is a cloud-native high-performance edge/middle/service proxy. Envoy's 1.31 is using `oghttp` as the default HTTP/2 codec, and there are potential bugs around stream management in the codec. To resolve this Envoy will switch off the `oghttp2` by default. The impact of this issue is that envoy will crash. This issue has been addressed in release version 1.31.2. All users are advised to upgrade. There are no known workarounds for this issue.	2024-09-20	7.5	CVE-2024-45807 security-advisories@github.com
espressif--arduino-esp32	arduino-esp32 is an Arduino core for the ESP32, ESP32-S2, ESP32-S3, ESP32-C3, ESP32-C6 and ESP32-H2 microcontrollers. The `arduino-esp32` CI is vulnerable to multiple Poisoned Pipeline Execution (PPE) vulnerabilities. Code injection in `tests_results.yml` workflow (`GHSL-2024-169`) and environment Variable injection (`GHSL-2024-170`). These issue have been addressed but users are advised to verify the contents of the downloaded artifacts.	2024-09-17	9.9	CVE-2024-45798 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
favethemes--Houzez Login Register	Privilege Escalation vulnerability in favethemes Houzez Login Register houzez-login-register.This issue affects Houzez Login Register: from n/a through 3.2.5.	2024-09-17	8.8	CVE-2024-21743 audit@patchstack.com
favethemes--Houzez	Incorrect Privilege Assignment vulnerability in favethemes Houzez houzez allows Privilege Escalation.This issue affects Houzez: from n/a through 3.2.4.	2024-09-17	8.8	CVE-2024-22303 audit@patchstack.com
FreeBSD--FreeBSD	An insufficient boundary validation in the USB code could lead to an out-of-bounds read on the heap, which could potentially lead to an arbitrary write and remote code execution.	2024-09-20	9.8	CVE-2024-41721 secteam@freebsd.org
galaxyproject--galaxy	Galaxy is a free, open-source system for analyzing data, authoring workflows, training and education, publishing tools, managing infrastructure, and more. The editor visualization, /visualizations endpoint, can be used to store HTML tags and trigger javascript execution upon edit operation. All supported branches of Galaxy (and more back to release_20.05) were amended with the supplied patches. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-20	7.6	CVE-2024-42346 security-advisories@github.com
gematik--app-referencevalidator	The reference validator is a tool to perform advanced validation of FHIR resources for TI applications and interoperability standards. The profile location routine in the referencevalidator commons package is vulnerable to `XML External Entities` attack due to insecure defaults of the used Woodstox WstxInputFactory. A malicious XML resource can lead to network requests issued by referencevalidator and thus to a `Server Side Request Forgery` attack. The vulnerability impacts applications which use referencevalidator to process XML resources from untrusted sources. The problem has been patched with the 2.5.1 version of the referencevalidator. Users are strongly recommended to update to this version or a more recent one. A pre-processing or manual analysis of input XML resources on existence of DTD definitions or external entities can mitigate the problem.	2024-09-19	8.6	CVE-2024-46984 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				security-advisories@github.com security-advisories@github.com
getsentry--sentry	Sentry is a developer-first error tracking and performance monitoring platform. An authenticated user can mute alert rules from arbitrary organizations and projects with a know rule ID. The user does not need to be a member of the organization or have permissions on the project. In our review, we have identified no instances where alerts have been muted by unauthorized parties. A patch was issued to ensure authorization checks are properly scoped on requests to mute alert rules. Authenticated users who do not have the necessary permissions are no longer able to mute alerts. Sentry SaaS users do not need to take any action. Self-Hosted Sentry users should upgrade to version **24.9.0** or higher. The rule mute feature was generally available as of 23.6.0 but users with early access may have had the feature as of 23.4.0. Affected users are advised to upgrade to version 24.9.0. There are no known workarounds for this vulnerability.	2024-09-17	7.1	CVE-2024-45606 security-advisories@github.com security-advisories@github.com security-advisories@github.com
Google--Chrome	Type Confusion in V8 in Google Chrome prior to 129.0.6668.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-09-17	8.8	CVE-2024-8904 chrome-cve-admin@google.com chrome-cve-admin@google.com
Google--Chrome	Inappropriate implementation in V8 in Google Chrome prior to 129.0.6668.58 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page. (Chromium security severity: Medium)	2024-09-17	8.8	CVE-2024-8905 chrome-cve-admin@google.com chrome-cve-admin@google.com
google--mesop	Mesop is a Python-based UI framework designed for rapid web apps development. A vulnerability has been discovered and fixed in Mesop that could potentially allow unauthorized access to files on the server hosting the Mesop application. The vulnerability was related to insufficient input validation in a specific endpoint. This could have allowed an attacker to access files not intended to be served. Users are strongly advised to update to the latest version of Mesop immediately. The latest version includes a fix for this vulnerability. At time of publication 0.12.4 is the most recently available version of Mesop.	2024-09-18	7.5	CVE-2024-45601 security-advisories@github.com security-advisories@github.com
Guardrails AI--guardrails	An arbitrary code execution vulnerability exists in versions 0.2.9 up to 0.5.10 of the Guardrails AI Guardrails framework because of the way it validates XML files. If a victim user loads a maliciously crafted XML file containing Python code, the code will be passed to an eval function, causing it to execute on the user's machine.	2024-09-18	7.8	CVE-2024-458586f8de1f0-f67e-45a6-b68f-98777fdb759c
Hewlett Packard Enterprise (HPE)--Aruba OS	An authenticated Path Traversal vulnerabilities exists in the ArubaOS. Successful exploitation of this vulnerability allows an attacker to install unsigned packages on the underlying operating system, enabling the threat actor to execute arbitrary code or install implants.	2024-09-17	7.2	CVE-2024-42501 security-alert@hpe.com
Hewlett Packard Enterprise (HPE)--Aruba OS	Authenticated command injection vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability result in the ability to inject shell commands on the underlying operating system.	2024-09-17	7.2	CVE-2024-42502 security-alert@hpe.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Hewlett Packard Enterprise (HPE)--Aruba OS	Authenticated command execution vulnerability exist in the ArubaOS command line interface (CLI). Successful exploitation of this vulnerabilities result in the ability to run arbitrary commands as a priviledge user on the underlying operating system.	2024-09-17	7.2	CVE-2024-42503 security-alert@hpe.com
highwarden--Super Store Finder	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in highwarden Super Store Finder allows SQL Injection.This issue affects Super Store Finder: from n/a through 6.9.7.	2024-09-17	9.3	CVE-2024-43976 audit@patchstack.com
highwarden--Super Store Finder	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in highwarden Super Store Finder allows SQL Injection.This issue affects Super Store Finder: from n/a before 6.9.8.	2024-09-17	9.3	CVE-2024-43978 audit@patchstack.com
highwarden--Super Store Finder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in highwarden Super Store Finder allows Cross-Site Scripting (XSS).This issue affects Super Store Finder: from n/a through 6.9.7.	2024-09-18	7.1	CVE-2024-43975 audit@patchstack.com
ivanti --endpoint_manager_cloud_services_appliance	Path Traversal in the Ivanti CSA before 4.6 Patch 519 allows a remote unauthenticated attacker to access restricted functionality.	2024-09-19	9.1	CVE-2024-8963 3c1d8aa1-5a33-4ea4-8992-aadd6440af75
jeremieglotin--Webo-facto	The Webo-facto plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 1.40 due to insufficient restriction on the 'doSsoAuthentification' function. This makes it possible for unauthenticated attackers to make themselves administrators by registering with a username that contains '-wfuser'.	2024-09-20	9.8	CVE-2024-8853 security@wordfence.com security@wordfence.com security@wordfence.com
LikeBtn--Like Button Rating	Cross-Site Request Forgery (CSRF) vulnerability in LikeBtn Like Button Rating allows Cross-Site Scripting (XSS).This issue affects Like Button Rating: from n/a through 2.6.54.	2024-09-17	7.1	CVE-2024-44064 audit@patchstack.com
linux --linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix mc_data out-of-bounds read warning Clear warning that read mc_data[i-1] may out-of-bounds.	2024-09-18	7.1	CVE-2024-46722 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix ucode out-of-bounds read warning Clear warning that read ucode[] may out-of-bounds.	2024-09-18	7.1	CVE-2024-46723 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix out-of-bounds read of df_v1_7_channel_number Check the fb_channel_number range to avoid the array out-of-bounds read error	2024-09-18	7.1	CVE-2024-46724 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix out-of-bounds write warning Check the ring type value to fix the out-of-bounds write warning	2024-09-18	7.8	CVE-2024-46725 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: VMCI: Fix use-after-free when removing resource in vmci_resource_remove() When removing a resource from vmci_resource_table in vmci_resource_remove(), the search is performed using the resource handle by comparing context and resource fields. It is possible though to create two resources with different types but same handle (same context and resource fields). When trying to remove one of the resources, vmci_resource_remove() may not remove the intended one, but the object will still be freed as in the case of the datagram type in vmci_datagram_destroy_handle(). vmci_resource_table will still hold a pointer to this freed resource leading to a use-after-free vulnerability. BUG: KASAN: use-after-free in vmci_handle_is_equal include/linux/vmw_vmci_defs.h:142 [inline] BUG: KASAN: use-after-free in vmci_resource_remove+0x3a1/0x410 drivers/misc/vmw_vmci/vmci_resource.c:147 Read of size 4 at addr ffff88801c16d800 by task syz-executor197/1592 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x82/0xa9 lib/dump_stack.c:106 print_address_description.constprop.0+0x21/0x366 mm/kasan/report.c:239 __kasan_report.cold+0x7f/0x132 mm/kasan/report.c:425 kasan_report+0x38/0x51 mm/kasan/report.c:442 vmci_handle_is_equal include/linux/vmw_vmci_defs.h:142 [inline] vmci_resource_remove+0x3a1/0x410 drivers/misc/vmw_vmci/vmci_resource.c:147 vmci_qp_broker_detach+0x89a/0x11b9 drivers/misc/vmw_vmci/vmci_queue_pair.c:2182 ctx_free_ctx+0x473/0xbe1 drivers/misc/vmw_vmci/vmci_context.c:444 kref_put include/linux/kref.h:65 [inline] vmci_ctx_put drivers/misc/vmw_vmci/vmci_context.c:497 [inline] vmci_ctx_destroy+0x170/0x1d6 drivers/misc/vmw_vmci/vmci_context.c:195 vmci_host_close+0x125/0x1ac drivers/misc/vmw_vmci/vmci_host.c:143 __fput+0x261/0xa34 fs/file_table.c:282 task_work_run+0xf0/0x194 kernel/task_work.c:164 tracehook_notify_resume include/linux/tracehook.h:189 [inline] exit_to_user_mode_loop+0x184/0x189 kernel/entry/common.c:187 exit_to_user_mode_prepare+0x11b/0x123 kernel/entry/common.c:220 __syscall_exit_to_user_mode_work kernel/entry/common.c:302 [inline] syscall_exit_to_user_mode+0x18/0x42 kernel/entry/common.c:313 do_syscall_64+0x41/0x85 arch/x86/entry/common.c:86 entry_SYSCALL_64_after_hwframe+0x6e/0x0 This change ensures the type is also checked when removing the resource from vmci_resource_table in vmci_resource_remove().	2024-09-18	7.8	CVE-2024-46738 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: binder: fix UAF caused by offsets overwrite Binder objects are processed and copied individually into the target buffer during transactions. Any raw data in-between these objects is copied as well. However, this raw data copy lacks an out-of-bounds check. If the raw data exceeds the data section size then the copy overwrites the offsets section. This eventually triggers an error that attempts to unwind the processed objects. However, at this point the offsets used to index these objects are now corrupted. Unwinding with corrupted offsets can result in decrements of arbitrary nodes and lead to their premature release. Other users of such nodes are	2024-09-18	7.8	CVE-2024-46740 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	left with a dangling pointer triggering a use-after-free. This issue is made evident by the following KASAN report (trimmed): == BUG: KASAN: slab-use-after-free in _raw_spin_lock+0xe4/0x19c Write of size 4 at addr ffff47fc91598f04 by task binder-util/743 CPU: 9 UID: 0 PID: 743 Comm: binder-util Not tainted 6.11.0-rc4 #1 Hardware name: linux,dummy-virt (DT) Call trace: _raw_spin_lock+0xe4/0x19c binder_free_buf+0x128/0x434 binder_thread_write+0x8a4/0x3260 binder_ioctl+0x18f0/0x258c [...] Allocated by task 743: __kmalloc_cache_noprof+0x110/0x270 binder_new_node+0x50/0x700 binder_transaction+0x413c/0x6da8 binder_thread_write+0x978/0x3260 binder_ioctl+0x18f0/0x258c [...] Freed by task 745: kfree+0xbc/0x208 binder_thread_read+0x1c5c/0x37d4 binder_ioctl+0x16d8/0x258c [...] == To avoid this issue, let's check that the raw data copy is within the boundaries of the data section.			416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: Fix double free of 'buf' in error path smatch warning: drivers/misc/fastrpc.c:1926 fastrpc_req_mmap() error: double free of 'buf' In fastrpc_req_mmap() error path, the fastrpc buffer is freed in fastrpc_req_munmap_impl() if unmap is successful. But in the end, there is an unconditional call to fastrpc_buf_free(). So the above case triggers the double free of fastrpc buf.	2024-09-18	7.8	CVE-2024-46741 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: of/irq: Prevent device address out-of-bounds read in interrupt map walk When of_irq_parse_raw() is invoked with a device address smaller than the interrupt parent node (from #address-cells property), KASAN detects the following out-of-bounds read when populating the initial match table (dyndbg="func of_irq_parse_* +p"): OF: of_irq_parse_one: dev=/soc@0/picasso/watchdog, index=0 OF: parent=/soc@0/pci@878000000000/gpio0@17,0, intsize=2 OF: intspec=4 OF: of_irq_parse_raw: ipar=/soc@0/pci@878000000000/gpio0@17,0, size=2 OF: -> addrsize=3 == BUG: KASAN: slab-out-of-bounds in of_irq_parse_raw+0x2b8/0x8d0 Read of size 4 at addr ffffff81beca5608 by task bash/764 CPU: 1 PID: 764 Comm: bash Tainted: G O 6.1.67-484c613561-nokia_sm_arm64 #1 Hardware name: Unknown Unknown Product/Unknown Product, BIOS 2023.01-12.24.03-dirty 01/01/2023 Call trace: dump_backtrace+0xdc/0x130 show_stack+0x1c/0x30 dump_stack_lvl+0x6c/0x84 print_report+0x150/0x448 kasan_report+0x98/0x140 __asan_load4+0x78/0xa0 of_irq_parse_raw+0x2b8/0x8d0 of_irq_parse_one+0x24c/0x270 parse_interrupts+0xc0/0x120 of_fwnode_add_links+0x100/0x2d0 fw_devlink_parse_fwtree+0x64/0xc0 device_add+0xb38/0xc30 of_device_add+0x64/0x90 of_platform_device_create_pdata+0xd0/0x170 of_platform_bus_create+0x244/0x600 of_platform_notify+0x1b0/0x254 blocking_notifier_call_chain+0x9c/0xd0 __of_changeset_entry_notify+0x1b8/0x230 __of_changeset_apply_notify+0x54/0xe4 of_overlay_fdt_apply+0xc04/0xd94 ... The buggy address belongs to the object at ffffff81beca5600 which belongs to the cache kmalloc-128 of size 128 The buggy address is located 8 bytes inside of 128-byte region [ffffff81beca5600, ffffff81beca5680) The buggy address belongs to the physical page: page:00000000230d3d03 refcount:1 mapcount:0	2024-09-18	7.1	CVE-2024-46743 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mapping:0000000000000000 index:0x0 pfn:0x1beca4 head:00000000230d3d03 order:1 compound_mapcount:0 compound_pincount:0 flags: 0x8000000000010200(slab|head|zone=2) raw: 8000000000010200 0000000000000000 dead000000000122 ffffff810000c300 raw: 0000000000000000 0000000000200020 00000001ffffffff 0000000000000000 page dump because: kasan: bad access detected Memory state around the buggy address: ffffff81beca5500: 04 fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ffffff81beca5580: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc >ffffff81beca5600: 00 fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ^ ffffff81beca5680: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ffffff81beca5700: 00 00 00 00 00 00 fc fc fc fc fc fc fc fc fc fc == ===== OF: -> got it ! Prevent the out-of-bounds read by copying the device address into a buffer of sufficient size.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: HID: cougar: fix slab-out-of-bounds Read in cougar_report_fixup report_fixup for the Cougar 500k Gaming Keyboard was not verifying that the report descriptor size was correct before accessing it	2024-09-18	7.1	CVE-2024-46747 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix double put of @cfile in smb2_set_path_size() If smb2_compound_op() is called with a valid @cfile and returned -EINVAL, we need to call cifs_get_writable_path() before retrying it as the reference of @cfile was already dropped by previous call. This fixes the following KASAN splat when running fstests generic/013 against Windows Server 2022: CIFS: Attempting to mount //w22-fs0/scratch run fstests generic/013 at 2024-09-02 19:48:59 == ===== BUG: KASAN: slab-use-after-free in detach_if_pending+0xab/0x200 Write of size 8 at addr ffff88811f1a3730 by task kworker/3:2/176 CPU: 3 UID: 0 PID: 176 Comm: kworker/3:2 Not tainted 6.11.0-rc6 #2 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 Workqueue: cifsoplockd cifs_oplock_break [cifs] Call Trace: <TASK> dump_stack_lvl+0x5d/0x80 ? detach_if_pending+0xab/0x200 print_report+0x156/0x4d9 ? detach_if_pending+0xab/0x200 ? __virt_addr_valid+0x145/0x300 ? __phys_addr+0x46/0x90 ? detach_if_pending+0xab/0x200 kasan_report+0xda/0x110 ? detach_if_pending+0xab/0x200 detach_if_pending+0xab/0x200	2024-09-18	7.8	CVE-2024-46796 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	timer_delete+0x96/0xe0 ? __pfx_timer_delete+0x10/0x10 ? rcu_is_watching+0x20/0x50 try_to_grab_pending+0x46/0x3b0 __cancel_work+0x89/0x1b0 ? __pfx___cancel_work+0x10/0x10 ? kasan_save_track+0x14/0x30 cifs_close_deferred_file+0x110/0x2c0 [cifs] ? __pfx_cifs_close_deferred_file+0x10/0x10 [cifs] ? __pfx_down_read+0x10/0x10 cifs_oplock_break+0x4c1/0xa50 [cifs] ? __pfx_cifs_oplock_break+0x10/0x10 [cifs] ? lock_is_held_type+0x85/0xf0 ? mark_held_locks+0x1a/0x90 process_one_work+0x4c6/0x9f0 ? find_held_lock+0x8a/0xa0 ? __pfx_process_one_work+0x10/0x10 ? lock_acquired+0x220/0x550 ? __list_add_valid_or_report+0x37/0x100 worker_thread+0x2e4/0x570 ? __kthread_parkme+0xd1/0xf0 ? __pfx_worker_thread+0x10/0x10 kthread+0x17f/0x1c0 ? kthread+0xda/0x1c0 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x31/0x60 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> Allocated by task 1118: kasan_save_stack+0x30/0x50 kasan_save_track+0x14/0x30 __kasan_kmalloc+0xaa/0xb0 cifs_new_fileinfo+0xc8/0x9d0 [cifs] cifs_atomic_open+0x467/0x770 [cifs] lookup_open.isra.0+0x665/0x8b0 path_openat+0x4c3/0x1380 do_filp_open+0x167/0x270 do_sys_openat2+0x129/0x160 __x64_sys_creat+0xad/0xe0 do_syscall_64+0xbb/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 83: kasan_save_stack+0x30/0x50 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3b/0x70 poison_slab_object+0xe9/0x160 __kasan_slab_free+0x32/0x50 kfree+0xf2/0x300 process_one_work+0x4c6/0x9f0 worker_thread+0x2e4/0x570 kthread+0x17f/0x1c0 ret_from_fork+0x31/0x60 ret_from_fork_asm+0x1a/0x30 Last potentially related work creation: kasan_save_stack+0x30/0x50 __kasan_record_aux_stack+0xad/0xc0 insert_work+0x29/0xe0 __queue_work+0x5ea/0x760 queue_work_on+0x6d/0x90 _cifsFileInfo_put+0x3f6/0x770 [cifs] smb2_compound_op+0x911/0x3940 [cifs] smb2_set_path_size+0x228/0x270 [cifs] cifs_set_file_size+0x197/0x460 [cifs] cifs_setattr+0xd9c/0x14b0 [cifs] notify_change+0x4e3/0x740 do_truncate+0xfa/0x180 vfs_truncate+0x195/0x200 __x64_sys_truncate+0x109/0x150 do_syscall_64+0xbb/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ASoC: dapm: Fix UAF for snd_soc_pcm_runtime object When using kernel with the following extra config, - CONFIG_KASAN=y - CONFIG_KASAN_GENERIC=y - CONFIG_KASAN_INLINE=y - CONFIG_KASAN_VMALLOC=y - CONFIG_FRAME_WARN=4096 kernel detects that snd_pcm_suspend_all() access a freed 'snd_soc_pcm_runtime' object when the system is suspended, which leads to a use-after-free bug: [52.047746] BUG: KASAN: use-after-free in snd_pcm_suspend_all+0x1a8/0x270 [52.047765] Read of size 1 at addr ffff0000b9434d50 by task systemd-sleep/2330 [52.047785] Call trace: [52.047787] dump_backtrace+0x0/0x3c0 [52.047794] show_stack+0x34/0x50 [52.047797] dump_stack_lvl+0x68/0x8c [52.047802] print_address_description.constprop.0+0x74/0x2c0 [52.047809] kasan_report+0x210/0x230 [52.047815] __asan_report_load1_noabort+0x3c/0x50 [52.047820] snd_pcm_suspend_all+0x1a8/0x270 [52.047824] snd_soc_suspend+0x19c/0x4e0 The snd_pcm_sync_stop() has a NULL check on 'substream->runtime' before making any access. So we need to always set 'substream->runtime' to NULL everytime we kfree() it.	2024-09-18	7.8	CVE-2024-46798 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: sch/netem: fix use after free in netem_dequeue If netem_dequeue() enqueues packet to inner qdisc and that qdisc returns __NET_XMIT_STOLEN. The packet is dropped but qdisc_tree_reduce_backlog() is not called to update the parent's q.qlen, leading to the similar use-after-free as Commit e04991a48dbaf382 ("netem: fix return value if duplicate enqueue fails") Commands to trigger KASAN UaF: ip link add type dummy ip link set lo up ip link set dummy0 up tc qdisc add dev lo parent root handle 1: drr tc filter add dev lo parent 1: basic classid 1:1 tc class add dev lo classid 1:1 drr tc qdisc add dev lo parent 1:1 handle 2: netem tc qdisc add dev lo parent 2: handle 3: drr tc filter add dev lo parent 3: basic classid 3:1 action mirred egress redirect dev dummy0 tc class add dev lo classid 3:1 drr ping -c1 -W0.01 localhost # Trigger bug tc class del dev lo classid 1:1 tc class add dev lo classid 1:1 drr ping -c1 -W0.01 localhost # UaF	2024-09-18	7.8	CVE-2024-46800 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
mattermost -- mattermost_desktop	Mattermost Desktop App versions <=5.8.0 fail to specify an absolute path when searching the cmd.exe file, which allows a local attacker who is able to put an cmd.exe file in the Downloads folder of a user's machine to cause remote code execution on that machine.	2024-09-16	7.8	CVE-2024-39613 responsibledisclosure@mattermost.com
Mautic--Mautic	Prior to the patched version, logged in users of Mautic are vulnerable to Relative Path Traversal/Arbitrary File Deletion. Regardless of the level of access the Mautic user had, they could delete files other than those in the media folders such as system files, libraries or other important files. This vulnerability exists in the implementation of the GrapesJS builder in Mautic.	2024-09-17	8.1	CVE-2021-27916 security@mautic.org
Mautic--Mautic	Prior to the patched version, logged in users of Mautic are able to access areas of the application that they should be prevented from accessing. Users could potentially access sensitive data such as names and surnames, company names and stage names.	2024-09-18	8.3	CVE-2022-25776 security@mautic.org
Mautic--Mautic	Prior to the patched version, there is an XSS vulnerability in the description fields within the Mautic application which could be exploited by a logged in user of Mautic with the appropriate permissions. This could lead to the user having elevated access to the system.	2024-09-17	7.6	CVE-2021-27915 security@mautic.org
Mautic--Mautic	Prior to this patch, a stored XSS vulnerability existed in the contact tracking and page hits report.	2024-09-18	7.3	CVE-2021-27917 security@mautic.org
Mautic--Mautic	The logic in place to facilitate the update process via the user interface lacks access control to verify if permission exists to perform the tasks. Prior to this patch being applied it might be possible for an attacker to access the Mautic version number or to execute parts of the upgrade process without permission. As upgrading in the user interface is deprecated, this functionality is no longer required.	2024-09-18	7	CVE-2022-25768 security@mautic.org
Mautic--Mautic	ImpactThe default .htaccess file has some restrictions in the access to PHP files to only allow specific PHP files to be executed in the root of the application. This logic isn't correct, as the regex in the second FilesMatch only checks the filename, not the full path.	2024-09-18	7.2	CVE-2022-25769 security@mautic.org security@mautic.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				org
Mautic--Mautic	Mautic allows you to update the application via an upgrade script. The upgrade logic isn't shielded off correctly, which may lead to vulnerable situation. This vulnerability is mitigated by the fact that Mautic needs to be installed in a certain way to be vulnerable.	2024-09-18	7.8	CVE-2022-25770 security@mautic.org
mfasoft -- secure_authentication_server	An improper access control (IDOR) vulnerability in the /api-selfportal/get-info-token-properties endpoint in MFASOFT Secure Authentication Server (SAS) 1.8.x through 1.9.x before 1.9.040924 allows remote attackers gain access to user tokens without authentication. The is a brute-force attack on the serial parameter by number identifier: GA00001, GA00002, GA00003, etc.	2024-09-16	7.5	CVE-2024-46937 cve@mitre.org cve@mitre.org
Microsoft-- Dynamics 365 Business Central Online	Improper authorization in Dynamics 365 Business Central resulted in a vulnerability that allows an authenticated attacker to elevate privileges over a network.	2024-09-17	8.1	CVE-2024-43460 secure@microsoft.com
Microsoft-- GroupMe	An improper access control vulnerability in GroupMe allows an a unauthenticated attacker to elevate privileges over a network by convincing a user to click on a malicious link.	2024-09-17	8.8	CVE-2024-38183 secure@microsoft.com
Microsoft-- Microsoft Office LTSC 2021	Microsoft Office Visio Remote Code Execution Vulnerability	2024-09-19	7.8	CVE-2024-38016 secure@microsoft.com
mihail-barinov-- Share This Image	The Share This Image plugin for WordPress is vulnerable to Open Redirect in all versions up to, and including, 2.03. This is due to insufficient validation on the redirect url supplied via the link parameter. This makes it possible for unauthenticated attackers to redirect users to potentially malicious sites if they can successfully trick them into performing an action.	2024-09-17	7.2	CVE-2024-8761 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
Millbeck Communications --Proroute H685t-w	There is a command injection vulnerability that may allow an attacker to inject malicious input on the device's operating system.	2024-09-17	8.8	CVE-2024-45682 ics-cert@hq.dhs.gov
n/a--Intel(R) Processors	Improper input validation in UEFI firmware error handler for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	2024-09-16	7.5	CVE-2024-21829 secure@intel.com
n/a-- MicroPython	A vulnerability was found in MicroPython 1.23.0. It has been classified as critical. Affected is the function mp_vfs_umount of the file extmod/vfs.c of the component VFS Unmount Handler. The manipulation leads to heap-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 29943546343c92334e8518695a11fc0e2ceea68b. It is recommended to apply a patch to fix this issue. In the VFS unmount process, the comparison between the mounted path string and the unmount requested string is based solely on the length of the unmount string, which can lead to a heap buffer overflow read.	2024-09-17	7.3	CVE-2024-8946 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--MicroPython	A vulnerability was found in MicroPython 1.23.0. It has been rated as critical. Affected by this issue is the function mpz_as_bytes of the file py/objint.c. The manipulation leads to heap-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The patch is identified as 908ab1ceca15ee6fd0ef82ca4cba770a3ec41894. It is recommended to apply a patch to fix this issue. In micropython objint component, converting zero from int to bytes leads to heap buffer-overflow-write at mpz_as_bytes.	2024-09-17	7.3	CVE-2024-8948 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
n/a--n/a	Directory Traversal in the web interface of the Tiptel IP 286 with firmware version 2.61.13.10 allows attackers to overwrite arbitrary files on the phone via the Ringtone upload function.	2024-09-19	9.9	CVE-2024-33109 cve@mitre.org cve@mitre.org
n/a--n/a	Insecure deserialization in sqlitedict up to v2.1.0 allows attackers to execute arbitrary code.	2024-09-18	9.8	CVE-2024-35515 cve@mitre.org cve@mitre.org
n/a--n/a	An arbitrary file upload vulnerability in the Media Manager function of Closed-Loop Technology CLESS Server v4.5.2 allows attackers to execute arbitrary code via uploading a crafted PHP file to the upload endpoint.	2024-09-19	9.8	CVE-2024-40125 cve@mitre.org cve@mitre.org
n/a--n/a	Buffer Overflow vulnerability in btstack mesh commit before v.864e2f2b6b7878c8fab3cf5ee84ae566e3380c58 allows a remote attacker to execute arbitrary code via the pb_adv_handle_tranaction_cont function in the src/mesh/pb_adv.c component	2024-09-18	9.8	CVE-2024-40568 cve@mitre.org
n/a--n/a	SQL Injection vulnerability in todesk v.1.1 allows a remote attacker to execute arbitrary code via the /todesk.com/news.html parameter.	2024-09-18	9.8	CVE-2024-44542 cve@mitre.org
n/a--n/a	The HTTPD binary in multiple ZTE routers has a stack-based buffer overflow vulnerability in webPrivateDecrypt function. This function is responsible for decrypting RSA encrypted ciphertext, the encrypted data is supplied base64 encoded. The decoded ciphertext is stored on the stack without checking its length. An unauthenticated attacker can get RCE as root by exploiting this vulnerability.	2024-09-16	9.8	CVE-2024-45414 cve@mitre.org
n/a--n/a	The HTTPD binary in multiple ZTE routers has a stack-based buffer overflow vulnerability in check_data_integrity function. This function is responsible for validating the checksum of data in post request. The checksum is sent encrypted in the request, the function decrypts it and stores the checksum on the stack without validating it. An unauthenticated attacker can get RCE as root by exploiting this vulnerability.	2024-09-16	9.8	CVE-2024-45415 cve@mitre.org
n/a--n/a	Arc before 2024-08-26 allows remote code execution in JavaScript boosts. Boosts that run JavaScript cannot be shared by default; however (because of misconfigured Firebase ACLs), it is possible to create or update a boost using another user's ID. This installs the boost in the victim's browser and runs arbitrary Javascript on that browser in a privileged context. NOTE: this is a no-action cloud vulnerability with zero affected users.	2024-09-20	9.8	CVE-2024-45489 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	An issue was discovered in Bravura Security Fabric versions 12.3.x before 12.3.5.32784, 12.4.x before 12.4.3.35110, 12.5.x before 12.5.2.35950, 12.6.x before 12.6.2.37183, and 12.7.x before 12.7.1.38241. An unauthenticated attacker can cause a resource leak by issuing multiple failed login attempts through API SOAP.	2024-09-18	9.1	CVE-2024-45523 cve@mitre.org
n/a--n/a	Best House Rental Management System 1.0 contains a SQL injection vulnerability in the delete_category() function of the file rental/admin_class.php.	2024-09-18	9.8	CVE-2024-46374 cve@mitre.org
n/a--n/a	Best House Rental Management System 1.0 contains an arbitrary file upload vulnerability in the signup() function of the file rental/admin_class.php.	2024-09-18	9.8	CVE-2024-46375 cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	Best House Rental Management System 1.0 contains an arbitrary file upload vulnerability in the update_account() function of the file rental/admin_class.php.	2024-09-18	9.8	CVE-2024-46376 cve@mitre.org
n/a--n/a	Best House Rental Management System 1.0 contains an arbitrary file upload vulnerability in the save_settings() function of the file rental/admin_class.php.	2024-09-18	9.8	CVE-2024-46377 cve@mitre.org
n/a--n/a	langchain_experimental (aka LangChain Experimental) 0.1.17 through 0.3.0 for LangChain allows attackers to execute arbitrary code through sympy.sympify (which uses eval) in LLMSymbolicMathChain. LLMSymbolicMathChain was introduced in fcccde406dd9e9b05fc9babcbeb9ff527b0ec0c6 (2023-10-05).	2024-09-19	9.8	CVE-2024-46946 cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	Victure PC420 1.1.39 was discovered to contain a hardcoded root password which is stored in plaintext.	2024-09-18	8.8	CVE-2023-41610 cve@mitre.org
n/a--n/a	Victure PC420 1.1.39 was discovered to use a weak encryption key for the file enabled_telnet.dat on the Micro SD card.	2024-09-18	8.8	CVE-2023-41612 cve@mitre.org
n/a--n/a	exec.CommandContext in Chaosblade 0.3 through 1.7.3, when server mode is used, allows OS command execution via the cmd parameter without authentication.	2024-09-18	8.6	CVE-2023-47105 cve@mitre.org cve@mitre.org
n/a--n/a	An issue in Pure Data 0.54-0 and fixed in 0.54-1 allows a local attacker to escalate privileges via the set*id () function.	2024-09-20	8.4	CVE-2023-47480 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	Triangle Microworks TMW IEC 61850 Client source code libraries before 12.2.0 lack a buffer size check when processing received messages. The resulting buffer overflow can cause a crash, resulting in a denial of service.	2024-09-18	8.2	CVE-2024-34057 cve@mitre.org cve@mitre.org
n/a--n/a	Stack overflow vulnerability in the Login function in the HNAP service in D-Link DCS-960L with firmware 1.09 allows attackers to execute of arbitrary code.	2024-09-18	8.8	CVE-2024-44589 cve@mitre.org cve@mitre.org
n/a--n/a	The HTTPD binary in multiple ZTE routers has a stack-based buffer overflow vulnerability in rsa_decrypt function. This function is an API wrapper for LUA to decrypt RSA encrypted ciphertext, the decrypted data is stored on the stack without checking its length. An authenticated attacker can get RCE as root by exploiting this vulnerability.	2024-09-16	8.1	CVE-2024-45413 cve@mitre.org
n/a--n/a	The HTTPD binary in multiple ZTE routers has a local file inclusion vulnerability in session_init function. The session -LUA- files are stored in the directory /var/lua_session, the function iterates on all files in this directory and executes them using the function dofile without any validation if it is a valid session file or not. An attacker who is able to write a malicious file in the sessions directory can get RCE as root.	2024-09-16	8.1	CVE-2024-45416 cve@mitre.org
n/a--n/a	logiops through 0.3.4, in its default configuration, allows any unprivileged user to configure its logid daemon via an unrestricted D-Bus service, including setting malicious keyboard macros. This allows for privilege escalation with minimal user interaction.	2024-09-19	8.5	CVE-2024-45752 cve@mitre.org cve@mitre.org
n/a--n/a	FrogCMS V0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/plugin/file_manager/rename	2024-09-17	8.8	CVE-2024-46085 cve@mitre.org
n/a--n/a	FrogCMS V0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/plugin/file_manager/delete/123	2024-09-18	8.8	CVE-2024-46086 cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	FrogCMS V0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/plugin/file_manager/create_directory	2024-09-17	8.8	CVE-2024-46362 cve@mitre.org
n/a--n/a	Dedecms V5.7.115 contains an arbitrary code execution via file upload vulnerability in the backend.	2024-09-18	8.8	CVE-2024-46373 cve@mitre.org
n/a--n/a	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admin/?/user/add	2024-09-19	8	CVE-2024-46394 cve@mitre.org
n/a--n/a	An issue was discovered in Technitium 11.0.2. There is a vulnerability (called BadDNS) in DNS resolving software, which triggers a resolver to ignore valid responses, thus causing DoS (denial of service) for normal resolution. The effects of an exploit would be widespread and highly impactful, because the attacker could just forge a response targeting the source port of a vulnerable resolver without the need to guess the correct TXID.	2024-09-18	7.5	CVE-2023-28451 cve@mitre.org cve@mitre.org
n/a--n/a	An issue was discovered in Technitium through 11.0.2. The forwarding mode enables attackers to create a query loop using Technitium resolvers, launching amplification attacks and causing potential DoS.	2024-09-18	7.5	CVE-2023-28455 cve@mitre.org cve@mitre.org
n/a--n/a	An issue was discovered in Technitium through 11.0.2. It enables attackers to launch amplification attacks (3 times more than other "golden model" software like BIND) and cause potential DoS.	2024-09-18	7.5	CVE-2023-28456 cve@mitre.org cve@mitre.org
n/a--n/a	An issue was discovered in Technitium through 11.0.3. It enables attackers to conduct a DNS cache poisoning attack and inject fake responses within 1 second, which is impactful.	2024-09-18	7.5	CVE-2023-28457 cve@mitre.org cve@mitre.org
n/a--n/a	CoreDNS through 1.10.1 enables attackers to achieve DNS cache poisoning and inject fake responses via a birthday attack.	2024-09-18	7.5	CVE-2023-30464 cve@mitre.org
n/a--n/a	A Business Logic vulnerability in Shopkit 1.0 allows an attacker to add products with negative quantities to the shopping cart via the qtd parameter in the add-to-cart function.	2024-09-16	7.5	CVE-2023-45854 cve@mitre.org cve@mitre.org
n/a--n/a	Technitium 11.5.3 allows remote attackers to cause a denial of service (bandwidth amplification) because the DNSBomb manipulation causes accumulation of low-rate DNS queries such that there is a large-sized response in a burst of traffic.	2024-09-18	7.5	CVE-2023-49203 cve@mitre.org cve@mitre.org
n/a--n/a	An Incorrect Access Control vulnerability was found in /music/index.php?page=user_list and /music/index.php?page=edit_user in Kashipara Music Management System v1.0. This allows a low privileged attacker to take over the administrator account.	2024-09-16	7.6	CVE-2024-42798 cve@mitre.org cve@mitre.org
n/a--n/a	An issue in TuomoKu SPx-GC v.1.3.0 and before allows a remote attacker to execute arbitrary code via the child_process.js function.	2024-09-16	7.3	CVE-2024-44623 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--Seamless Firmware Updates for some Intel reference platforms	Race condition in Seamless Firmware Updates for some Intel(R) reference platforms may allow a privileged user to potentially enable denial of service via local access.	2024-09-16	7.9	CVE-2024-23599 secure@intel.com
n/a--UEFI firmware for some Intel(R)	A race condition in UEFI firmware for some Intel(R) processors may allow a privileged user to potentially enable escalation of privilege via local access.	2024-09-16	7.5	CVE-2023-41833 secure@intel.co

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
processors				m
n/a--UEFI firmware for some Intel(R) Processors	Improper access control in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	2024-09-16	7.5	CVE-2023-43626 secure@intel.com
n/a--UEFI firmware for some Intel(R) Processors	Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to enable information disclosure or denial of service via local access.	2024-09-16	7.2	CVE-2024-21781 secure@intel.com
n/a--UEFI firmware for some Intel(R) Processors	Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	2024-09-16	7.5	CVE-2024-21871 secure@intel.com
n/a--UEFI firmware for some Intel(R) reference processors	Untrusted pointer dereference in UEFI firmware for some Intel(R) reference processors may allow a privileged user to potentially enable escalation of privilege via local access.	2024-09-16	8.2	CVE-2023-42772 secure@intel.com
n/a--VMware vCenter Server	The vCenter Server contains a heap-overflow vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger this vulnerability by sending a specially crafted network packet potentially leading to remote code execution.	2024-09-17	9.8	CVE-2024-38812 security@vmware.com
n/a--VMware vCenter Server	The vCenter Server contains a privilege escalation vulnerability. A malicious actor with network access to vCenter Server may trigger this vulnerability to escalate privileges to root by sending a specially crafted network packet.	2024-09-17	7.5	CVE-2024-38813 security@vmware.com
nextcloud -- desktop	In Nextcloud Desktop Client 3.13.1 through 3.13.3 on Linux, synchronized files (between the server and client) may become world writable or world readable. This is fixed in 3.13.4.	2024-09-16	9.1	CVE-2024-46958 cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org
Open Asset Import Library--Assimp	Heap-based buffer overflow vulnerability in Assimp versions prior to 5.4.3 allows a local attacker to execute arbitrary code by importing a specially crafted file into the product.	2024-09-18	8.4	CVE-2024-45679 vultures@jpcert.or.jp vultures@jpcert.or.jp
opennetworking -- libfluid_msg	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routines fluid_msg::of13::InstructionSet::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-23915 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routines fluid_msg::ActionSet::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-23916 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routines fluid_msg::ActionList::unpack13. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31164 prodsec@nozominetworks.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
opennetworking -- libfluid_msg	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::SetFieldAction::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31165 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::HelloElemVersionBitmap::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31166 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::QueuePropertyList::unpack13. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31167 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::EchoCommon::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31168 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::QueueGetConfigReply::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31169 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::StatsReplyQueue::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31170 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::StatsReplyPort::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31171 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::StatsReplyTable::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31172 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::StatsReplyFlow::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31173 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::FeaturesReply::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31174 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::TablePropertiesList::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31175 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::TableFeaturePropOXM::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31176 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg modules). This vulnerability is associated with program routines fluid_msg::of13::TableFeaturePropActions::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31177 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program	2024-09-18	7.5	CVE-2024-31178 prodsec@nozomi

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	routine fluid_msg::of13::TableFeaturePropNextTables::unpack. This issue affects libfluid: 0.1.0.			networks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::TableFeaturePropInstruction::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31179 prodsec@nozomi networks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::GroupDesc::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31180 prodsec@nozomi networks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::GroupStats::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31181 prodsec@nozomi networks.com
opennetworking -- libfluid_msg	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::QueuePropertyList::unpack10. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31182 prodsec@nozomi networks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::Hello::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31183 prodsec@nozomi networks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MeterStats::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31184 prodsec@nozomi networks.com
opennetworking -- libfluid_msg	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MeterBandList::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31185 prodsec@nozomi networks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::QueueGetConfigReply::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31186 prodsec@nozomi networks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyPortDescription::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31187 prodsec@nozomi networks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyTableFeatures::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31188 prodsec@nozomi networks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartRequestTableFeatures::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31189 prodsec@nozomi networks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyMeterConfig::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31190 prodsec@nozomi networks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyMeter::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31191 prodsec@nozomi networks.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyGroupDesc::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31192 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyGroup::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31193 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyPortStats::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31194 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyTable::unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31195 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::ActionList::unpack10. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31196 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Improper Null Termination vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::Port:unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31197 prodsec@nozominetworks.com
opennetworking -- libfluid_msg	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::Port:unpack. This issue affects libfluid: 0.1.0.	2024-09-18	7.5	CVE-2024-31198 prodsec@nozominetworks.com
OpenPLC-- OpenPLC_v3	A stack-based buffer overflow vulnerability exists in the OpenPLC Runtime EtherNet/IP parser functionality of OpenPLC _v3 b4702061dc14d1024856f71b4543298d77007b88. A specially crafted EtherNet/IP request can lead to remote code execution. An attacker can send a series of EtherNet/IP requests to trigger this vulnerability.	2024-09-18	9	CVE-2024-34026 talos-cna@cisco.com
OpenPLC-- OpenPLC_v3	An out-of-bounds read vulnerability exists in the OpenPLC Runtime EtherNet/IP PCCC parser functionality of OpenPLC_v3 b4702061dc14d1024856f71b4543298d77007b88. A specially crafted network request can lead to denial of service. An attacker can send a series of EtherNet/IP requests to trigger this vulnerability.This is the first instance of the incorrect comparison.	2024-09-18	7.5	CVE-2024-36980 talos-cna@cisco.com
OpenPLC-- OpenPLC_v3	An out-of-bounds read vulnerability exists in the OpenPLC Runtime EtherNet/IP PCCC parser functionality of OpenPLC_v3 b4702061dc14d1024856f71b4543298d77007b88. A specially crafted network request can lead to denial of service. An attacker can send a series of EtherNet/IP requests to trigger this vulnerability.This is the final instance of the incorrect comparison.	2024-09-18	7.5	CVE-2024-36981 talos-cna@cisco.com
OpenPLC-- OpenPLC_v3	Multiple invalid pointer dereference vulnerabilities exist in the OpenPLC Runtime EtherNet/IP parser functionality of OpenPLC_v3 16bf8bac1a36d95b73e7b8722d0edb8b9c5bb56a. A specially crafted EtherNet/IP request can lead to denial of service. An attacker can send a series of EtherNet/IP requests to trigger these vulnerabilities.This instance of the vulnerability occurs within the `Protected_Logical_Read_Reply` function	2024-09-18	7.5	CVE-2024-39589 talos-cna@cisco.com
OpenPLC-- OpenPLC_v3	Multiple invalid pointer dereference vulnerabilities exist in the OpenPLC Runtime EtherNet/IP parser functionality of OpenPLC_v3 16bf8bac1a36d95b73e7b8722d0edb8b9c5bb56a. A specially crafted EtherNet/IP request can lead to denial of service. An attacker can send a series of EtherNet/IP requests to trigger these vulnerabilities.This instance of the vulnerability occurs within the `Protected_Logical_Write_Reply` function	2024-09-18	7.5	CVE-2024-39590 talos-cna@cisco.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oretnom23 -- simple_forum\/discussion_system	A vulnerability, which was classified as critical, was found in SourceCodester Simple Forum-Discussion System 1.0. Affected is an unknown function of the file /index.php. The manipulation of the argument page leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-09-20	8.8	CVE-2024-9032 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
owen2345--camaleon-cms	Camaleon CMS is a dynamic and advanced content management system based on Ruby on Rails. An arbitrary file write vulnerability accessible via the upload method of the MediaController allows authenticated users to write arbitrary files to any location on the web server Camaleon CMS is running on (depending on the permissions of the underlying filesystem). E.g. This can lead to a delayed remote code execution in case an attacker is able to write a Ruby file into the config/initializers/ subfolder of the Ruby on Rails application. This issue has been addressed in release version 2.8.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-18	9.9	CVE-2024-46986 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
owen2345--camaleon-cms	Camaleon CMS is a dynamic and advanced content management system based on Ruby on Rails. A path traversal vulnerability accessible via MediaController's download_private_file method allows authenticated users to download any file on the web server Camaleon CMS is running on (depending on the file permissions). This issue may lead to Information Disclosure. This issue has been addressed in release version 2.8.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-18	7.7	CVE-2024-46987 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
PickPlugins--Team Showcase	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PickPlugins Team Showcase allows Reflected XSS.This issue affects Team Showcase: from n/a through 1.22.25.	2024-09-18	7.1	CVE-2024-44002 audit@patchstack.com
playsms -- playsms	A vulnerability classified as critical has been found in playSMS 1.4.4/1.4.5/1.4.6/1.4.7. Affected is an unknown function of the file /playsms/index.php?app=main&inc=core_auth&route=forgot&op=forgot of the component Template Handler. The manipulation of the argument username/email/captcha leads to code injection. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The project maintainer was informed early about the issue. Investigation shows that playSMS up to 1.4.3 contained a fix but later versions re-introduced the flaw. As long as the latest version of the playsms/tpl package is used, the software is not affected. Version >=1.4.4 shall fix this issue for sure.	2024-09-16	9.8	CVE-2024-8880 cna@vuldb.com cna@vuldb.com cna@vuldb.com
propertyhive--PropertyHive	The PropertyHive plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.19. This is due to missing or incorrect nonce validation on the 'save_account_details' function. This makes it possible for unauthenticated attackers to edit the name, email address, and password of an administrator account via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-09-17	8.8	CVE-2024-8490 security@wordfence.com security@wordfence.com security@wordfence.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				security@wordfence.com
PTZOptics--PT30X-SDI	PTZOptics PT30X-SDI/NDI-xx before firmware 6.3.40 is vulnerable to an insufficient authentication issue. The camera does not properly enforce authentication to /cgi-bin/param.cgi when requests are sent without an HTTP Authorization header. The result is a remote and unauthenticated attacker can leak sensitive data such as usernames, password hashes, and configurations details. Additionally, the attacker can update individual configuration values or overwrite the whole file.	2024-09-17	9.1	CVE-2024-8956 disclosure@vulncheck.com disclosure@vulncheck.com
PTZOptics--PT30X-SDI	PTZOptics PT30X-SDI/NDI-xx before firmware 6.3.40 is vulnerable to an OS command injection issue. The camera does not sufficiently validate the ntp_addr configuration value which may lead to arbitrary command execution when ntp_client is started. When chained with CVE-2024-8956, a remote and unauthenticated attacker can execute arbitrary OS commands on affected devices.	2024-09-17	7.2	CVE-2024-8957 disclosure@vulncheck.com disclosure@vulncheck.com
rathena--FluxCP	FluxCP is a web-based Control Panel for rAthena servers written in PHP. A javascript injection is possible via venders/buyers list pages and shop names, that are currently not sanitized. This allows executing arbitrary javascript code on the user's browser just by visiting the shop pages. As a result all logged in to fluxcp users can have their session info stolen. This issue has been addressed in release version 1.3. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-16	7.3	CVE-2024-45799 security-advisories@github.com
Red Hat--OpenShift Service Mesh 2	A flaw was found in Envoy. It is possible to modify or manipulate headers from external clients when pass-through routes are used for the ingress gateway. This issue could allow a malicious user to forge what is logged by Envoy as a requested path and cause the Envoy proxy to make requests to internal-only services or arbitrary external systems. This is a regression of the fix for CVE-2023-27487.	2024-09-19	8.2	CVE-2024-7207 secalert@redhat.com secalert@redhat.com secalert@redhat.com
Red Hat--Red Hat Build of Keycloak	A flaw exists in the SAML signature validation method within the Keycloak XMLSignatureUtil class. The method incorrectly determines whether a SAML signature is for the full document or only for specific assertions based on the position of the signature in the XML document, rather than the Reference element used to specify the signed element. This flaw allows attackers to create crafted responses that can bypass the validation, potentially leading to privilege escalation or impersonation attacks.	2024-09-19	7.7	CVE-2024-8698 secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Enterprise Linux AI (RHEL AI)	A flaw was found in the vLLM library. A completions API request with an empty prompt will crash the vLLM API server, resulting in a denial of service.	2024-09-17	7.5	CVE-2024-8768 secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com
Red Hat--Red Hat OpenShift Container Platform 4.12	A flaw was found in OpenShift. This issue occurs due to the misuse of elevated privileges in the OpenShift Container Platform's build process. During the build initialization step, the git-clone container is run with a privileged security context, allowing unrestricted access to the node. An attacker with developer-level access can provide a crafted .gitconfig file containing commands executed during the cloning process, leading to arbitrary command execution on the worker node. An attacker running code in a privileged container could escalate their permissions on the node running the container.	2024-09-17	9.9	CVE-2024-45496 secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com
Red Hat--Red Hat OpenShift Container Platform 4.12	A flaw was found in openshift/builder. This vulnerability allows command injection via path traversal, where a malicious user can execute arbitrary commands on the OpenShift node running the builder container. When using the "Docker" strategy, executable files inside the privileged build container can be overridden using the `spec.source.secrets.secret.destinationDir` attribute of the `BuildConfig` definition. An attacker running code in a privileged container could escalate their permissions on the node running the container.	2024-09-17	9.1	CVE-2024-7387 secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com
sfs -- insuree_gl	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SFS Consulting InsureE GL allows SQL Injection.This issue affects InsureE GL: before 4.6.2.	2024-09-16	9.8	CVE-2024-6401 nvd@nist.gov iletisim@usom.gov.tr
sfs -- winsure	Improper Restriction of XML External Entity Reference vulnerability in SFS Consulting ww.Winsure allows XML Injection.This issue affects ww.Winsure: before 4.6.2.	2024-09-16	9.8	CVE-2024-7098 iletisim@usom.gov.tr
sfs -- winsure	Improper Control of Generation of Code ('Code Injection') vulnerability in SFS Consulting ww.Winsure allows Code Injection.This issue affects ww.Winsure: before 4.6.2.	2024-09-16	9.8	CVE-2024-7104 iletisim@usom.gov.tr
SKT Themes--SKT Templates Elementor & Gutenberg	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SKT Themes SKT Templates - Elementor & Gutenberg templates allows Reflected XSS.This issue affects	2024-09-17	7.1	CVE-2024-44007 audit@patchstack.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
templates	SKT Templates - Elementor & Gutenberg templates: from n/a through 6.14.			
smart-hmi -- webiq	The Windows version of WebIQ 2.15.9 is affected by a directory traversal vulnerability that allows remote attackers to read any file on the system.	2024-09-16	7.5	CVE-2024-8752 vulnreport@tenable.com
sofastack--sofa-hessian	sofa-hessian is an internal improved version of Hessian3/4 powered by Ant Group CO., Ltd. The SOFA Hessian protocol uses a blacklist mechanism to restrict deserialization of potentially dangerous classes for security protection. But there is a gadget chain that can bypass the SOFA Hessian blacklist protection mechanism, and this gadget chain only relies on JDK and does not rely on any third-party components. This issue is fixed by an update to the blacklist, users can upgrade to sofahessian version 3.5.5 to avoid this issue. Users unable to upgrade may maintain a blacklist themselves in the directory `external/serialize.blacklist`.	2024-09-19	9.8	CVE-2024-46983 security-advisories@github.com
SourceCodester--Best House Rental Management System	A vulnerability, which was classified as critical, has been found in SourceCodester Best House Rental Management System 1.0. Affected by this issue is some unknown functionality of the file /ajax.php?action=signup. The manipulation of the argument firstname/lastname/email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-09-20	7.3	CVE-2024-9039 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
spicethemes--Spice Starter Sites	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in spicethemes Spice Starter Sites allows Reflected XSS.This issue affects Spice Starter Sites: from n/a through 1.2.5.	2024-09-18	7.1	CVE-2024-44003 audit@patchstack.com
Spiffy Plugins--Spiffy Calendar	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Spiffy Plugins Spiffy Calendar allows SQL Injection.This issue affects Spiffy Calendar: from n/a through 4.9.12.	2024-09-17	7.6	CVE-2024-43969 audit@patchstack.com
SureCart--SureCart	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SureCart allows Reflected XSS.This issue affects SureCart: from n/a through 2.29.3.	2024-09-18	7.1	CVE-2024-43970 audit@patchstack.com
syscomgo -- omflow	OMFLOW from The SYSCOM Group does not properly restrict access to the system settings modification functionality, allowing remote attackers with regular privileges to update system settings or create accounts with administrator privileges, thereby gaining control of the server.	2024-09-16	8.8	CVE-2024-8779 twcert@cert.org.tw twcert@cert.org.tw
syscomgo -- omflow	OMFLOW from The SYSCOM Group has an information leakage vulnerability, allowing unauthorized remote attackers to read arbitrary system configurations. If LDAP authentication is enabled, attackers can obtain plaintext credentials.	2024-09-16	7.5	CVE-2024-8777 twcert@cert.org.tw twcert@cert.org.tw
TAKENAKA ENGINEERING CO., LTD.--HDVR-400	Improper authentication vulnerability in multiple digital video recorders provided by TAKENAKA ENGINEERING CO., LTD. allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings.	2024-09-18	8.8	CVE-2024-41929 vultures@jpcert.or.jp vultures@jpcert.or.jp
TAKENAKA ENGINEERING CO., LTD.--HDVR-400	OS command injection vulnerability in multiple digital video recorders provided by TAKENAKA ENGINEERING CO., LTD. allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings.	2024-09-18	8.8	CVE-2024-43778 vultures@jpcert.or.jp vultures@jpcert.or.jp

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
TAKENAKA ENGINEERING CO., LTD.--HDVR-400	Hidden functionality issue in multiple digital video recorders provided by TAKENAKA ENGINEERING CO., LTD. allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings.	2024-09-18	8.8	CVE-2024-47001 vultures@jpcert.or.jp vultures@jpcert.or.jp
The Document Foundation--LibreOffice	Improper Digital Signature Invalidation vulnerability in Zip Repair Mode of The Document Foundation LibreOffice allows Signature forgery vulnerability in LibreOfficeThis issue affects LibreOffice: from 24.2 before < 24.2.5.	2024-09-17	7.8	CVE-2024-7788 security@documentfoundation.org
totolink --t8_firmware	TOTOLINK AC1200 T8 v4.1.5cu.861_B20230220 has a buffer overflow vulnerability in the setWizardCfg function via the ssid5g parameter.	2024-09-16	9.8	CVE-2024-46419 cve@mitre.org
totolink --t8_firmware	TOTOLINK AC1200 T8 v4.1.5cu.861_B20230220 has a buffer overflow vulnerability in the setWiFiAclRules function via the desc parameter.	2024-09-16	9.8	CVE-2024-46451 cve@mitre.org
totolink --t8_firmware	TOTOLINK AC1200 T8 v4.1.5cu.861_B20230220 has a buffer overflow vulnerability in the UploadCustomModule function, which allows attackers to cause a Denial of Service (DoS) via the File parameter.	2024-09-16	7.5	CVE-2024-46424 cve@mitre.org
traefik--traefik	Traefik is a golang, Cloud Native Application Proxy. When a HTTP request is processed by Traefik, certain HTTP headers such as X-Forwarded-Host or X-Forwarded-Port are added by Traefik before the request is routed to the application. For a HTTP client, it should not be possible to remove or modify these headers. Since the application trusts the value of these headers, security implications might arise, if they can be modified. For HTTP/1.1, however, it was found that some of theses custom headers can indeed be removed and in certain cases manipulated. The attack relies on the HTTP/1.1 behavior, that headers can be defined as hop-by-hop via the HTTP Connection header. This issue has been addressed in release versions 2.11.9 and 3.1.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-19	9.8	CVE-2024-45410 security-advisories@github.com security-advisories@github.com security-advisories@github.com
udecode--plate	Plate is a javascript toolkit that makes it easier for you to develop with Slate, a popular framework for building text editors. One longstanding feature of Plate is the ability to add custom DOM attributes to any element or leaf using the `attributes` property. These attributes are passed to the node component using the `nodeProps` prop. It has come to our attention that this feature can be used for malicious purposes, including cross-site scripting (XSS) and information exposure (specifically, users' IP addresses and whether or not they have opened a malicious document). Note that the risk of information exposure via attributes is only relevant to applications in which web requests to arbitrary URLs are not ordinarily allowed. Plate editors that allow users to embed images from arbitrary URLs, for example, already carry the risk of leaking users' IP addresses to third parties. All Plate editors using an affected version of @udecode/plate-core are vulnerable to these information exposure attacks via the style attribute and other attributes that can cause web requests to be sent. In addition, whether or not a Plate editor is vulnerable to cross-site scripting attacks using attributes depends on a number of factors. The most likely DOM attributes to be vulnerable are href and src on links and iframes respectively. Any component that spreads {...nodeProps} onto an <a> or <iframe> element and does not later override href or src will be vulnerable to XSS. In patched versions of Plate, we have disabled element.attributes and leaf.attributes for most attribute names by default, with some exceptions including target, alt, width, height, colspan and rowspan on the link, image, video, table cell and table header cell plugins. If this is a breaking change for you, you can selectively re-enable attributes for certain plugins as follows. Please carefully research and assess the security implications of any attribute you allow, as even	2024-09-20	8.3	CVE-2024-47061 security-advisories@github.com security-advisories@github.com security-advisories@github.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	seemingly innocuous attributes such as style can be used maliciously. If you are unable to upgrade to any of the patched versions, you should use a tool like patch-package or yarn patch to remove the logic from @udecode/plate-core that adds attributes to nodeProps.			
vercel--next.js	Next.js is a React framework for building full-stack web applications. By sending a crafted HTTP request, it is possible to poison the cache of a non-dynamic server-side rendered route in the pages router (this does not affect the app router). When this crafted request is sent it could coerce Next.js to cache a route that is meant to not be cached and send a `Cache-Control: s-maxage=1, stale-while-revalidate` header which some upstream CDNs may cache as well. To be potentially affected all of the following must apply: 1. Next.js between 13.5.1 and 14.2.9, 2. Using pages router, & 3. Using non-dynamic server-side rendered routes e.g. `pages/dashboard.tsx` not `pages/blog/[slug].tsx`. This vulnerability was resolved in Next.js v13.5.7, v14.2.10, and later. We recommend upgrading regardless of whether you can reproduce the issue or not. There are no official or recommended workarounds for this issue, we recommend that users patch to a safe version.	2024-09-17	7.5	CVE-2024-46982 security-advisories@github.com security-advisories@github.com security-advisories@github.com
WC Lovers--WCFM Marketplace	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WC Lovers WCFM Marketplace allows Reflected XSS.This issue affects WCFM Marketplace: from n/a through 3.6.10.	2024-09-17	7.1	CVE-2024-44009 audit@patchstack.com
Welcart Inc.--Welcart e-Commerce	SQL injection vulnerability in Welcart e-Commerce prior to 2.11.2 allows an attacker who can login to the product to obtain or alter the information stored in the database.	2024-09-18	8.8	CVE-2024-42404 vultures@jpcert.or.jp vultures@jpcert.or.jp
WP Sunshine--Sunshine Photo Cart	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Sunshine Sunshine Photo Cart allows Reflected XSS.This issue affects Sunshine Photo Cart: from n/a through 3.2.5.	2024-09-18	7.1	CVE-2024-43971 audit@patchstack.com
WPTaskForce--WPCargo Track & Trace	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPTaskForce WPCargo Track & Trace allows SQL Injection.This issue affects WPCargo Track & Trace: from n/a through 7.0.6.	2024-09-17	9.3	CVE-2024-44004 audit@patchstack.com
Yokogawa Electric Corporation--Dual-redundant Platform for Computer (PC2CKM)	Denial of Service (DoS) vulnerability has been found in Dual-redundant Platform for Computer. If a computer on which the affected product is installed receives a large number of UDP broadcast packets in a short period, occasionally that computer may restart. If both the active and standby computers are restarted at the same time, the functionality on that computer may be temporarily unavailable.	2024-09-17	7.5	CVE-2024-8110 7168b535-132a-4efe-a076-338f829b2eb9
zitadel--zitadel	Zitadel is an open source identity management platform. ZITADEL's user account deactivation mechanism did not work correctly with service accounts. Deactivated service accounts retained the ability to request tokens, which could lead to unauthorized access to applications and resources. Versions 2.62.1, 2.61.1, 2.60.2, 2.59.3, 2.58.5, 2.57.5, 2.56.6, 2.55.8, and 2.54.10 have been released which address this issue. Users are advised t upgrade. Users unable to upgrade may instead of deactivating the service account, consider creating new credentials and replacing the old ones wherever they are used. This effectively prevents the deactivated service account from being utilized. Be sure to revoke all existing authentication keys associated with the service account and to rotate the service account's password.	2024-09-20	8.1	CVE-2024-47000 security-advisories@github.com
zitadel--zitadel	Zitadel is an open source identity management platform. ZITADEL's user grants deactivation mechanism did not work correctly. Deactivated user grants were still provided in token, which could lead to unauthorized	2024-09-20	7.3	CVE-2024-46999 security-advisories@github

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	access to applications and resources. Additionally, the management and auth API always returned the state as active or did not provide any information about the state. Versions 2.62.1, 2.61.1, 2.60.2, 2.59.3, 2.58.5, 2.57.5, 2.56.6, 2.55.8, and 2.54.10 have been released which address this issue. Users are advised to upgrade. Users unable to upgrade may explicitly remove the user grants to make sure the user does not get access anymore.			b.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
10Web--Photo Gallery by 10Web	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in 10Web Photo Gallery by 10Web allows Stored XSS.This issue affects Photo Gallery by 10Web: from n/a through 1.8.27.	2024-10-06	5.9	CVE-2024-44043 audit@patchstack.com
acekyd--Display Medium Posts	The Display Medium Posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's display_medium_posts shortcode in all versions up to, and including, 5.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-04	6.4	CVE-2024-9445 security@wordfence.com security@wordfence.com security@wordfence.com
Ada Support--Ada.cx Sentry Component	Ada.cx's Sentry configuration allowed for blind server-side request forgeries (SSRF) through the use of a data scraping endpoint.	2024-10-04	5.3	CVE-2024-9410 vulnreport@tenable.com
adreastrian--Guten Post Layout An Advanced Post Grid Collection for WordPress Gutenberg	The Guten Post Layout - An Advanced Post Grid Collection for WordPress Gutenberg plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' attribute within the 'wp:guten-post-layout/post-grid' Gutenberg block in all versions up to, and including, 1.2.4 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.	2024-10-01	6.4	CVE-2024-8288 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
Alexander Bhm--Include Fussball.de Widgets	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Alexander Böhm Include Fussball.De Widgets allows Stored XSS.This issue affects Include Fussball.De Widgets: from n/a through 4.0.0.	2024-10-05	6.5	CVE-2024-47643 audit@patchstack.com
algoritmika--Quantity Dynamic Pricing & Bulk Discounts for WooCommerce	The Quantity Dynamic Pricing & Bulk Discounts for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.8.0. 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.	2024-10-04	6.1	CVE-2024-9384 security@wordfence.com security@wordfence.com security@wordfence.com
apple -- ipados	A logic issue was addressed with improved validation. This issue is fixed in iOS 18.0.1 and iPadOS 18.0.1. A user's saved passwords may be read aloud by VoiceOver.	2024-10-04	5.5	CVE-2024-44204 product-security@apple.com
apple -- ipados	This issue was addressed with improved checks. This issue is fixed in iOS 18.0.1 and iPadOS 18.0.1. Audio messages in Messages may be able to capture a few seconds of audio before the microphone indicator is activated.	2024-10-04	4.3	CVE-2024-44207 product-security@apple.com
ARI Soft--ARI Fancy Lightbox	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ARI Soft ARI Fancy Lightbox allows Stored XSS.This issue affects ARI Fancy Lightbox: from n/a through 1.3.17.	2024-10-06	6.5	CVE-2024-47310 audit@patchstack.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				com
Ashraf--XLTab Accordions and Tabs for Elementor Page Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ashraf XLTab - Accordions and Tabs for Elementor Page Builder allows Stored XSS.This issue affects XLTab - Accordions and Tabs for Elementor Page Builder: from n/a through 1.3.	2024-10-05	6.5	CVE-2024-47375 audit@patchstack.com
Atakan Au--Automatically Hierarchic Categories in Menu	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Atakan Au Automatically Hierarchic Categories in Menu allows Stored XSS.This issue affects Automatically Hierarchic Categories in Menu: from n/a through 2.0.5.	2024-10-06	6.5	CVE-2024-47365 audit@patchstack.com
automatic-rock--SVG Complete	The SVG Complete plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.2 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 the SVG file.	2024-10-01	6.4	CVE-2024-9119 security@wordfence.com security@wordfence.com
Averta--Depicter Slider	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Averta Depicter Slider allows Stored XSS.This issue affects Depicter Slider: from n/a through 3.2.2.	2024-10-05	5.9	CVE-2024-47381 audit@patchstack.com
averta--Shortcodes and extra features for Phlox theme	The Shortcodes and extra features for Phlox theme plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in the Modern Heading and Icon Picker widgets all versions up to, and including, 2.16.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-05	6.4	CVE-2024-8486 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
AVG/Avast--Antivirus	An out-of-bounds write in the engine module in AVG/Avast Antivirus signature <24092400 released on 24/Sep/2024 on MacOS allows a malformed eml file to crash the application during file processing.	2024-10-04	5.1	CVE-2024-9481 security@nortonlifelock.com
AVG/Avast--Antivirus	An out-of-bounds write in the engine module in AVG/Avast Antivirus signature <24092400 released on 24/Sep/2024 on MacOS allows a malformed Mach-O file to crash the application during file processing.	2024-10-04	5.1	CVE-2024-9482 security@nortonlifelock.com
AVG/Avast--Antivirus	A null-pointer-dereference in the signature verification module in AVG/Avast Antivirus signature <24092400 released on 24/Sep/2024 on MacOS may allow a malformed xar file to crash the application during processing.	2024-10-04	5.1	CVE-2024-9483 security@nortonlifelock.com
AVG/Avast--Antivirus	An null-pointer-derefrence in the engine module in AVG/Avast Antivirus signature <24092400 released on 24/Sep/2024 on MacOS allows a malformed xar file to crash the application during file processing.	2024-10-04	5.1	CVE-2024-9484 security@nortonlifelock.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Axton--WP-WebAuthn	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Axton WP-WebAuthn allows Stored XSS.This issue affects WP-WebAuthn: from n/a through 1.3.1.	2024-10-06	6.5	CVE-2024-47650 audit@patchstack.com
azexo--Elastik Page Builder	The Elastik Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 0.27.4 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 the SVG file.	2024-10-01	6.4	CVE-2024-9274 security@wordfence.com security@wordfence.com
backstage--backstage	Backstage is an open framework for building developer portals. Configuration supplied through APP_CONFIG_* environment variables, for example APP_CONFIG_backend_listen_port=7007, where unexpectedly ignoring the visibility defined in configuration schema. This occurred even if the configuration schema specified that they should have backend or secret visibility. This was an intended feature of the APP_CONFIG_* way of supplying configuration, but now clearly goes against the expected behavior of the configuration system. This behavior leads to a risk of potentially exposing sensitive configuration details intended to remain private or restricted to backend processes. The issue has been resolved in version 0.3.75 of the @backstage/plugin-app-backend package. As a temporary measure, avoid supplying secrets using the APP_CONFIG_ configuration pattern. Consider alternative methods for setting secrets, such as the environment substitution available for Backstage configuration.	2024-10-03	5.8	CVE-2024-47762 security-advisories@github.com security-advisories@github.com
BdThemes--Element Pack Elementor Addons	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BdThemes Element Pack Elementor Addons allows Stored XSS.This issue affects Element Pack Elementor Addons: from n/a through 5.7.5.	2024-10-05	6.5	CVE-2024-47392 audit@patchstack.com
BdThemes--Ultimate Store Kit Elementor Addons	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BdThemes Ultimate Store Kit Elementor Addons allows Stored XSS.This issue affects Ultimate Store Kit Elementor Addons: from n/a through 2.0.5.	2024-10-05	6.5	CVE-2024-47629 audit@patchstack.com
bitpressadmin--Bit File Manager 100% Free & Open Source File Manager and Code Editor for WordPress	The Bit File Manager - 100% Free & Open Source File Manager and Code Editor for WordPress plugin for WordPress is vulnerable to Limited JavaScript File Upload in all versions up to, and including, 6.5.7. This is due to a lack of proper checks on allowed file types. This makes it possible for authenticated attackers, with Subscriber-level access and above, and granted permissions by an administrator, to upload .css and .js files, which could lead to Stored Cross-Site Scripting.	2024-10-05	6.8	CVE-2024-8743 security@wordfence.com security@wordfence.com
Blockspare--Blockspare	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Blockspare allows Stored XSS.This issue affects Blockspare: from n/a through 3.2.4.	2024-10-06	6.5	CVE-2024-47363 audit@patchstack.com
BoldThemes--Bold Page Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BoldThemes Bold Page Builder allows Stored XSS.This issue affects Bold Page Builder: from n/a through 5.1.1.	2024-10-06	6.5	CVE-2024-47298 audit@patchstack.com
BoldThemes--Bold Page Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BoldThemes Bold Page Builder allows Stored XSS.This issue affects Bold Page Builder: from n/a before 5.1.1.	2024-10-05	6.5	CVE-2024-47391 audit@patchstack.com
bPlugins LLC--Logo Carousel Clients	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in bPlugins LLC Logo Carousel - Clients logo carousel for WP	2024-10-05	6.5	CVE-2024-47631 audit@patchstack.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
logo carousel for WP	allows Stored XSS.This issue affects Logo Carousel - Clients logo carousel for WP: from n/a through 1.2.			com
Brainstorm Force--Starter Templates	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brainstorm Force Starter Templates allows Stored XSS.This issue affects Starter Templates: from n/a through 4.4.0.	2024-10-06	5.9	CVE-2024-47345 audit@patchstack.com
brian_voelker--slim_select	Slim Select 2.0 versions through 2.9.0 are affected by a potential cross-site scripting vulnerability. In select.ts:createOption(), the text variable from the user-provided Options object is assigned to an innerHTML without sanitation. Software that depends on this library to dynamically generate lists using unsanitized user-provided input may be vulnerable to cross-site scripting, resulting in attacker executed JavaScript. At this time, no patch is available.	2024-10-02	5.4	CVE-2024-9440 disclosure@vulncheck.com disclosure@vulncheck.com disclosure@vulncheck.com
brianbrey--Easy Load More	The Easy Load More plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.0.3. 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.	2024-10-01	6.1	CVE-2024-8728 security@wordfence.com security@wordfence.com
brochris--Auto Featured Image from Title	The Auto Featured Image from Title plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.3. 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.	2024-10-01	6.1	CVE-2024-8786 security@wordfence.com security@wordfence.com
cagdasdag--KB Support WordPress Help Desk and Knowledge Base	The KB Support - WordPress Help Desk and Knowledge Base plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on the 'kbs_ajax_load_front_end_replies' and 'kbs_ajax_mark_reply_as_read' functions in all versions up to, and including, 1.6.6. This makes it possible for unauthenticated attackers to read replies of any ticket, and mark any reply as read.	2024-10-01	6.5	CVE-2024-8632 security@wordfence.com security@wordfence.com security@wordfence.com
Canonical Ltd.--Juju	Vulnerable juju hook tool abstract UNIX domain socket. When combined with an attack of JUJU_CONTEXT_ID, any user on the local system with access to the default network namespace may connect to the @/var/lib/juju/agents/unit-xxxx-yyyy/agent.socket and perform actions that are normally reserved to a juju charm.	2024-10-02	6.5	CVE-2024-8037 security@ubuntu.com security@ubuntu.com
Catch Themes--Catch Base	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Catch Themes Catch Base allows Stored XSS.This issue affects Catch Base: from n/a through 3.4.6.	2024-10-06	5.1	CVE-2024-47313 audit@patchstack.com
Catch Themes--Create	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Catch Themes Create allows Stored XSS.This issue affects Create: from n/a through 2.9.1.	2024-10-06	5.1	CVE-2024-47356 audit@patchstack.com
Catch Themes--Full frame	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Catch Themes Full frame allows Stored XSS.This issue affects Full frame: from n/a through 2.7.2.	2024-10-06	5.1	CVE-2024-44010 audit@patchstack.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				com
cconover--Relogo	The Relogo plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 0.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-10-01	6.4	CVE-2024-9269 security@wordfence.com security@wordfence.com
Cisco--Cisco Data Center Network Manager	A vulnerability in the REST API endpoints of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to read or write files on an affected device. This vulnerability exists because of missing authorization controls on some REST API endpoints. An attacker could exploit this vulnerability by sending crafted API requests to an affected endpoint. A successful exploit could allow the attacker to perform limited network-admin functions such as reading device configuration information, uploading files, and modifying uploaded files. Note: This vulnerability only affects a subset of REST API endpoints and does not affect the web-based management interface.	2024-10-02	6.3	CVE-2024-20438 ykramarz@cisco.com
Cisco--Cisco Data Center Network Manager	A vulnerability in the Cisco Nexus Dashboard Fabric Controller (NDFC) software, formerly Cisco Data Center Network Manager (DCNM), could allow an attacker with access to a backup file to view sensitive information. This vulnerability is due to the improper storage of sensitive information within config only and full backup files. An attacker could exploit this vulnerability by parsing the contents of a backup file that is generated from an affected device. A successful exploit could allow the attacker to access sensitive information, including NDFC-connected device credentials, the NDFC site manager private key, and the scheduled backup file encryption key.	2024-10-02	6.3	CVE-2024-20448 ykramarz@cisco.com
Cisco--Cisco Data Center Network Manager	A vulnerability in a logging function of Cisco Nexus Dashboard Fabric Controller (NDFC) and Cisco Nexus Dashboard Orchestrator (NDO) could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because HTTP proxy credentials could be recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view HTTP proxy server admin credentials in clear text that are configured on Nexus Dashboard to reach an external network. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information.	2024-10-02	6.3	CVE-2024-20490 ykramarz@cisco.com
Cisco--Cisco Data Center Network Manager	A vulnerability in a specific REST API endpoint of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to learn sensitive information on an affected device. This vulnerability is due to insufficient authorization controls on the affected REST API endpoint. An attacker could exploit this vulnerability by sending crafted API requests to the affected endpoint. A successful exploit could allow the attacker to download config only or full backup files and learn sensitive configuration information. This vulnerability only affects a specific REST API endpoint and does not affect the web-based management interface.	2024-10-02	5.7	CVE-2024-20441 ykramarz@cisco.com
Cisco--Cisco Data Center Network Manager	A vulnerability in Cisco Nexus Dashboard Fabric Controller (NDFC), formerly Cisco Data Center Network Manager (DCNM), could allow an authenticated, remote attacker with network-admin privileges to perform a command injection attack against an affected device. This vulnerability is due to insufficient validation of command arguments. An attacker could exploit this vulnerability by submitting crafted command arguments to a specific REST API endpoint. A successful exploit could allow the attacker to overwrite sensitive files or crash a specific container, which would restart on its own, causing a low-impact denial of service (DoS) condition.	2024-10-02	5.5	CVE-2024-20444 ykramarz@cisco.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cisco--Cisco Data Center Network Manager	A vulnerability in a specific REST API endpoint of Cisco NDFC could allow an authenticated, low-privileged, remote attacker to upload or delete files on an affected device. This vulnerability exists because of missing authorization controls on the affected REST API endpoint. An attacker could exploit this vulnerability by sending crafted API requests to the affected endpoint. A successful exploit could allow the attacker to upload files into a specific container or delete files from a specific folder within that container. This vulnerability only affects a specific REST API endpoint and does not affect the web-based management interface.	2024-10-02	5.4	CVE-2024-20477 ykramarz@cisco.com
Cisco--Cisco Identity Services Engine Software	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability is due to a lack of proper data protection mechanisms for certain configuration settings. An attacker with Read-Only Administrator privileges could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to view device credentials that are normally not visible to Read-Only Administrators.	2024-10-02	6.5	CVE-2024-20515 ykramarz@cisco.com
Cisco--Cisco Meraki MX Firmware	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition in the AnyConnect service on an affected device. This vulnerability is due to insufficient resource management when establishing TLS/SSL sessions. An attacker could exploit this vulnerability by sending a series of crafted TLS/SSL messages to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.	2024-10-02	5.8	CVE-2024-20500 ykramarz@cisco.com
Cisco--Cisco Meraki MX Firmware	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to insufficient resource management while establishing SSL VPN sessions. An attacker could exploit this vulnerability by sending a series of crafted HTTPS requests to the VPN server of an affected device. A successful exploit could allow the attacker to cause the Cisco AnyConnect VPN server to stop accepting new connections, preventing new SSL VPN connections from being established. Existing SSL VPN sessions are not impacted. Note: When the attack traffic stops, the Cisco AnyConnect VPN server recovers gracefully without requiring manual intervention.	2024-10-02	5.8	CVE-2024-20502 ykramarz@cisco.com
Cisco--Cisco Meraki MX Firmware	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to hijack an AnyConnect VPN session or cause a denial of service (DoS) condition for individual users of the AnyConnect VPN service on an affected device. This vulnerability is due to weak entropy for handlers that are used during the VPN authentication process as well as a race condition that exists in the same process. An attacker could exploit this vulnerability by correctly guessing an authentication handler and then sending crafted HTTPS requests to an affected device. A successful exploit could allow the attacker to take over the AnyConnect VPN session from a target user or prevent the target user from establishing an AnyConnect VPN session with the affected device.	2024-10-02	5.8	CVE-2024-20509 ykramarz@cisco.com
Cisco--Cisco Meraki MX Firmware	A vulnerability in the Cisco AnyConnect VPN server of Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices could allow an unauthenticated, remote attacker to cause a DoS condition for targeted users of the AnyConnect service on an affected device. This vulnerability is due to insufficient entropy for handlers that are used during SSL VPN session establishment. An unauthenticated attacker could exploit this vulnerability by brute forcing valid session handlers. An authenticated attacker could exploit this vulnerability by connecting to the AnyConnect VPN service of an affected device to retrieve a valid session handler and, based on that handler, predict further valid session handlers. The attacker	2024-10-02	5.8	CVE-2024-20513 ykramarz@cisco.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	would then send a crafted HTTPS request using the brute-forced or predicted session handler to the AnyConnect VPN server of the device. A successful exploit could allow the attacker to terminate targeted SSL VPN sessions, forcing remote users to initiate new VPN connections and reauthenticate.			
Cisco--Cisco Nexus Dashboard Insights	A vulnerability in a logging function of Cisco Nexus Dashboard Insights could allow an attacker with access to a tech support file to view sensitive information. This vulnerability exists because remote controller credentials are recorded in an internal log that is stored in the tech support file. An attacker could exploit this vulnerability by accessing a tech support file that is generated from an affected system. A successful exploit could allow the attacker to view remote controller admin credentials in clear text. Note: Best practice is to store debug logs and tech support files safely and to share them only with trusted parties because they may contain sensitive information.	2024-10-02	6.3	CVE-2024-20491 ykramarz@cisco.com
Cisco--Cisco Nexus Dashboard Orchestrator	A vulnerability in the SSL/TLS implementation of Cisco Nexus Dashboard Orchestrator (NDO) could allow an unauthenticated, remote attacker to intercept sensitive information from an affected device. This vulnerability exists because the Cisco NDO Validate Peer Certificate site management feature validates the certificates for Cisco Application Policy Infrastructure Controller (APIC), Cisco Cloud Network Controller (CNC), and Cisco Nexus Dashboard only when a new site is added or an existing one is reregistered. An attacker could exploit this vulnerability by using machine-in-the-middle techniques to intercept the traffic between the affected device and Cisco NDO and then using a crafted certificate to impersonate the affected device. A successful exploit could allow the attacker to learn sensitive information during communications between these devices.	2024-10-02	5.9	CVE-2024-20385 ykramarz@cisco.com
Cisco--Cisco Nexus Dashboard	A vulnerability in the REST API endpoints of Cisco Nexus Dashboard could allow an authenticated, low-privileged, remote attacker to perform limited Administrator actions on an affected device. This vulnerability is due to insufficient authorization controls on some REST API endpoints. An attacker could exploit this vulnerability by sending crafted API requests to an affected endpoint. A successful exploit could allow the attacker to perform limited Administrator functions such as viewing portions of the web UI, generating config only or full backup files, and deleting tech support files. This vulnerability only affects a subset of REST API endpoints and does not affect the web-based management interface.	2024-10-02	5.4	CVE-2024-20442 ykramarz@cisco.com
Cisco--Cisco Small Business RV Series Router Firmware	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. In order to exploit this vulnerability, the attacker must have valid admin credentials. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system.	2024-10-02	6.5	CVE-2024-20470 ykramarz@cisco.com
Cisco--Cisco Small Business RV Series Router Firmware	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	2024-10-02	6.8	CVE-2024-20516 ykramarz@cisco.com
Cisco--Cisco Small Business RV Series	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected	2024-10-02	6.8	CVE-2024-20517 ykramarz@cisco.co

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Router Firmware	device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.			m
Cisco--Cisco Small Business RV Series Router Firmware	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	2024-10-02	6.5	CVE-2024-20518 ykramarz@cisco.com
Cisco--Cisco Small Business RV Series Router Firmware	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	2024-10-02	6.5	CVE-2024-20519 ykramarz@cisco.com
Cisco--Cisco Small Business RV Series Router Firmware	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	2024-10-02	6.5	CVE-2024-20520 ykramarz@cisco.com
Cisco--Cisco Small Business RV Series Router Firmware	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to execute arbitrary code as the root user. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the root user.	2024-10-02	6.5	CVE-2024-20521 ykramarz@cisco.com
Cisco--Cisco Small Business RV Series Router Firmware	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	2024-10-02	6.5	CVE-2024-20522 ykramarz@cisco.com
Cisco--Cisco Small Business RV Series	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated,	2024-10-02	6.8	CVE-2024-20523 ykramarz@cisco.co

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Router Firmware	Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.			m
Cisco--Cisco Small Business RV Series Router Firmware	A vulnerability in the web-based management interface of Cisco Small Business RV042, RV042G, RV320, and RV325 Routers could allow an authenticated, Administrator-level, remote attacker to cause an unexpected reload of an affected device, resulting in a denial of service (DoS) condition. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. This vulnerability is due to improper validation of user input that is in incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	2024-10-02	6.8	CVE-2024-20524 ykramarz@cisco.com
Cisco--Cisco TelePresence Video Communication Server (VCS) Expressway	A vulnerability in the restricted shell of Cisco Expressway Series could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have Administrator-level credentials with read-write privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a series of crafted CLI commands. A successful exploit could allow the attacker to escape the restricted shell and gain root privileges on the underlying operating system of the affected device. Note: Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices.	2024-10-02	6	CVE-2024-20492 ykramarz@cisco.com
Cisco--Cisco Unified Computing System (Managed)	A vulnerability in the Redfish API of Cisco UCS B-Series, Cisco UCS Managed C-Series, and Cisco UCS X-Series Servers could allow an authenticated, remote attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending crafted commands through the Redfish API on an affected device. A successful exploit could allow the attacker to elevate privileges to root.	2024-10-02	6.5	CVE-2024-20365 ykramarz@cisco.com
Clinical-Genomics--scout	Scout is a web-based visualizer for VCF-files. Open redirect vulnerability allows performing phishing attacks on users by redirecting them to malicious page. /login API endpoint is vulnerable to open redirect attack via next parameter due to absence of sanitization logic. Additionally, due to lack of scheme validation, HTTPS Downgrade Attack can be performed on the users. This vulnerability is fixed in 4.89.	2024-09-30	5.4	CVE-2024-47530 security-advisories@github.com security-advisories@github.com
Clinical-Genomics--scout	Scout is a web-based visualizer for VCF-files. Due to the lack of sanitization in the filename, it is possible bypass intended file extension and make users download malicious files with any extension. With malicious content injected inside the file data and users unknowingly downloading it and opening may lead to the compromise of users' devices or data. This vulnerability is fixed in 4.89.	2024-09-30	4.6	CVE-2024-47531 security-advisories@github.com security-advisories@github.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cliogrow--Clio Grow	The Clio Grow plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.0.2. 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.	2024-10-04	6.1	CVE-2024-8802 security@wordfence.com security@wordfence.com
code-projects--Restaurant Reservation System	A vulnerability has been found in code-projects Restaurant Reservation System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /filter2.php. The manipulation of the argument from/to leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "from" to be affected. But it must be assumed that parameter "to" is affected as well.	2024-10-02	6.3	CVE-2024-9429 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Condless--Cities Shipping Zones for WooCommerce	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Condless Cities Shipping Zones for WooCommerce allows PHP Local File Inclusion.This issue affects Cities Shipping Zones for WooCommerce: from n/a through 1.2.7.	2024-10-05	6.6	CVE-2024-47309 audit@patchstack.com
connekthq--WordPress Infinite Scroll Ajax Load More	The WordPress Infinite Scroll - Ajax Load More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button_label' parameter in all versions up to, and including, 7.1.2 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.	2024-10-02	6.4	CVE-2024-8505 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
contact-banker--WordPress Captcha Plugin by Captcha Bank	The WordPress Captcha Plugin by Captcha Bank plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 4.0.36. 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.	2024-10-04	6.1	CVE-2024-9375 security@wordfence.com security@wordfence.com
cornelraiu-1--WP Search Analytics	The WP Search Analytics plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.4.10. 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.	2024-10-01	6.1	CVE-2024-9209 security@wordfence.com security@wordfence.com
CozyThemes--Cozy Blocks	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CozyThemes Cozy Blocks allows Stored XSS.This issue affects Cozy Blocks: from n/a through 2.0.11.	2024-10-06	6.5	CVE-2024-47355 audit@patchstack.com
cvat-ai--cvat	Computer Vision Annotation Tool (CVAT) is an interactive video and image annotation tool for computer vision. An attacker with a CVAT account may retrieve certain information about any project, task, job or membership resource on the CVAT instance. The information exposed in this way is the same as the information returned on a GET request to the resource. In addition, the attacker can also alter the default source and target storage associated with any project or task. Upgrade to CVAT 2.19.1 or any later version to fix the issue.	2024-09-30	5.4	CVE-2024-47172 security-advisories@github.com security-advisories@github.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cyberhobo--Geo Mashup	The Geo Mashup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's geo_mashup_visible_posts_list shortcode in all versions up to, and including, 1.13.13 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.	2024-10-01	6.4	CVE-2024-8990 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
dartiss--Code Embed	The Code Embed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's script embed functionality in all versions up to, and including, 2.4 due to insufficient restrictions on who can utilize the functionality. 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.	2024-10-04	6.4	CVE-2024-8804 security@wordfence.com security@wordfence.com
daveshine--Gravity Forms Toolbar	The Gravity Forms Toolbar plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 1.7.0 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.	2024-10-01	6.1	CVE-2024-8718 security@wordfence.com security@wordfence.com security@wordfence.com
deTheme--DethemeKit For Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in deTheme DethemeKit For Elementor allows Stored XSS.This issue affects DethemeKit For Elementor: from n/a through 2.1.7.	2024-10-05	6.5	CVE-2024-47632 audit@patchstack.com
dgamoni--LocateAndFilter	The LocateAndFilter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.6.14 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-10-01	6.4	CVE-2024-9304 security@wordfence.com security@wordfence.com
dotcamp -- ultimate_blocks	The Ultimate Blocks WordPress plugin before 3.2.2 does not validate and escape some of its block attributes before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	2024-09-30	5.4	CVE-2024-8536 contact@wpscan.com
draytek -- vigor3910_firmware	Stored XSS, by authenticated users, is caused by poor sanitization of the Login Page Greeting message in DrayTek Vigor310 devices through 4.3.2.6.	2024-10-03	5.4	CVE-2024-41587 cve@mitre.org cve@mitre.org
dvankooten--MC4WP: Mailchimp Top Bar	The MC4WP: Mailchimp Top Bar plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.6.0. 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.	2024-10-02	6.1	CVE-2024-9210 security@wordfence.com security@wordfence.com security@wordfence.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ElementInvader--ElementInvader Addons for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ElementInvader ElementInvader Addons for Elementor allows Stored XSS.This issue affects ElementInvader Addons for Elementor: from n/a through 1.2.7.	2024-10-05	6.5	CVE-2024-47630 audit@patchstack.com
ESAFENET--CDG	A vulnerability was found in ESAFENET CDG V5. It has been rated as critical. Affected by this issue is some unknown functionality of the file /MultiServerBackService?path=1. The manipulation of the argument fileId leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-05	6.3	CVE-2024-9536 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
ESAFENET--CDG	A vulnerability was found in ESAFENET CDG V5. It has been rated as critical. Affected by this issue is the function delCatelogs of the file /CDGServer3/document/Catelogs;logindojojs?command=DelCatelogs. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-10-06	6.3	CVE-2024-9560 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Esri--ArcGIS Enterprise Web App Builder	There is a stored Cross-site Scripting vulnerability in Esri Portal for ArcGIS Enterprise Sites versions 10.8.1 - 11.1 that may allow a remote, authenticated attacker to create a crafted link that is stored in the site configuration which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high. The attack could disclose a privileged token which may result in the attacker gaining full control of the Portal.	2024-10-04	4.8	CVE-2024-25702 psirt@esri.com
Esri--Enterprise Web App Builder	There is a stored Cross-site Scripting vulnerability in Esri Portal for ArcGIS Enterprise versions 10.8.1 - 10.9.1 that may allow a remote, authenticated attacker to create a crafted link that is stored in the Layer Showcase application configuration which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high. The attack could disclose a privileged token which may result in the attacker gaining full control of the Portal.	2024-10-04	4.8	CVE-2024-25694 psirt@esri.com
Esri--Portal for ArcGIS Enterprise Experience Builder	There is a stored Cross-site Scripting vulnerability in Esri Portal for ArcGIS Enterprise Experience Builder versions 10.8.1 - 11.1 that may allow a remote, authenticated attacker to create a crafted link that is stored in the Experience Builder Embed widget which when loaded could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high. The attack could disclose a privileged token which may result in the attacker gaining full control of the Portal.	2024-10-04	4.8	CVE-2024-25701 psirt@esri.com
Esri--Portal for ArcGIS Enterprise Experience Builder	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser.	2024-10-04	4.6	CVE-2024-38036 psirt@esri.com
Esri--Portal	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 11.1, 10.9.1 and 10.8.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser.	2024-10-04	6.1	CVE-2024-25691 psirt@esri.com
Esri--Portal	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 11.0 and 10.9.1 that may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks.	2024-10-04	6.1	CVE-2024-38037 psirt@esri.com
Esri--Portal	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser.	2024-10-04	6.1	CVE-2024-38038 psirt@esri.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Esri--Portal	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 10.8.1 - 11.2 that may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks.	2024-10-04	6.1	CVE-2024-8148 psirt@esri.com
Esri--Portal	There is an HTML injection vulnerability in Esri Portal for ArcGIS versions 11.0 and below that may allow a remote, authenticated attacker to create a crafted link which when clicked could render arbitrary HTML in the victim's browser (no stateful change made or customer data rendered).	2024-10-04	5.4	CVE-2024-38039 psirt@esri.com
Esri--Portal	There is a reflected cross site scripting in Esri Portal for ArcGIS 11.1 and below on Windows and Linux x64 allows a remote authenticated attacker with administrative access to supply a crafted string which could potentially execute arbitrary JavaScript code in the their own browser (Self XSS). A user cannot be phished into clicking a link to execute code.	2024-10-04	4.8	CVE-2024-25707 psirt@esri.com
Esri--Portal	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 11.1 and 11.2 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser.	2024-10-04	4.6	CVE-2024-8149 psirt@esri.com
Essential Plugin--Meta slider and carousel with lightbox	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Essential Plugin Meta slider and carousel with lightbox allows Stored XSS.This issue affects Meta slider and carousel with lightbox: from n/a through 2.0.1.	2024-10-06	6.5	CVE-2024-47307 audit@patchstack.com
expressjs--express	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Express. This vulnerability affects the use of the Express Response object. This issue impacts Express: from 3.4.5 before 4.0.0.	2024-10-03	4.7	CVE-2024-9266 36c7be3b-2937-45df-85ea-ca7133ea542c
Fahad Mahmood--WP Datepicker	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Fahad Mahmood WP Datepicker allows Stored XSS.This issue affects WP Datepicker: from n/a through 2.1.1.	2024-10-06	5.9	CVE-2024-44042 audit@patchstack.com
Faronics--DeepFreeze	Deep Freeze 9.00.020.5760 is vulnerable to an out-of-bounds read vulnerability by triggering the 0x70014 IOCTL code of the FarDisk.sys driver.	2024-10-03	6.4	CVE-2024-8159 help@fluidattacks.com help@fluidattacks.com
fishpie--PDF Image Generator	The PDF Image Generator plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.5.6. 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.	2024-10-01	6.1	CVE-2024-9241 security@wordfence.com security@wordfence.com
FreePBX--security-reporting	OSS Endpoint Manager is an endpoint manager module for FreePBX. OSS Endpoint Manager module activation can allow authenticated web users unauthorized access to read system files with the permissions of the webserver process. This vulnerability is fixed in 14.0.4.	2024-10-01	6.8	CVE-2024-47071 security-advisories@github.com security-advisories@github.com
galdub--Free Responsive	The Free Responsive Testimonials, Social Proof Reviews, and Customer Reviews - Stars Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting	2024-10-01	6.4	CVE-2024-8989 security@wordfenc

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Testimonials, Social Proof Reviews, and Customer Reviews Stars Testimonials	via the plugin's stars_testimonials shortcode in all versions up to, and including, 3.3.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			e.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
GhozyLab, Inc.--Gallery Lightbox	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in GhozyLab, Inc. Gallery Lightbox allows Stored XSS.This issue affects Gallery Lightbox: from n/a through 1.0.0.39.	2024-10-05	5.9	CVE-2024-47623 audit@patchstack.com
ghuger--Custom Banners	The Custom Banners plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.3. 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.	2024-10-01	6.1	CVE-2024-8799 security@wordfence.com security@wordfence.com
GitLab--GitLab	An issue has been discovered in GitLab EE/CE affecting all versions starting from 8.0 before 16.4. The product did not sufficiently warn about security implications of granting merge rights to protected branches.	2024-10-01	6.6	CVE-2023-3441 cve@gitlab.com cve@gitlab.com cve@gitlab.com
grandplugins--AVIF Uploader	The AVIF & SVG Uploader plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in version 1.1.0 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 the SVG file.	2024-10-01	6.4	CVE-2024-9060 security@wordfence.com security@wordfence.com security@wordfence.com
guillaume-lostweb--WP Cleanup and Basic Functions	The WP Cleanup and Basic Functions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.2.1 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 the SVG file.	2024-10-05	6.4	CVE-2024-9455 security@wordfence.com security@wordfence.com
hashthemes--Hash Form Drag & Drop Form Builder	The Hash Form - Drag & Drop Form Builder plugin for WordPress is vulnerable to limited file uploads due to a misconfigured file type validation in the 'handleUpload' function in all versions up to, and including, 1.1.9. This makes it possible for unauthenticated attackers to upload files that are excluded from both the 'allowedExtensions' and 'unallowed_extensions' arrays on the affected site's server, including files that may contain cross-site scripting.	2024-10-05	6.1	CVE-2024-9417 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
HelpieWP--Accordion & FAQ Helpie WordPress Accordion FAQ	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in HelpieWP Accordion & FAQ - Helpie WordPress Accordion FAQ Plugin allows Stored XSS.This issue affects Accordion & FAQ - Helpie WordPress Accordion FAQ Plugin: from n/a through 1.27.	2024-10-05	5.9	CVE-2024-47647 audit@patchstack.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Plugin				
Hewlett Packard Enterprise--HPE IceWall Agent products	A security vulnerability in HPE IceWall Agent products could be exploited remotely to cause a Cross-Site Request Forgery (CSRF) in the login flow.	2024-10-03	4.3	CVE-2024-42504 security-alert@hpe.com
HP Inc.--Certain HP LaserJet Printers	Certain HP LaserJet printers may potentially experience a denial of service when a user sends a raw JPEG file to the printer. The printer displays a "JPEG Unsupported" message which may not clear, potentially blocking queued print jobs.	2024-10-02	5.3	CVE-2024-9423 hp-security-alert@hp.com
IBM--WebSphere Application Server	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2024-09-30	4.8	CVE-2024-45073 psirt@us.ibm.com
icegram--Email Subscribers by Icegram Express Email Marketing, Newsletters, Automation for WordPress & WooCommerce	The Email Subscribers by Icegram Express - Email Marketing, Newsletters, Automation for WordPress & WooCommerce plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 5.7.34. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes.	2024-10-02	5.4	CVE-2024-8254 security@wordfence.com security@wordfence.com security@wordfence.com
icopydoc--YML for Yandex Market	The YML for Yandex Market plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'page' parameter in all versions up to, and including, 4.7.2 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.	2024-10-02	6.1	CVE-2024-9378 security@wordfence.com security@wordfence.com security@wordfence.com
ILLID--Advanced Woo Labels	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ILLID Advanced Woo Labels allows Stored XSS.This issue affects Advanced Woo Labels: from n/a through 2.01.	2024-10-05	6.5	CVE-2024-47622 audit@patchstack.com
ishitaka--XO Slider	The XO Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'get_slider' function in all versions up to, and including, 3.8.6 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.	2024-10-01	6.4	CVE-2024-8324 security@wordfence.com security@wordfence.com security@wordfence.com
iworks--PWA easy way to Progressive Web App	The PWA - easy way to Progressive Web App plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.6.3 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 the SVG file.	2024-10-02	6.4	CVE-2024-8967 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfenc

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				e.com
James Low--CSS JS Files	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in James Low CSS JS Files allows Path Traversal.This issue affects CSS JS Files: from n/a through 1.5.0.	2024-10-05	4.9	CVE-2024-9146 audit@patchstack.com
Jegtheme--Jeg Elementor Kit	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jegtheme Jeg Elementor Kit allows Stored XSS.This issue affects Jeg Elementor Kit: from n/a through 2.6.8.	2024-10-05	6.5	CVE-2024-47390 audit@patchstack.com
jkohlbach--Store Exporter for WooCommerce Export Products, Export Orders, Export Subscriptions, and More	The Store Exporter for WooCommerce - Export Products, Export Orders, Export Subscriptions, and More plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.7.2.1. 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.	2024-10-01	6.1	CVE-2024-8793 security@wordfence.com security@wordfence.com
joelcj91--Loggedin Limit Active Logins	The Loggedin - Limit Active Logins plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.3.1. 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. This is only exploitable when the leave a review notice is present.	2024-10-01	6.1	CVE-2024-9228 security@wordfence.com security@wordfence.com
Katie Seaborn--Zotpress	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Katie Seaborn Zotpress allows Stored XSS.This issue affects Zotpress: from n/a through 7.3.10.	2024-10-05	6.5	CVE-2024-47621 audit@patchstack.com
kau-boy--Hello World	The Hello World plugin for WordPress is vulnerable to Arbitrary File Reading in all versions up to, and including, 2.1.1 via the hello_world_lyric() function. This makes it possible for authenticated attackers, with subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	2024-10-01	6.5	CVE-2024-9224 security@wordfence.com security@wordfence.com security@wordfence.com
Keap--Keap Official Opt-in Forms	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Keap Keap Official Opt-in Forms allows Stored XSS.This issue affects Keap Official Opt-in Forms: from n/a through 2.0.1.	2024-10-05	6.5	CVE-2024-47642 audit@patchstack.com
Kevon Adonis--WP Abstracts	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kevon Adonis WP Abstracts allows Stored XSS.This issue affects WP Abstracts: from n/a through 2.6.5.	2024-10-06	5.9	CVE-2024-44045 audit@patchstack.com
Kiteworks--OwnCloud	Cross site request forgery in Kiteworks OwnCloud allows an unauthenticated attacker to forge requests. If a request has no Authorization header, it is created with an empty string as value by a rewrite rule. The CSRF check is done by comparing the header value to null, meaning that the existing CSRF check is bypassed in this case. An attacker can, for example, create a new administrator account if the request is executed in the browser of an authenticated victim.	2024-10-01	6.8	CVE-2023-7273 a341c0d1-ebf7-493f-a84e-38cf86618674 a341c0d1-ebf7-493f-a84e-

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				38cf86618674
kraftplugins--Demo Importer Plus	The Demo Importer Plus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.0.1 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 the SVG file.	2024-10-02	6.4	CVE-2024-9172 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
Kraftplugins--Mega Elements	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kraftplugins Mega Elements allows Stored XSS.This issue affects Mega Elements: from n/a through 1.2.4.	2024-10-06	6.5	CVE-2024-47343 audit@patchstack.com
LA-Studio--LA-Studio Element Kit for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LA-Studio LA-Studio Element Kit for Elementor allows Stored XSS.This issue affects LA-Studio Element Kit for Elementor: from n/a through 1.3.9.3.	2024-10-05	6.5	CVE-2024-47628 audit@patchstack.com
Leap13--Premium Blocks Gutenberg Blocks for WordPress	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Leap13 Premium Blocks - Gutenberg Blocks for WordPress allows Stored XSS.This issue affects Premium Blocks - Gutenberg Blocks for WordPress: from n/a through 2.1.33.	2024-10-06	6.5	CVE-2024-47368 audit@patchstack.com
Leevio--Happy Addons for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Leevio Happy Addons for Elementor allows Stored XSS.This issue affects Happy Addons for Elementor: from n/a through 3.12.0.	2024-10-06	6.5	CVE-2024-47357 audit@patchstack.com
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. Stored Cross-Site Scripting (XSS) can be achieved by uploading a new Background for a Custom Map. Users with "admin" role can set background for a custom map, this allow the upload of SVG file that can contain XSS payload which will trigger on load. This led to Stored Cross-Site Scripting (XSS). The vulnerability is fixed in 24.9.0.	2024-10-01	5.4	CVE-2024-47528 security-advisories@github.com security-advisories@github.com
LinkGraph--Search Atlas SEO	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LinkGraph Search Atlas SEO allows Stored XSS.This issue affects Search Atlas SEO: from n/a through 1.8.2.	2024-10-05	5.9	CVE-2024-47387 audit@patchstack.com
Linux and Microsoft Windows--Octopus Server	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Linux and Microsoft Windows Octopus Server on Windows, Linux allows SQL Injection.This issue affects Octopus Server: from 2024.1.0 before 2024.1.13038, from 2024.2.0 before 2024.2.9482, from 2024.3.0 before 2024.3.12766.	2024-09-30	4.3	CVE-2024-9194 security@octopus.com
LiteSpeed Technologies--LiteSpeed Cache	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LiteSpeed Technologies LiteSpeed Cache allows Stored XSS.This issue affects LiteSpeed Cache: from n/a through 6.5.0.2.	2024-10-05	6.5	CVE-2024-47373 audit@patchstack.com
madalinungureanu--Paid Membership	The Paid Membership Subscriptions - Effortless Memberships, Recurring Payments & Content Restriction plugin for WordPress is vulnerable to Reflected Cross-Site	2024-10-02	6.1	CVE-2024-9222 security@wordfenc

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Subscriptions Effortless Memberships, Recurring Payments & Content Restriction	Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.12.8. 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.			e.com security@wordfence.com security@wordfence.com
MagePeople Team--Multipurpose Ticket Booking Manager	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MagePeople Team Multipurpose Ticket Booking Manager allows Stored XSS.This issue affects Multipurpose Ticket Booking Manager: from n/a through 4.2.2.	2024-10-06	5.9	CVE-2024-44037 audit@patchstack.com
ManageEngine--Analytics Plus	Zohocorp ManageEngine Analytics Plus versions before 5410 and Zoho Analytics On-Premise versions before 5410 are vulnerable to Path traversal.	2024-10-03	6.5	CVE-2024-91000fc0942c-577d-436f-ae8e-945763c79b020fc0942c-577d-436f-ae8e-945763c79b02
Martin Gibson--IdeaPush	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Martin Gibson IdeaPush allows Stored XSS.This issue affects IdeaPush: from n/a through 8.66.	2024-10-06	5.9	CVE-2024-44041 audit@patchstack.com
mascotdevelopers--R Animated Icon Plugin	The R Animated Icon Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0 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 the SVG file.	2024-10-01	6.4	CVE-2024-9272 security@wordfence.com security@wordfence.com
memberful--Memberful Membership Plugin	The Memberful - Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'memberful_buy_subscription_link' and 'memberful_podcasts_link' shortcodes in all versions up to, and including, 1.73.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-04	6.4	CVE-2024-9242 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
migumello--Aggregator Advanced Settings	The Aggregator Advanced Settings plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-10-04	6.4	CVE-2024-9368 security@wordfence.com security@wordfence.com
miunosoft--Auto Amazon Links Amazon Associates Affiliate Plugin	The Auto Amazon Links - Amazon Associates Affiliate Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 5.4.2. 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.	2024-10-04	6.1	CVE-2024-9349 security@wordfence.com security@wordfence.com security@wordfenc

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				e.com
Move addons--Move Addons for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Move addons Move Addons for Elementor allows Stored XSS.This issue affects Move Addons for Elementor: from n/a through 1.3.4.	2024-10-06	6.5	CVE-2024-47364 audit@patchstack.com
moveaddons--Move Addons for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in moveaddons Move Addons for Elementor allows Stored XSS.This issue affects Move Addons for Elementor: from n/a through 1.3.3.	2024-10-01	6.5	CVE-2024-47396 audit@patchstack.com
n/a--cocoon	Versions of the package cocoon before 0.4.0 are vulnerable to Reusing a Nonce, Key Pair in Encryption when the encrypt, wrap, and dump functions are sequentially called. An attacker can generate the same ciphertext by creating a new encrypted message with the same cocoon object. **Note:** The issue does NOT affect objects created with Cocoon::new which utilizes ThreadRng.	2024-10-02	4.5	CVE-2024-21530 report@snyk.io report@snyk.io report@snyk.io report@snyk.io report@snyk.io
n/a--git-shallow-clone	All versions of the package git-shallow-clone are vulnerable to Command injection due to missing sanitization or mitigation flags in the process variable of the gitShallowClone function.	2024-10-01	5.3	CVE-2024-21531 report@snyk.io report@snyk.io
n/a--n/a	An issue was discovered in Infinera hiT 7300 5.60.50. Cleartext storage of sensitive information in the memory of the @CT desktop management application allows guest OS administrators to obtain various users' passwords by accessing memory dumps of the desktop application.	2024-09-30	6.5	CVE-2024-28807 cve@mitre.org
n/a--n/a	An issue was discovered in Infinera hiT 7300 5.60.50. Sensitive information inside diagnostic files (exported by the @CT application) allows an attacker to achieve loss of confidentiality by analyzing these files.	2024-09-30	6.6	CVE-2024-28810 cve@mitre.org
n/a--n/a	In Nintendo Mario Kart 8 Deluxe before 3.0.3, the LAN/LDN local multiplayer implementation allows a remote attacker to exploit a stack-based buffer overflow upon deserialization of session information via a malformed browse-reply packet, aka KartLANPwn. The victim is not required to join a game session with an attacker. The victim must open the "Wireless Play" (or "LAN Play") menu from the game's title screen, and an attacker nearby (LDN) or on the same LAN network as the victim can send a crafted reply packet to the victim's console. This enables a remote attacker to obtain complete denial-of-service on the game's process, or potentially, remote code execution on the victim's console. The issue is caused by incorrect use of the Nintendo Pia library,	2024-09-30	6.3	CVE-2024-45200 cve@mitre.org cve@mitre.org
n/a--n/a	Bandisoft BandiView 7.05 is vulnerable to Incorrect Access Control in sub_0x3d80fc via a crafted POC file.	2024-10-03	6.5	CVE-2024-45870 cve@mitre.org
n/a--n/a	Bandisoft BandiView 7.05 is Incorrect Access Control via sub_0x232bd8 resulting in denial of service (DOS).	2024-10-03	6.3	CVE-2024-45871 cve@mitre.org
n/a--n/a	Bandisoft BandiView 7.05 is vulnerable to Buffer Overflow via sub_0x410d1d. The vulnerability occurs due to insufficient validation of PSD files.	2024-10-03	6.3	CVE-2024-45872 cve@mitre.org
n/a--n/a	Giflib Project v5.2.2 is vulnerable to a heap buffer overflow via gif2rgb.	2024-09-30	6.5	CVE-2024-45993 cve@mitre.org cve@mitre.org

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	Scriptcase v9.10.023 and before is vulnerable to Cross Site Scripting (XSS) in proj_new.php via the Descricao parameter.	2024-10-01	6.1	CVE-2024-46079 cve@mitre.org
n/a--n/a	A remote code execution (RCE) vulnerability in the component /admin/store.php of Emlog Pro before v2.3.15 allows attackers to use remote file downloads and self-extract fucntions to upload webshells to the target server, thereby obtaining system privileges.	2024-09-30	6.3	CVE-2024-46540 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	TP-Link Tapo P125M and Kasa KP125M v1.0.3 was discovered to improperly validate certificates, allowing attackers to eavesdrop on communications and access sensitive information via a man-in-the-middle attack.	2024-09-30	6.3	CVE-2024-46548 cve@mitre.org
n/a--n/a	An XSS vulnerability was discovered in Veritas Data Insight before 7.1. It allows a remote attacker to inject an arbitrary web script into an HTTP request that could reflect back to an authenticated user without sanitization if executed by that user.	2024-10-04	6.1	CVE-2024-47854 cve@mitre.org
n/a--n/a	In SonarSource SonarQube 10.4 through 10.5 before 10.6, a vulnerability was discovered in the authorizations/group-memberships API endpoint that allows SonarQube users with the administrator role to inject blind SQL commands.	2024-10-04	6.7	CVE-2024-47911 cve@mitre.org
n/a--n/a	A cross-site scripting (XSS) vulnerability has been identified in Flatpress 1.3. This vulnerability allows an attacker to inject malicious scripts into web pages viewed by other users.	2024-10-02	5.4	CVE-2024-33210 cve@mitre.org
n/a--n/a	PCAN-Ethernet Gateway FD before 1.3.0 and PCAN-Ethernet Gateway before 2.11.0 are vulnerable to Command injection via shell metacharacters in a Software Update to processing.php.	2024-10-01	5.6	CVE-2024-44610 cve@mitre.org cve@mitre.org
n/a--n/a	An issue in Malwarebytes Premium Security v5.0.0.883 allows attackers to execute arbitrary code via placing crafted binaries into unspecified directories. NOTE: Malwarebytes argues that this issue requires admin privileges and that the contents cannot be altered by non-admin users.	2024-10-01	5.7	CVE-2024-44744 cve@mitre.org cve@mitre.org
n/a--n/a	A Stored Cross-Site Scripting (XSS) vulnerability in Solvait 24.4.2 allows remote attackers to inject malicious scripts into the application. This issue arises due to insufficient input validation and sanitization in "Intrest" feature.	2024-09-30	5.4	CVE-2024-45920 cve@mitre.org
n/a--n/a	Scriptcase v9.10.023 and before is vulnerable to Cross Site Scripting (XSS). An authenticated user can craft malicious payloads in the To-Do List. The assigned user will trigger a stored XSS, which is particularly dangerous because tasks are assigned to various users on the platform.	2024-10-01	5.4	CVE-2024-46081 cve@mitre.org
n/a--n/a	Scriptcase v.9.10.023 and before is vulnerable to Cross Site Scripting (XSS) in nm_cor.php via the form and field parameters.	2024-10-01	5.4	CVE-2024-46082 cve@mitre.org cve@mitre.org
n/a--n/a	Scriptcase v9.10.023 and before is vulnerable to Cross Site Scripting (XSS). An authenticated user can craft malicious payloads using the messages feature, which allows the injection of malicious code into any user's account on the platform. It is important to note that regular users can trigger actions for administrator users.	2024-10-01	5.4	CVE-2024-46083 cve@mitre.org
n/a--n/a	DrayTek Vigor3910 devices through 4.3.2.6 are vulnerable to stored Cross Site Scripting (XSS) by authenticated users due to poor sanitization of the router name.	2024-10-03	4.7	CVE-2024-41583 cve@mitre.org cve@mitre.org
n/a--n/a	DrayTek Vigor3910 devices through 4.3.2.6 are vulnerable to reflected XSS by authenticated users, caused by missing validation of the sFormAuthStr parameter.	2024-10-03	4.7	CVE-2024-41584 cve@mitre.org

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				cve@mitre.org
n/a--n/a	Zenario 9.7.61188 allows authenticated admin users to upload PDF files containing malicious code into the target system. If the PDF file is accessed through the website, it can trigger a Cross Site Scripting (XSS) attack.	2024-10-02	4.8	CVE-2024-45960 cve@mitre.org
n/a--n/a	October 3.6.30 allows an authenticated admin account to upload a PDF file containing malicious JavaScript into the target system. If the file is accessed through the website, it could lead to a Cross-Site Scripting (XSS) attack or execute arbitrary code via a crafted JavaScript to the target.	2024-10-02	4.7	CVE-2024-45962 cve@mitre.org
n/a--n/a	Zenario 9.7.61188 is vulnerable to Cross Site Scripting (XSS) in the Image library via the "Organizer tags" field.	2024-10-02	4.8	CVE-2024-45964 cve@mitre.org
n/a--n/a	Contao 5.4.1 allows an authenticated admin account to upload a SVG file containing malicious javascript code into the target system. If the file is accessed through the website, it could lead to a Cross-Site Scripting (XSS) attack or execute arbitrary code via a crafted javascript to the target.	2024-10-02	4.7	CVE-2024-45965 cve@mitre.org
n/a--n/a	Pagekit 1.0.18 is vulnerable to Cross Site Scripting (XSS) in index.php/admin/site/widget.	2024-10-01	4.7	CVE-2024-45967 cve@mitre.org
n/a--n/a	A reflected cross-site scripting (XSS) vulnerability on the homepage of Metronic Admin Dashboard Template v2.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload.	2024-09-30	4.8	CVE-2024-46475 cve@mitre.org
n/a--ThingsBoard	A vulnerability has been found in ThingsBoard up to 3.7.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component HTTP RPC API. The manipulation leads to resource consumption. 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. Upgrading to version 3.7.1 is able to address this issue. It is recommended to upgrade the affected component. The vendor was informed on 2024-07-24 about this vulnerability and announced the release of 3.7.1 for the second half of September 2024.	2024-10-01	5.3	CVE-2024-9358 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
nerdpressteam--Smart Custom 404 Error Page	The Smart Custom 404 Error Page plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via $_SERVER['REQUEST_URI'] in all versions up to, and including, 11.4.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-04	6.1	CVE-2024-9204 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
Nicejob--NiceJob	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Nicejob NiceJob allows Stored XSS.This issue affects NiceJob: from n/a before 3.6.5.	2024-10-06	6.5	CVE-2024-44025 audit@patchstack.com
NicheAddons--Charity Addon for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NicheAddons Charity Addon for Elementor allows Stored XSS.This issue affects Charity Addon for Elementor: from n/a through 1.3.0.	2024-10-06	6.5	CVE-2024-44026 audit@patchstack.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
NicheAddons--Medical Addon for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NicheAddons Medical Addon for Elementor allows Stored XSS.This issue affects Medical Addon for Elementor: from n/a through 1.4.	2024-10-06	6.5	CVE-2024-44024 audit@patchstack.com
NicheAddons--Primary Addon for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NicheAddons Primary Addon for Elementor allows Stored XSS.This issue affects Primary Addon for Elementor: from n/a through 1.5.7.	2024-10-06	6.5	CVE-2024-44033 audit@patchstack.com
NicheAddons--Restaurant & Cafe Addon for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NicheAddons Restaurant & Cafe Addon for Elementor allows Stored XSS.This issue affects Restaurant & Cafe Addon for Elementor: from n/a through 1.5.5.	2024-10-06	6.5	CVE-2024-44032 audit@patchstack.com
NLnet Labs--Unbound	NLnet Labs Unbound up to and including version 1.21.0 contains a vulnerability when handling replies with very large RRsets that it needs to perform name compression for. Malicious upstreams responses with very large RRsets can cause Unbound to spend a considerable time applying name compression to downstream replies. This can lead to degraded performance and eventually denial of service in well orchestrated attacks. The vulnerability can be exploited by a malicious actor querying Unbound for the specially crafted contents of a malicious zone with very large RRsets. Before Unbound replies to the query it will try to apply name compression which was an unbounded operation that could lock the CPU until the whole packet was complete. Unbound version 1.21.1 introduces a hard limit on the number of name compression calculations it is willing to do per packet. Packets that need more compression will result in semi-compressed packets or truncated packets, even on TCP for huge messages, to avoid locking the CPU for long. This change should not affect normal DNS traffic.	2024-10-03	5.3	CVE-2024-8508 sep@nlnetlabs.nl
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server contains a vulnerability where a user may cause an out-of-bounds read issue by releasing a shared memory region while it is in use. A successful exploit of this vulnerability may lead to denial of service.	2024-10-01	4.9	CVE-2024-0116 psirt@nvidia.com
optinhound--Easy WordPress Subscribe Optin Hound	The Easy WordPress Subscribe - Optin Hound plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.4.3. 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.	2024-10-01	6.1	CVE-2024-9267 security@wordfence.com security@wordfence.com security@wordfence.com
Paul Bearne--Author Avatars List/Block	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Paul Bearne Author Avatars List/Block allows Stored XSS.This issue affects Author Avatars List/Block: from n/a through 2.1.21.	2024-10-05	6.5	CVE-2024-47370 audit@patchstack.com
Payflex--Payflex Payment Gateway	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Payflex Payflex Payment Gateway.This issue affects Payflex Payment Gateway: from n/a through 2.6.1.	2024-10-05	4.7	CVE-2024-47646 audit@patchstack.com
PickPlugins--Accordion	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PickPlugins Accordion accordions allows Stored XSS.This issue affects Accordion: from n/a through 2.2.99.	2024-10-06	6.5	CVE-2024-47342 audit@patchstack.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
PickPlugins--Post Grid and Gutenberg Blocks	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PickPlugins Post Grid and Gutenberg Blocks allows Stored XSS.This issue affects Post Grid and Gutenberg Blocks: from n/a through 2.2.89.	2024-10-06	6.5	CVE-2024-47340 audit@patchstack.com
Pierre Lebedel--Kodex Posts likes	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pierre Lebedel Kodex Posts likes allows Stored XSS.This issue affects Kodex Posts likes: from n/a through 2.5.0.	2024-10-06	5.9	CVE-2024-44036 audit@patchstack.com
plainware--ShiftController Employee Shift Scheduling	The ShiftController Employee Shift Scheduling plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via URL keys in all versions up to, and including, 4.9.66 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.	2024-10-04	6.1	CVE-2024-9435 security@wordfence.com security@wordfence.com security@wordfence.com
Plainware--ShiftController Employee Shift Scheduling	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Plainware ShiftController Employee Shift Scheduling allows Stored XSS.This issue affects ShiftController Employee Shift Scheduling: from n/a through 4.9.64.	2024-10-06	5.9	CVE-2024-44040 audit@patchstack.com
planet -- gs-4210-24p2s_firmware	Certain switch models from PLANET Technology have a Hard-coded Credential in the password recovering functionality, allowing an unauthenticated attacker to connect to the device via the serial console and use this credential to reset any user's password.	2024-09-30	6.8	CVE-2024-8449 twcert@cert.org.tw twcert@cert.org.tw
planet -- gs-4210-24p2s_firmware	The swctrl service is used to detect and remotely manage PLANET Technology devices. For certain switch models, the authentication tokens used during communication with this service are encoded user passwords. Due to insufficient strength, unauthorized remote attackers who intercept the packets can directly crack them to obtain plaintext passwords.	2024-09-30	5.9	CVE-2024-8455 twcert@cert.org.tw twcert@cert.org.tw
planet -- gs-4210-24p2s_firmware	Certain switch models from PLANET Technology use an insecure hashing function to hash user passwords without being salted. Remote attackers with administrator privileges can read configuration files to obtain the hash values, and potentially crack them to retrieve the plaintext passwords.	2024-09-30	4.9	CVE-2024-8453 twcert@cert.org.tw twcert@cert.org.tw
planet -- gs-4210-24p2s_firmware	Certain switch models from PLANET Technology have a web application that does not properly validate specific parameters, allowing remote authenticated users with administrator privileges to inject arbitrary JavaScript, leading to Stored XSS attack.	2024-09-30	4.8	CVE-2024-8457 twcert@cert.org.tw twcert@cert.org.tw
planet -- gs-4210-24p2s_firmware	Certain switch models from PLANET Technology store SNMPv3 users' passwords in plaintext within the configuration files, allowing remote attackers with administrator privileges to read the file and obtain the credentials.	2024-09-30	4.9	CVE-2024-8459 twcert@cert.org.tw twcert@cert.org.tw

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Pluck CMS--Pluck CMS	An incorrect limitation of a path to a restricted directory (path traversal) has been detected in Pluck CMS, affecting version 4.7.18. An unauthenticated attacker could extract sensitive information from the server via the absolute path of a file located in the same directory or subdirectory as the module, but not from recursive directories.	2024-10-01	5.3	CVE-2024-9405 cve-coordination@incibe.es
pomerium--pomerium	Pomerium is an identity and context-aware access proxy. The Pomerium databroker service is responsible for managing all persistent Pomerium application state. Requests to the databroker service API are authorized by the presence of a JSON Web Token (JWT) signed by a key known by all Pomerium services in the same deployment. However, incomplete validation of this JWT meant that some service account access tokens would incorrectly be treated as valid for the purpose of databroker API authorization. Improper access to the databroker API could allow exfiltration of user info, spoofing of user sessions, or tampering with Pomerium routes, policies, and other settings. A Pomerium deployment is susceptible to this issue if all of the following conditions are met, you have issued a service account access token using Pomerium Zero or Pomerium Enterprise, the access token has an explicit expiration date in the future, and the core Pomerium databroker gRPC API is not otherwise secured by network access controls. This vulnerability is fixed in 0.27.1.	2024-10-02	6.8	CVE-2024-47616 security-advisories@github.com security-advisories@github.com security-advisories@github.com
prontotools--Login Logout Shortcode	The Login Logout Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' parameter in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-04	6.4	CVE-2024-9421 security@wordfence.com security@wordfence.com security@wordfence.com
Quillforms--Quill Forms	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Quillforms Quill Forms allows Stored XSS.This issue affects Quill Forms: from n/a through 3.7.0.	2024-10-05	6.5	CVE-2024-47393 audit@patchstack.com
QuomodoSoft--ElementsReady Addons for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in QuomodoSoft ElementsReady Addons for Elementor allows Stored XSS.This issue affects ElementsReady Addons for Elementor: from n/a through 6.4.0.	2024-10-06	6.5	CVE-2024-47329 audit@patchstack.com
quomodosoft--QS Dark Mode Plugin	The QS Dark Mode Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.9 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 the SVG file.	2024-10-01	6.4	CVE-2024-9118 security@wordfence.com security@wordfence.com security@wordfence.com
radiustheme -- the_post_grid	The Post Grid WordPress plugin before 7.5.0 does not sanitise and escape some of its Grid settings, which could allow high privilege users such as Editor and above to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	2024-09-30	4.8	CVE-2024-3635 contact@wpscan.com
rainbowgeek--SEOPress On-site SEO	The SEOPress - On-site SEO plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 8.1.1. 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.	2024-10-02	6.1	CVE-2024-9225 security@wordfence.com security@wordfence.com security@wordfenc

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				e.com
rankmath--Rank Math SEO AI SEO Tools to Dominate SEO Rankings	The Rank Math SEO - AI SEO Tools to Dominate SEO Rankings plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check on the 'update_metadata' function in all versions up to, and including, 1.0.228. This makes it possible for unauthenticated attackers to insert new and update existing metadata beginning with 'rank_math', and delete arbitrary existing user metadata and term metadata. Deleting existing usermeta can cause a loss of access to the administrator dashboard for any registered users, including Administrators.	2024-10-05	6.5	CVE-2024-9161 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
Red Hat--Red Hat Enterprise Linux 8	A vulnerability was found in Golang FIPS OpenSSL. This flaw allows a malicious user to randomly cause an uninitialized buffer length variable with a zeroed buffer to be returned in FIPS mode. It may also be possible to force a false positive match between non-equal hashes when comparing a trusted computed hmac sum to an untrusted input sum if an attacker can send a zeroed buffer in place of a pre-computed sum. It is also possible to force a derived key to be all zeros instead of an unpredictable value. This may have follow-on implications for the Go TLS stack.	2024-10-01	6.5	CVE-2024-9355 secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com
Red Hat--Red Hat Enterprise Linux 8	A flaw was found in Go. When FIPS mode is enabled on a system, container runtimes may incorrectly handle certain file paths due to improper validation in the containers/common Go library. This flaw allows an attacker to exploit symbolic links and trick the system into mounting sensitive host directories inside a container. This issue also allows attackers to access critical host files, bypassing the intended isolation between containers and the host system.	2024-10-01	5.4	CVE-2024-9341 secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com
Red Hat--Red Hat Enterprise Linux 8	A vulnerability exists in the bind-propagation option of the Dockerfile RUN --mount instruction. The system does not properly validate the input passed to this option, allowing users to pass arbitrary parameters to the mount instruction. This issue can be exploited to mount sensitive directories from the host into a container during the build process and, in some cases, modify the contents of those mounted files. Even if SELinux is used, this vulnerability can bypass its protection by allowing the source directory to be relabeled to give the container access to host files.	2024-10-01	4.7	CVE-2024-9407 secalert@redhat.com secalert@redhat.com
remydcf--Re:WP	The Re:WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-10-04	6.4	CVE-2024-9271 security@wordfence.com security@wordfence.com security@wordfence.com
Revolution Slider--Slider Revolution	The Slider Revolution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 6.7.18 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary	2024-10-01	6.4	CVE-2024-8107 security@wordfence.com security@wordfenc

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	web scripts in pages that will execute whenever a user accesses the SVG file. By default, this can only be exploited by administrators, but the ability to use and configure Slider Revolution can be extended to authors.			e.com security@wordfence.com
Rometheme--RomethemeKit For Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Rometheme RomethemeKit For Elementor allows Stored XSS.This issue affects RomethemeKit For Elementor: from n/a through 1.5.0.	2024-10-05	6.5	CVE-2024-47626 audit@patchstack.com
rumbletalk--RumbleTalk Live Group Chat HTML5	The RumbleTalk Live Group Chat - HTML5 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'rumbletalk-admin-button' shortcode in all versions up to, and including, 6.3.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-01	6.4	CVE-2024-8720 security@wordfence.com security@wordfence.com
Salon Booking System--Salon booking system	Authorization Bypass Through User-Controlled Key vulnerability in Salon Booking System Salon booking system.This issue affects Salon booking system: from n/a through 10.9.	2024-10-05	4.3	CVE-2024-47316 audit@patchstack.com
sanrl--RabbitLoader Website Speed Optimization for improving Core Web Vital metrics with Cache, Image Optimization, and more	The RabbitLoader - Website Speed Optimization for improving Core Web Vital metrics with Cache, Image Optimization, and more plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.21.0. 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.	2024-10-02	6.1	CVE-2024-8800 security@wordfence.com security@wordfence.com security@wordfence.com
Schneider Elektronik--Series 700	An unauthenticated remote attacker may use the devices traffic capture without authentication to grab plaintext administrative credentials.	2024-10-02	6.5	CVE-2024-35294 info@cert.vde.com
SeedProd--Coming Soon Page, Under Construction & Maintenance Mode by SeedProd	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SeedProd Coming Soon Page, Under Construction & Maintenance Mode by SeedProd allows Stored XSS.This issue affects Coming Soon Page, Under Construction & Maintenance Mode by SeedProd: from n/a through 6.17.4.	2024-10-06	5.9	CVE-2024-47299 audit@patchstack.com
shawfactor--LH Copy Media File	The LH Copy Media File plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.08. 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.	2024-10-01	6.1	CVE-2024-9220 security@wordfence.com security@wordfence.com
sigmadevs--Easy Demo Importer A Modern One-Click Demo Import Solution	The Easy Demo Importer - A Modern One-Click Demo Import Solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.1.2 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 the SVG file.	2024-10-04	6.4	CVE-2024-9071 security@wordfence.com security@wordfence.com security@wordfence.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Sonarr--Sonarr	Sonarr - CWE-601: URL Redirection to Untrusted Site ('Open Redirect')	2024-10-06	6.1	CVE-2024-45247 cna@cyber.gov.il
soumettre--Soumettre.fr	The Soumettre.fr plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the soumettre_disconnect_gateway function in all versions up to, and including, 2.1.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to disconnect the gateway and delete the API key.	2024-10-01	4.3	CVE-2024-8675 security@wordfence.com security@wordfence.com
spicethemes--Spice Starter Sites	The Spice Starter Sites plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the spice_starter_sites_importer_creater function in all versions up to, and including, 1.2.5. This makes it possible for unauthenticated attackers to import demo content.	2024-10-01	5.3	CVE-2024-8430 security@wordfence.com security@wordfence.com
sulu--sulu	Sulu is a PHP content management system. This vulnerability allows an attacker to inject arbitrary HTML/JavaScript code through the media download URL in Sulu CMS. It affects the SuluMediaBundle component. The vulnerability is a Reflected Cross-Site Scripting (XSS) issue, which could potentially allow attackers to steal sensitive information, manipulate the website's content, or perform actions on behalf of the victim. This vulnerability is fixed in 2.6.5 and 2.5.21.	2024-10-03	6.1	CVE-2024-47617 security-advisories@github.com security-advisories@github.com security-advisories@github.com
techjewel--Contact Form Plugin by Fluent Forms for Quiz, Survey, and Drag & Drop WP Form Builder	The Contact Form Plugin by Fluent Forms for Quiz, Survey, and Drag & Drop WP Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via form label fields in all versions up to, and including, 5.1.19 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with access to edit forms (administrator by default), to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-05	4.9	CVE-2024-9528 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
TECHNO SUPPORT COMPANY--Smart-tab Android app	Smart-tab Android app installed April 2023 or earlier contains an active debug code vulnerability. If this vulnerability is exploited, an attacker with physical access to the device may exploit the debug function to gain access to the OS functions, escalate the privilege, change the device's settings, or spoof devices in other rooms.	2024-09-30	6.8	CVE-2024-41999 vultures@jpcert.or.jp vultures@jpcert.or.jp
TemeGUM--Gum Elementor Addon	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in TemeGUM Gum Elementor Addon allows Stored XSS.This issue affects Gum Elementor Addon: from n/a through 1.3.6.	2024-10-06	6.5	CVE-2024-44027 audit@patchstack.com
TemeGUM--Gum Elementor Addon	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in TemeGUM Gum Elementor Addon allows Stored XSS.This issue affects Gum Elementor Addon: from n/a through 1.3.7.	2024-10-06	6.5	CVE-2024-44035 audit@patchstack.com
themehigh--Checkout Field Editor (Checkout	The Checkout Field Editor (Checkout Manager) for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'render_review_request_notice' function in all versions up to, and including, 2.0.3	2024-10-04	4.7	CVE-2024-8499 security@wordfence.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Manager) for WooCommerce	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.			security@wordfence.com security@wordfence.com
ThemeKraft--BuddyForms	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeKraft BuddyForms allows Stored XSS.This issue affects BuddyForms: from n/a through 2.8.12.	2024-10-05	5.9	CVE-2024-47377 audit@patchstack.com
ThemeLooks--Enter Addons	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeLooks Enter Addons allows Stored XSS.This issue affects Enter Addons: from n/a through 2.1.8.	2024-10-05	6.5	CVE-2024-47625 audit@patchstack.com
ThemeNcode LLC--TNC PDF viewer	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeNcode LLC TNC PDF viewer allows Stored XSS.This issue affects TNC PDF viewer: from n/a through 3.1.0.	2024-10-05	5.9	CVE-2024-47372 audit@patchstack.com
themes4wp--Popularis Extra	The Popularis Extra plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.2.6. 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.	2024-10-04	6.1	CVE-2024-9353 security@wordfence.com security@wordfence.com security@wordfence.com
Themify--Themify WooCommerce Product Filter	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themify Themify - WooCommerce Product Filter allows Stored XSS.This issue affects Themify - WooCommerce Product Filter: from n/a through 1.5.1.	2024-10-06	5.9	CVE-2024-44046 audit@patchstack.com
themifyme--Themify Builder	The Themify Builder plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 7.6.2. 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.	2024-10-05	6.1	CVE-2024-9385 security@wordfence.com security@wordfence.com security@wordfence.com
thevisionofhamza--BerqWP Automated All-In-One PageSpeed Optimization for Core Web Vitals, Cache, CDN, Images, CSS, and JavaScript	The BerqWP - Automated All-In-One PageSpeed Optimization Plugin for Core Web Vitals, Cache, CDN, Images, CSS, and JavaScript plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'url' parameter in all versions up to, and including, 2.1.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-10-02	6.1	CVE-2024-9344 security@wordfence.com security@wordfence.com security@wordfence.com
TinyPNG--TinyPNG	Cross-Site Request Forgery (CSRF) vulnerability in TinyPNG.This issue affects TinyPNG: from n/a through 3.4.3.	2024-10-05	5.4	CVE-2024-47635 audit@patchstack.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
torstenbulk--DK PDF	The DK PDF plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.9.6. 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.	2024-10-01	6.1	CVE-2024-8727 security@wordfence.com security@wordfence.com
Tribulant--Slideshow Gallery	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tribulant Slideshow Gallery allows Stored XSS.This issue affects Slideshow Gallery: from n/a through 1.8.3.	2024-10-05	5.9	CVE-2024-47376 audit@patchstack.com
Trustmary--Review & testimonial widgets	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Trustmary Review & testimonial widgets allows Stored XSS.This issue affects Review & testimonial widgets: from n/a through 1.0.5.	2024-10-06	6.5	CVE-2024-44022 audit@patchstack.com
tychesoftwares--Product Delivery Date for WooCommerce Lite	The Product Delivery Date for WooCommerce - Lite plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.7.3. 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. This is only exploitable when notices are present.	2024-10-04	6.1	CVE-2024-9345 security@wordfence.com security@wordfence.com security@wordfence.com
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 plugin's 'um_loggedin' shortcode in all versions up to, and including, 2.8.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-10-04	6.4	CVE-2024-8519 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
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 Cross-Site Request Forgery in all versions up to, and including, 2.8.6. This is due to missing or incorrect nonce validation on the admin_init or user_action_hook function. This makes it possible for unauthenticated attackers to modify a users membership status via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-10-04	5.3	CVE-2024-8520 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfenc

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				e.com
Unknown--Slider by 10Web	The Slider by 10Web WordPress plugin before 1.2.59 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	2024-09-30	4.8	CVE-2024-8283 contact@wpscan.com
Unknown--Starbox	The Starbox WordPress plugin before 3.5.3 does not properly render social media profiles URLs in certain contexts, like the malicious user's profile or pages where the starbox shortcode is used, which may be abused by users with at least the contributor role to conduct Stored XSS attacks.	2024-09-30	5.4	CVE-2024-8239 contact@wpscan.com
VdoCipher--VdoCipher	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in VdoCipher allows Stored XSS.This issue affects VdoCipher: from n/a through 1.29.	2024-10-05	6.5	CVE-2024-47639 audit@patchstack.com
Vladimir Statsenko--Terms descriptions	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Vladimir Statsenko Terms descriptions allows Stored XSS.This issue affects Terms descriptions: from n/a through 3.4.6.	2024-10-06	5.9	CVE-2024-47336 audit@patchstack.com
vowelweb--Ibtana WordPress Website Builder	The Ibtana - WordPress Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' attribute within the 'wp:ive/ive-productscarousel' Gutenberg block in all versions up to, and including, 1.2.4.4 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.	2024-10-02	6.4	CVE-2024-8282 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
Walter Pinem--WP MyLinks	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Walter Pinem WP MyLinks allows Stored XSS.This issue affects WP MyLinks: from n/a through 1.0.6.	2024-10-05	5.9	CVE-2024-47371 audit@patchstack.com
Webangon--The Pack Elementor addons	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Webangon The Pack Elementor addons allows Stored XSS.This issue affects The Pack Elementor addons: from n/a through 2.0.8.8.	2024-10-05	5.9	CVE-2024-47383 audit@patchstack.com
Webvitaly--Page-list	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Webvitaly Page-list allows Stored XSS.This issue affects Page-list: from n/a through 5.6.	2024-10-05	6.5	CVE-2024-47382 audit@patchstack.com
wowDevs--Sky Addons for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in wowDevs Sky Addons for Elementor allows Stored XSS.This issue affects Sky Addons for Elementor: from n/a through 2.5.11.	2024-10-06	6.5	CVE-2024-47332 audit@patchstack.com
WP Travel--WP Travel Gutenberg Blocks	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Travel WP Travel Gutenberg Blocks allows Stored XSS.This issue affects WP Travel Gutenberg Blocks: from n/a through 3.6.0.	2024-10-05	6.5	CVE-2024-47627 audit@patchstack.com
WP Travel--WP Travel	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Travel allows Stored XSS.This issue affects WP Travel: from n/a through 9.3.1.	2024-10-06	5.9	CVE-2024-44039 audit@patchstack.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				com
wpblockart--Magazine Blocks Blog Designer, Magazine & Newspaper Website Builder, Page Builder with Posts Blocks, Post Grid	The Magazine Blocks - Blog Designer, Magazine & Newspaper Website Builder, Page Builder with Posts Blocks, Post Grid plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.3.14. 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.	2024-10-02	6.1	CVE-2024-9218 security@wordfence.com security@wordfence.com security@wordfence.com
wpblockshub--WP Blocks Hub	The WP Blocks Hub plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.2 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 the SVG file.	2024-10-04	6.4	CVE-2024-9372 security@wordfence.com security@wordfence.com
wpcentrics--Fish and Ships Most flexible shipping table rate. A WooCommerce shipping rate	The Fish and Ships - Most flexible shipping table rate. A WooCommerce shipping rate plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.5.9. 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.	2024-10-04	6.1	CVE-2024-9237 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
wpdevelop--WP Booking Calendar	The WP Booking Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 10.6 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. In addition, site administrators have the option to grant lower-level users with access to manage the plugin's settings which may extend this vulnerability to those users.	2024-10-04	4.4	CVE-2024-9306 security@wordfence.com security@wordfence.com
WPDeveloper--Essential Blocks for Gutenberg	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloper Essential Blocks for Gutenberg allows Stored XSS.This issue affects Essential Blocks for Gutenberg: from n/a through 4.8.4.	2024-10-05	6.5	CVE-2024-47385 audit@patchstack.com
WPDeveloperr--Confetti Fall Animation	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloperr Confetti Fall Animation allows Stored XSS.This issue affects Confetti Fall Animation: from n/a through 1.3.0.	2024-09-30	6.5	CVE-2024-47641 audit@patchstack.com
WPVibes--Elementor Addon Elements	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPVibes Elementor Addon Elements allows Stored XSS.This issue affects Elementor Addon Elements: from n/a through 1.13.6.	2024-10-06	6.5	CVE-2024-47366 audit@patchstack.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zephyrproject-rtos--Zephyr	In ascs_cp_rsp_add in /subsys/bluetooth/audio/ascs.c, an unchecked tailroom could lead to a global buffer overflow.	2024-10-04	6.3	CVE-2024-6442 vulnerabilities@zephyrproject.org
zephyrproject-rtos--Zephyr	In utf8_trunc in zephyr/lib/utils/utf8.c, last_byte_p can point to one byte before the string pointer if the string is empty.	2024-10-04	6.3	CVE-2024-6443 vulnerabilities@zephyrproject.org
zephyrproject-rtos--Zephyr	No proper validation of the length of user input in olcp_ind_handler in zephyr/subsys/bluetooth/services/ots/ots_client.c.	2024-10-04	6.3	CVE-2024-6444 vulnerabilities@zephyrproject.org
ZKteco--iClock v3.1-168	ZKteco - CWE 200 Exposure of Sensitive Information to an Unauthorized Actor	2024-10-06	4.3	CVE-2024-45250 cna@cyber.gov.il
Zoho Forms--Zoho Forms	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Zoho Forms allows Stored XSS.This issue affects Zoho Forms: from n/a through 4.0.	2024-10-05	6.5	CVE-2024-47633 audit@patchstack.com
Apple--iOS and iPadOS	This issue was addressed through improved state management. This issue is fixed in iOS 17.7 and iPadOS 17.7, iOS 18 and iPadOS 18. Private Browsing tabs may be accessed without authentication.	2024-09-17	5.3	CVE-2024-44127 product-security@apple.com product-security@apple.com
Apple--iOS and iPadOS	An authentication issue was addressed with improved state management. This issue is fixed in iOS 18 and iPadOS 18. Private Browsing tabs may be accessed without authentication.	2024-09-17	5.3	CVE-2024-44202 product-security@apple.com
Apple--macOS	The issue was addressed with improved checks. This issue is fixed in visionOS 2, macOS Sequoia 15. A malicious app with root privileges may be able to modify the contents of system files.	2024-09-17	6	CVE-2024-40825 product-security@apple.com product-security@apple.com
astrasecuritysuite--WP Hardening (discontinued)	The WP Hardening - Fix Your WordPress Security plugin for WordPress is vulnerable to Security Feature Bypass in all versions up to, and including, 1.2.6. This is due to use of an incorrect regular expression within the "Stop User Enumeration" feature. This makes it possible for unauthenticated attackers to bypass intended security restrictions and expose site usernames.	2024-09-18	5.3	CVE-2024-6641 security@wordfence.com security@wordfence.com
backstage--backstage	Backstage is an open framework for building developer portals. A malicious actor with authenticated access to a Backstage instance with the catalog backend plugin installed is able to interrupt the service using a specially crafted query to the catalog API. This has been fixed in the `1.26.0` release of the `@backstage/plugin-catalog-backend`. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-17	6.5	CVE-2024-45815 security-advisories@github.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
backstage--backstage	Backstage is an open framework for building developer portals. When using the AWS S3 or GCS storage provider for TechDocs it is possible to access content in the entire storage bucket. This can leak contents of the bucket that are not intended to be accessible, as well as bypass permission checks in Backstage. This has been fixed in the 1.10.13 release of the `@backstage/plugin-techdocs-backend` package. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-17	6.5	CVE-2024-45816 security-advisories@github.com
backstage--backstage	Backstage is an open framework for building developer portals. An attacker with control of the contents of the TechDocs storage buckets is able to inject executable scripts in the TechDocs content that will be executed in the victim's browser when browsing documentation or navigating to an attacker provided link. This has been fixed in the 1.10.13 release of the `@backstage/plugin-techdocs-backend` package. users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-17	6.5	CVE-2024-46976 security-advisories@github.com
CIRCUTOR--CIRCUTOR Q-SMT	An attacker with no knowledge of the current users in the web application, could build a dictionary of potential users and check the server responses as it indicates whether or not the user is present in CIRCUTOR Q-SMT in its firmware version 1.0.4.	2024-09-18	5.3	CVE-2024-8891 cve-coordination@incibe.es
CIRCUTOR--CIRCUTOR TCP2RS+	Vulnerability in CIRCUTOR TCP2RS+ firmware version 1.3b, which could allow an attacker to modify any configuration value, even if the device has the user/password authentication option enabled, without authentication by sending packets through the UDP protocol and port 2000, deconfiguring the device and thus disabling its use. This equipment is at the end of its useful life cycle.	2024-09-18	5.3	CVE-2024-8892 cve-coordination@incibe.es
code-projects--Crud Operation System	A vulnerability, which was classified as critical, was found in code-projects Crud Operation System 1.0. Affected is an unknown function of the file updata.php. The manipulation of the argument sid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-09-20	6.3	CVE-2024-9011 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
code-projects--Online Quiz Site	A vulnerability, which was classified as critical, has been found in code-projects Online Quiz Site 1.0. This issue affects some unknown processing of the file showtest.php. The manipulation of the argument subid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-09-20	6.3	CVE-2024-9009 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
code-projects--Restaurant Reservation System	A vulnerability classified as critical has been found in code-projects Restaurant Reservation System 1.0. Affected is an unknown function of the file /filter.php. The manipulation of the argument from/to 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 initial researcher advisory only mentions the parameter "from" to be affected. But it must be assumed that parameter "to" is affected as well.	2024-09-22	6.3	CVE-2024-9086 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
CodeCanyon--RISE Ultimate Project Manager	A vulnerability has been found in CodeCanyon RISE Ultimate Project Manager 3.7.0 and classified as critical. This vulnerability affects unknown code of the file /index.php/dashboard/save. 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. It is recommended to upgrade the affected component.	2024-09-17	5.5	CVE-2024-8945 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Codezips--Online Shopping Portal	A vulnerability classified as problematic was found in Codezips Online Shopping Portal 1.0. Affected by this vulnerability is an unknown functionality of the file insert-product.php. The manipulation of the argument productimage1/productimage2/productimage3 leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-09-20	4.3	CVE-2024-9038 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
contao--contao	Contao is an Open Source CMS. In affected versions an untrusted user can inject insert tags into the canonical tag, which are then replaced on the web page (front end). Users are advised to update to Contao 4.13.49, 5.3.15 or 5.4.3. Users unable to upgrade should disable canonical tags in the root page settings.	2024-09-17	5.3	CVE-2024-45612 security-advisories@github.com security-advisories@github.com
contao--contao	Contao is an Open Source CMS. In affected versions authenticated users in the back end can list files outside the document root in the file selector widget. Users are advised to update to Contao 4.13.49. There are no known workarounds for this vulnerability.	2024-09-17	4.3	CVE-2024-45604 security-advisories@github.com security-advisories@github.com
CryoutCreations--Kahuna	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Kahuna allows Stored XSS.This issue affects Kahuna: from n/a through 1.7.0.	2024-09-18	6.5	CVE-2024-43994 audit@patchstack.com
CryoutCreations--Liquido	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Liquido allows Stored XSS.This issue affects Liquido: from n/a through 1.0.1.2.	2024-09-18	6.5	CVE-2024-43993 audit@patchstack.com
CryoutCreations--Roseta	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Roseta allows Stored XSS.This issue affects Roseta: from n/a through 1.3.0.	2024-09-17	6.5	CVE-2024-45451 audit@patchstack.com
CryoutCreations--Septera	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Septera septera allows Stored XSS.This issue affects Septera: from n/a through 1.5.1.	2024-09-17	6.5	CVE-2024-45452 audit@patchstack.com
CryoutCreations--Verbosa	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Verbosa allows Stored XSS.This issue affects Verbosa: from n/a through 1.2.3.	2024-09-17	6.5	CVE-2024-44050 audit@patchstack.com
D-Link--DAR-7000	A vulnerability classified as critical has been found in D-Link DAR-7000 up to 20240912. Affected is an unknown function of the file /view/DBManage/Backup_Server_commit.php. The manipulation of the argument host 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. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2024-09-19	6.3	CVE-2024-9004 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
decidim--decidim	decidim is a Free Open-Source participatory democracy, citizen participation and open government for cities and organizations. The admin panel is subject to potential Cross-site scripting (XSS) attach in case an admin assigns a valuator to a	2024-09-16	6.8	CVE-2024-32034 security-advisories@github.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	proposal, or does any other action that generates an admin activity log where one of the resources has an XSS crafted. This issue has been addressed in release version 0.27.7, 0.28.2, and newer. Users are advised to upgrade. Users unable to upgrade may redirect the pages /admin and /admin/logs to other admin pages to prevent this access (i.e. `/admin/organization/edit`).			com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
decidim--decidim	decidim is a Free Open-Source participatory democracy, citizen participation and open government for cities and organizations. The WYSWYG editor QuillJS is subject to potential XSS attach in case the attacker manages to modify the HTML before being uploaded to the server. The attacker is able to change e.g. to <svg onload=alert('XSS')> if they know how to craft these requests themselves. This issue has been addressed in release version 0.27.7. All users are advised to upgrade. Users unable to upgrade should review the user accounts that have access to the admin panel (i.e. general Administrators, and participatory space's Administrators) and remove access to them if they don't need it. Disable the "Enable rich text editor for participants" setting in the admin dashboard	2024-09-16	5.4	CVE-2024-39910 security-advisories@github.com security-advisories@github.com
delvedor--find-my-way	find-my-way is a fast, open source HTTP router, internally using a Radix Tree (aka compact Prefix Tree), supports route params, wildcards, and it's framework independent. A bad regular expression is generated any time one has two parameters within a single segment, when adding a `-` at the end, like `/:a-:b-`. This may cause a denial of service in some instances. Users are advised to update to find-my-way v8.2.2 or v9.0.1. or subsequent versions. There are no known workarounds for this issue.	2024-09-18	5.3	CVE-2024-45813 security-advisories@github.com security-advisories@github.com
devfelixmoira--Limit Login Attempts Plus WordPress Limit Login Attempts By Felix	The Limit Login Attempts Plus plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 1.1.0. This is due to insufficient restrictions on where the IP Address information is being retrieved for request logging and login restrictions. Attackers can supply the X-Forwarded-For header with with a different IP Address that will be logged and can be used to bypass settings that may have blocked out an IP address or country from logging in.	2024-09-19	5.3	CVE-2022-4533 security@wordfence.com security@wordfence.com
devise-two-factor--devise-two-factor	Under the default configuration, Devise-Two-Factor versions >= 2.2.0 & < 6.0.0 generate TOTP shared secrets that are 120 bits instead of the 128-bit minimum defined by RFC 4226. Using a shared secret shorter than the minimum to generate a multi-factor authentication code could make it easier for an attacker to guess the shared secret and generate valid TOTP codes.	2024-09-17	5.3	CVE-2024-8796 disclosure@synopsys.com
digitalnature--Mystique	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in digitalnature Mystique allows Stored XSS.This issue affects Mystique: from n/a through 2.5.7.	2024-09-18	6.5	CVE-2024-43988 audit@patchstack.com
directus--directus	Directus is a real-time API and App dashboard for managing SQL database content. When relying on blocking access to localhost using the default `0.0.0.0` filter a user may bypass this block by using other registered loopback devices (like `127.0.0.2` - `127.127.127.127`). This issue has been addressed in release versions 10.13.3 and	2024-09-18	5	CVE-2024-46990 security-advisories@github.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	11.1.0. Users are advised to upgrade. Users unable to upgrade may block this bypass by manually adding the `127.0.0.0/8` CIDR range which will block access to any `127.X.X.X` ip instead of just `127.0.0.1`.			security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
dondon-benjamincouk--WP Custom Fields Search	The WP Custom Fields Search plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpcfs-preset shortcode in all versions up to, and including, 1.2.35 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.	2024-09-19	6.4	CVE-2024-8364 security@wordfence.com security@wordfence.com security@wordfence.com
dvankooten--MC4WP: Mailchimp for WordPress	The MC4WP: Mailchimp for WordPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'email' parameter when a placeholder such as {email} is used for the field in versions 4.9.9 to 4.9.15 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.	2024-09-19	6.1	CVE-2024-8850 security@wordfence.com security@wordfence.com security@wordfence.com
dvankooten--MC4WP: Mailchimp for WordPress	The MC4WP: Mailchimp for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 4.9.16 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.	2024-09-21	4.4	CVE-2024-8680 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
Dylan Kuhn--Geo Mashup	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Dylan Kuhn Geo Mashup allows Stored XSS.This issue affects Geo Mashup: from n/a through 1.13.12.	2024-09-17	6.5	CVE-2024-44008 audit@patchstack.com
envoyproxy--envoy	Envoy is a cloud-native high-performance edge/middle/service proxy. A security vulnerability in Envoy allows external clients to manipulate Envoy headers, potentially leading to unauthorized access or other malicious actions within the mesh. This issue arises due to Envoy's default configuration of internal trust boundaries, which considers all RFC1918 private address ranges as internal. The default behavior for handling internal addresses in Envoy has been changed. Previously, RFC1918 IP addresses were automatically considered internal, even if the internal_address_config was empty. The default configuration of Envoy will continue to trust internal addresses while in this release and it will not trust them by default in next release. If you have tooling such as probes on your private network which need to be treated as trusted (e.g. changing arbitrary x-envoy	2024-09-20	6.5	CVE-2024-45806 security-advisories@github.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	headers) please explicitly include those addresses or CIDR ranges into `internal_address_config`. Successful exploitation could allow attackers to bypass security controls, access sensitive data, or disrupt services within the mesh, like Istio. This issue has been addressed in versions 1.31.2, 1.30.6, 1.29.9, and 1.28.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.			
envoyproxy--envoy	Envoy is a cloud-native high-performance edge/middle/service proxy. A vulnerability has been identified in Envoy that allows malicious attackers to inject unexpected content into access logs. This is achieved by exploiting the lack of validation for the `REQUESTED_SERVER_NAME` field for access loggers. This issue has been addressed in versions 1.31.2, 1.30.6, 1.29.9, and 1.28.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-20	6.5	CVE-2024-45808 security-advisories@github.com
envoyproxy--envoy	Envoy is a cloud-native high-performance edge/middle/service proxy. Envoy will crash when the http async client is handling `sendLocalReply` under some circumstance, e.g., websocket upgrade, and requests mirroring. The http async client will crash during the `sendLocalReply()` in http async client, one reason is http async client is duplicating the status code, another one is the destroy of router is called at the destructor of the async stream, while the stream is deferred deleted at first. There will be problems that the stream decoder is destroyed but its reference is called in `router.onDestroy()`, causing segment fault. This will impact ext_authz if the `upgrade` and `connection` header are allowed, and request mirrorring. This issue has been addressed in versions 1.31.2, 1.30.6, 1.29.9, and 1.28.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-20	6.5	CVE-2024-45810 security-advisories@github.com
envoyproxy--envoy	Envoy is a cloud-native high-performance edge/middle/service proxy. Jwt filter will lead to an Envoy crash when clear route cache with remote JWKs. In the following case: 1. remote JWKs are used, which requires async header processing; 2. clear_route_cache is enabled on the provider; 3. header operations are enabled in JWT filter, e.g. header to claims feature; 4. the routing table is configured in a way that the JWT header operations modify requests to not match any route. When these conditions are met, a crash is triggered in the upstream code due to nullptr reference conversion from route(). The root cause is the ordering of continueDecoding and clearRouteCache. This issue has been addressed in versions 1.31.2, 1.30.6, and 1.29.9. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-20	5.3	CVE-2024-45809 security-advisories@github.com
galaxyproject--galaxy	Galaxy is a free, open-source system for analyzing data, authoring workflows, training and education, publishing tools, managing infrastructure, and more. An attacker can potentially replace the contents of public datasets resulting in data loss or tampering. All supported branches of Galaxy (and more back to release_21.05) were amended with the below patch. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-20	6.5	CVE-2024-42351 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
getsentry--sentry	Sentry is a developer-first error tracking and performance monitoring platform. An authenticated user delete the user issue alert notifications for arbitrary users given a know alert ID. A patch was issued to ensure authorization checks are properly scoped on requests to delete user alert notifications. Sentry SaaS users do not need to take any action. Self-Hosted Sentry users should upgrade to version 24.9.0 or higher. There are no known workarounds for this vulnerability.	2024-09-17	6.5	CVE-2024-45605 security-advisories@github.com security-advisories@github.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				security-advisories@github.com
GitLab--GitLab	An issue has been discovered in GitLab EE affecting all versions starting from 11.1 before 17.1.7, 17.2 before 17.2.5, and 17.3 before 17.3.2. Under certain conditions an open redirect vulnerability could allow for an account takeover by breaking the OAuth flow.	2024-09-16	6.4	CVE-2024-4283 cve@gitlab.com cve@gitlab.com
ibm -- aspera_shares	IBM Aspera Shares 1.0 through 1.10.0 PL3 does not invalidate session after a password reset which could allow an authenticated user to impersonate another user on the system.	2024-09-16	6.5	CVE-2024-38315 psirt@us.ibm.com psirt@us.ibm.com
IBM--Business Automation Workflow	IBM Business Automation Workflow 22.0.2, 23.0.1, 23.0.2, and 24.0.0 could allow a privileged user to perform unauthorized activities due to improper client side validation.	2024-09-18	4.9	CVE-2024-43188 psirt@us.ibm.com
IBM--Cognos Analytics	IBM Cognos Analytics 11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 12.0.0, 12.0.1, 12.0.2, 12.0.3, and IBM Cognos Analytics Reports for iOS 11.0.0.7 could allow a local attacker to obtain sensitive information in the form of an API key. An attacker could use this information to launch further attacks against affected applications.	2024-09-22	5.5	CVE-2024-40703 psirt@us.ibm.com psirt@us.ibm.com
IDX Broker--IMPress for IDX Broker	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in IDX Broker IMPress for IDX Broker allows Stored XSS.This issue affects IMPress for IDX Broker: from n/a through 3.2.2.	2024-09-17	6.5	CVE-2024-44047 audit@patchstack.com
intumit -- smartrobot_firmware	SmartRobot from INTUMIT does not properly validate a specific page parameter, allowing unautheticated remote attackers to inject JavaScript code to the parameter for Reflected Cross-site Scripting attacks.	2024-09-16	6.1	CVE-2024-8776 twcert@cert.org.tw twcert@cert.org.tw
itsourcecode--Online Bookstore	A vulnerability was found in itsourcecode Online Bookstore 1.0. It has been rated as critical. This issue affects some unknown processing of the file admin_add.php. The manipulation of the argument image leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-09-20	6.3	CVE-2024-9036 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
jeanmarc77--123solar	A vulnerability was found in jeanmarc77 123solar 1.8.4.5. It has been rated as critical. Affected by this issue is some unknown functionality of the file config/config_invt1.php. The manipulation of the argument PASSOx leads to code injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The patch is identified as f4a8c748ec436e5a79f91ccb6a6f73752b336aa5. It is recommended to apply a patch to fix this issue.	2024-09-19	6.3	CVE-2024-9006 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Jeroen Peters--Name Directory	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jeroen Peters Name Directory allows Reflected XSS.This issue affects Name Directory: from n/a through 1.29.0.	2024-09-17	6.5	CVE-2024-43938 audit@patchstack.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA before 2024.1 hTML injection via the project name was possible	2024-09-16	6.1	CVE-2024-46970 cve@jetbrains.com
JetBrains--YouTrack	In JetBrains YouTrack before 2024.3.44799 user without appropriate permissions could restore workflows attached to a project	2024-09-19	4.3	CVE-2024-47159 cve@jetbrains.com
JetBrains--YouTrack	In JetBrains YouTrack before 2024.3.44799 access to global app config data without appropriate permissions was possible	2024-09-19	4.3	CVE-2024-47160 cve@jetbrains.com
JetBrains--YouTrack	In JetBrains YouTrack before 2024.3.44799 token could be revealed on Imports page	2024-09-19	4.1	CVE-2024-47162 cve@jetbrains.com
Jinan Chicheng Company--JFlow	A vulnerability was found in Jinan Chicheng Company JFlow 2.0.0. It has been rated as problematic. This issue affects the function AttachmentUploadController of the file /WF/Ath/EntityMutliFile_Load.do of the component Attachment Handler. The manipulation of the argument oid leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-09-19	4.3	CVE-2024-9003 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Johan van der Wijk--Content Blocks (Custom Post Widget)	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Johan van der Wijk Content Blocks (Custom Post Widget) allows Stored XSS.This issue affects Content Blocks (Custom Post Widget): from n/a through 3.3.5.	2024-09-17	6.5	CVE-2024-44051 audit@patchstack.com
Latepoint--LatePoint	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Latepoint LatePoint allows Stored XSS.This issue affects LatePoint: from n/a through 4.9.91.	2024-09-18	6.5	CVE-2024-43992 audit@patchstack.com
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: usb: typec: ucsi: Fix null pointer dereference in trace ucsi_register_altmode checks IS_ERR for the alt pointer and treats NULL as valid. When CONFIG_TYPEC_DP_ALTMODE is not enabled, ucsi_register_displayport returns NULL which causes a NULL pointer dereference in trace. Rather than return NULL, call typec_port_register_altmode to register DisplayPort alternate mode as a non-controllable mode when CONFIG_TYPEC_DP_ALTMODE is not enabled.	2024-09-18	5.5	CVE-2024-46719 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix dereference after null check check the pointer hive before use.	2024-09-18	5.5	CVE-2024-46720 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix possible NULL pointer dereference profile->parent->dents[AAFS_PROF_DIR] could be NULL only if its parent is made from __create_missing_ancestors(..) and 'ent->old' is NULL in aa_replace_profiles(..). In that case, it must return an error code and the code, -ENOENT represents its state that the path of its parent is not existed yet. BUG: kernel NULL pointer dereference, address: 0000000000000030 PGD 0 P4D 0 PREEMPT SMP PTI CPU: 4 PID: 3362 Comm: apparmor_parser Not tainted 6.8.0-24-generic #24 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.15.0-1 04/01/2014 RIP: 0010:aafs_create.constprop.0+0x7f/0x130 Code: 4c 63 e0 48 83 c4 18 4c 89 e0 5b 41 5c 41 5d 41 5e 41 5f 5d 31 d2 31 c9 31 f6 31 ff 45 31 c0 45 31 c9 45 31 d2 c3 cc cc cc cc <4d> 8b 55 30 4d 8d ba a0 00 00 00 4c 89 55 c0 4c 89 ff e8 7a 6a ae RSP: 0018:ffffc9000b2c7c98 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 00000000000041ed RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffc9000b2c7cd8 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffffff82baac10 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 00007be9f22cf740(0000) GS:ffff88817bc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000030 CR3: 0000000134b08000 CR4: 00000000000006f0 Call Trace: <TASK> ? show_regs+0x6d/0x80 ? __die+0x24/0x80 ? page_fault_oops+0x99/0x1b0 ? kernelmode_fixup_or_oops+0xb2/0x140 ? __bad_area_nosemaphore+0x1a5/0x2c0 ? find_vma+0x34/0x60 ? bad_area_nosemaphore+0x16/0x30 ? do_user_addr_fault+0x2a2/0x6b0 ? exc_page_fault+0x83/0x1b0 ? asm_exc_page_fault+0x27/0x30 ? aafs_create.constprop.0+0x7f/0x130 ? aafs_create.constprop.0+0x51/0x130 __aafs_profile_mkdir+0x3d6/0x480 aa_replace_profiles+0x83f/0x1270 policy_update+0xe3/0x180 profile_load+0xbc/0x150 ? rw_verify_area+0x47/0x140 vfs_write+0x100/0x480 ? __x64_sys_openat+0x55/0xa0 ? syscall_exit_to_user_mode+0x86/0x260 ksys_write+0x73/0x100 __x64_sys_write+0x19/0x30 x64_sys_call+0x7e/0x25c0 do_syscall_64+0x7f/0x180 entry_SYSCALL_64_after_hwframe+0x78/0x80 RIP: 0033:0x7be9f211c574 Code: c7 00 16 00 00 00 b8 ff ff ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 f3 0f 1e fa 80 3d d5 ea 0e 00 00 74 13 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 54 c3 0f 1f 00 55 48 89 e5 48 83 ec 20 48 89 RSP: 002b:00007ffd26f2b8c8 EFLAGS: 00000202 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 00005d504415e200 RCX: 00007be9f211c574 RDX: 0000000000001fc1 RSI: 00005d504418bc80 RDI: 0000000000000004 RBP: 0000000000001fc1 R08: 0000000000001fc1 R09: 0000000080000000 R10: 0000000000000000 R11: 0000000000000202 R12: 00005d504418bc80 R13: 0000000000000004 R14: 00007ffd26f2b9b0 R15: 00007ffd26f2ba30 </TASK> Modules linked in: snd_seq_dummy snd_hrtimer qrtr snd_hda_codec_generic snd_hda_intel snd_intel_dspcfg snd_intel_sdw_acpi snd_hda_codec snd_hda_core snd_hwdep snd_pcm snd_seq_midi snd_seq_midi_event snd_rawmidi snd_seq snd_seq_device i2c_i801 snd_timer i2c_smbus qxl snd soundcore drm_ttm_helper lpc_ich ttm joydev input_leds	2024-09-18	5.5	CVE-2024-46721 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	serio_raw mac_hid binfmt_misc msr parport_pc ppdev lp parport efi_pstore nfnetlink dmi_sysfs qemu_fw_cfg ip_tables x_tables autofs4 hid_generic usbhid hid ahci libahci psmouse virtio_rng xhci_pci xhci_pci_renesas CR2: 0000000000000030 ---[end trace 0000000000000000]--- RIP: 0010:aafs_create.constprop.0+0x7f/0x130 Code: 4c 63 e0 48 83 c4 18 4c 89 e0 5b 41 5c 41 5d 41 5e 41 5f 5d 31 d2 31 c9 31 f6 31 ff 45 31 c0 45 31 c9 45 31 d2 c3 cc cc cc cc <4d> 8b 55 30 4d 8d ba a0 00 00 00 4c 89 55 c0 4c 89 ff e8 7a 6a ae RSP: 0018:ffffc9000b2c7c98 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 00000000000041ed RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffc9000b2c7cd8 R08: 0000000000000000 R09: 0000000000000000 R10: 0000 ---truncated---			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Ensure index calculation will not overflow [WHY & HOW] Make sure vmid0p72_idx, vnom0p8_idx and vmax0p9_idx calculation will never overflow and exceess array size. This fixes 3 OVERRUN and 1 INTEGER_OVERFLOW issues reported by Coverity.	2024-09-18	5.5	CVE-2024-46726 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ublk_drv: fix NULL pointer dereference in ublk_ctrl_start_recovery() When two UBLK_CMD_START_USER_RECOVERY commands are submitted, the first one sets 'ubq->ubq_daemon' to NULL, and the second one triggers WARN in ublk_queue_reinit() and subsequently a NULL pointer dereference issue. Fix it by adding the check in ublk_ctrl_start_recovery() and return immediately in case of zero 'ub->nr_queues_ready'. BUG: kernel NULL pointer dereference, address: 0000000000000028 RIP: 0010:ublk_ctrl_start_recovery.constprop.0+0x82/0x180 Call Trace: <TASK> ? __die+0x20/0x70 ? page_fault_oops+0x75/0x170 ? exc_page_fault+0x64/0x140 ? asm_exc_page_fault+0x22/0x30 ? ublk_ctrl_start_recovery.constprop.0+0x82/0x180 ublk_ctrl_uring_cmd+0x4f7/0x6c0 ? pick_next_task_idle+0x26/0x40 io_uring_cmd+0x9a/0x1b0 io_issue_sqe+0x193/0x3f0 io_wq_submit_work+0x9b/0x390 io_worker_handle_work+0x165/0x360 io_wq_worker+0xcb/0x2f0 ? finish_task_switch.isra.0+0x203/0x290 ? finish_task_switch.isra.0+0x203/0x290 ? __pfx_io_wq_worker+0x10/0x10 ret_from_fork+0x2d/0x50 ? __pfx_io_wq_worker+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK>	2024-09-18	5.5	CVE-2024-46735 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: fix kernel crash if commands allocation fails If the commands allocation fails in nvmet_tcp_alloc_cmds() the kernel crashes in nvmet_tcp_release_queue_work() because of a NULL pointer dereference. nvmet: failed to install queue 0 cntlid 1 ret 6 Unable to handle kernel NULL pointer dereference at virtual address 0000000000000008 Fix the bug by setting queue->nr_cmds to zero in case nvmet_tcp_alloc_cmd() fails.	2024-09-18	5.5	CVE-2024-46737 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: uio_hv_generic: Fix kernel NULL pointer dereference in hv_uio_rescind For primary VM Bus channels, primary_channel pointer is always NULL. This pointer is valid only for the secondary channels. Also, rescind callback is meant for primary channels only. Fix NULL pointer dereference by retrieving the device_obj from the parent for the primary channel.	2024-09-18	5.5	CVE-2024-46739 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: smb/server: fix potential null-ptr-deref of lease_ctx_info in smb2_open() null-ptr-deref will occur when (req_op_level == SMB2_OPLOCK_LEVEL_LEASE) and parse_lease_state() return NULL. Fix this by check if 'lease_ctx_info' is NULL. Additionally, remove the redundant parentheses in parse_durable_handle_context().	2024-09-18	5.5	CVE-2024-46742 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btnxpuart: Fix Null pointer dereference in btnxpuart_flush() This adds a check before freeing the rx->skb in flush and close functions to handle the kernel crash seen while removing driver after FW download fails or before FW download completes. dmesg log: [54.634586] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000080 [54.643398] Mem abort info: [54.646204] ESR = 0x0000000096000004 [54.649964] EC = 0x25: DABT (current EL), IL = 32 bits [54.655286] SET = 0, FnV = 0 [54.658348] EA = 0, S1PTW = 0 [54.661498] FSC = 0x04: level 0 translation fault [54.666391] Data abort info: [54.669273] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [54.674768] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [54.674771] GCS = 0, Overlay = 0, DirtyBit = 0, Xs =	2024-09-18	5.5	CVE-2024-46749 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	0 [54.674775] user pgtable: 4k pages, 48-bit VAs, pgdp=0000000048860000 [54.674780] [0000000000000080] pgd=0000000000000000, p4d=0000000000000000 [54.703880] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP [54.710152] Modules linked in: btnxpuart(-) overlay fsl_jr_uio caam_jr caamkeyblob_desc caamhash_desc caamalg_desc crypto_engine authenc libdes crct10dif_ce polyval_ce polyval_generic snd_soc_imx_spdif snd_soc_imx_card snd_soc_ak5558 snd_soc_ak4458 caam secvio error snd_soc_fsl_micfil snd_soc_fsl_spdif snd_soc_fsl_sai snd_soc_fsl_utils imx_pcm_dma gpio_ir_recv rc_core sch_fq_codel fuse [54.744357] CPU: 3 PID: 72 Comm: kworker/u9:0 Not tainted 6.6.3-otbr-g128004619037 #2 [54.744364] Hardware name: FSL i.MX8MM EVK board (DT) [54.744368] Workqueue: hci0 hci_power_on [54.757244] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [54.757249] pc : kfree_skb_reason+0x18/0xb0 [54.772299] lr : btnxpuart_flush+0x40/0x58 [btnxpuart] [54.782921] sp : ffff8000805ebca0 [54.782923] x29: ffff8000805ebca0 x28: ffffa5c6cf1869c0 x27: ffffa5c6cf186000 [54.782931] x26: ffff377b84852400 x25: ffff377b848523c0 x24: ffff377b845e7230 [54.782938] x23: ffffa5c6ce8dbe08 x22: ffffa5c6ceb65410 x21: 00000000ffffff92 [54.782945] x20: ffffa5c6ce8dbe98 x19: fffffffffffffffac x18: ffffffffffffffff [54.807651] x17: 0000000000000000 x16: ffffa5c6ce2824ec x15: ffff8001005eb857 [54.821917] x14: 0000000000000000 x13: ffffa5c6cf1a02e0 x12: 0000000000000642 [54.821924] x11: 0000000000000040 x10: ffffa5c6cf19d690 x9 : ffffa5c6cf19d688 [54.821931] x8 : ffff377b86000028 x7 : 0000000000000000 x6 : 0000000000000000 [54.821938] x5 : ffff377b86000000 x4 : 0000000000000000 x3 : 0000000000000000 [54.843331] x2 : 0000000000000000 x1 : 0000000000000002 x0 : fffffffffffffffac [54.857599] Call trace: [54.857601] kfree_skb_reason+0x18/0xb0 [54.863878] btnxpuart_flush+0x40/0x58 [btnxpuart] [54.863888] hci_dev_open_sync+0x3a8/0xa04 [54.872773] hci_power_on+0x54/0x2e4 [54.881832] process_one_work+0x138/0x260 [54.881842] worker_thread+0x32c/0x438 [54.881847] kthread+0x118/0x11c [54.881853] ret_from_fork+0x10/0x20 [54.896406] Code: a9be7bfd 910003fd f9000bf3 aa0003f3 (b940d400) [54.896410] ---[end trace 0000000000000000]---			8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: can: mcp251x: fix deadlock if an interrupt occurs during mcp251x_open The mcp251x_hw_wake() function is called with the mpc_lock mutex held and disables the interrupt handler so that no interrupts can be processed while waking the device. If an interrupt has already occurred then waiting for the interrupt handler to complete will deadlock because it will be trying to acquire the same mutex. CPU0 CPU1 ---- ---- mcp251x_open() mutex_lock(&priv->mcp_lock) request_threaded_irq() <interrupt> mcp251x_can_ist() mutex_lock(&priv->mcp_lock) mcp251x_hw_wake() disable_irq() <-- deadlock Use disable_irq_nosync() instead because the interrupt handler does everything while holding the mutex so it doesn't matter if it's still running.	2024-09-18	5.5	CVE-2024-46791 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ksmbd: unset the binding mark of a reused connection Steve French reported null pointer dereference error from sha256 lib. cifs.ko can send session setup requests on reused connection. If reused connection is used for binding session, conn->binding can still remain true and generate_preauth_hash() will not set sess->Preauth_HashValue and it will be NULL. It is used as a material to create an encryption key in ksmbd_gen_smb311_encryptionkey. ->Preauth_HashValue cause	2024-09-18	5.5	CVE-2024-46795 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	null pointer dereference error from crypto_shash_update(). BUG: kernel NULL pointer dereference, address: 0000000000000000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP PTI CPU: 8 PID: 429254 Comm: kworker/8:39 Hardware name: LENOVO 20MAS08500/20MAS08500, BIOS N2CET69W (1.52) Workqueue: ksmbd-io handle_ksmbd_work [ksmbd] RIP: 0010:lib_sha256_base_do_update.isra.0+0x11e/0x1d0 [sha256_ssse3] <TASK> ? show_regs+0x6d/0x80 ? __die+0x24/0x80 ? page_fault_oops+0x99/0x1b0 ? do_user_addr_fault+0x2ee/0x6b0 ? exc_page_fault+0x83/0x1b0 ? asm_exc_page_fault+0x27/0x30 ? __pfx_sha256_transform_rorx+0x10/0x10 [sha256_ssse3] ? lib_sha256_base_do_update.isra.0+0x11e/0x1d0 [sha256_ssse3] ? __pfx_sha256_transform_rorx+0x10/0x10 [sha256_ssse3] ? __pfx_sha256_transform_rorx+0x10/0x10 [sha256_ssse3] _sha256_update+0x77/0xa0 [sha256_ssse3] sha256_avx2_update+0x15/0x30 [sha256_ssse3] crypto_shash_update+0x1e/0x40 hmac_update+0x12/0x20 crypto_shash_update+0x1e/0x40 generate_key+0x234/0x380 [ksmbd] generate_smb3encryptionkey+0x40/0x1c0 [ksmbd] ksmbd_gen_smb311_encryptionkey+0x72/0xa0 [ksmbd] ntlm_authenticate.isra.0+0x423/0x5d0 [ksmbd] smb2_sess_setup+0x952/0xaa0 [ksmbd] __process_request+0xa3/0x1d0 [ksmbd] __handle_ksmbd_work+0x1c4/0x2f0 [ksmbd] handle_ksmbd_work+0x2d/0xa0 [ksmbd] process_one_work+0x16c/0x350 worker_thread+0x306/0x440 ? __pfx_worker_thread+0x10/0x10 kthread+0xef/0x120 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x44/0x70 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1b/0x30 </TASK>			416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: powerpc/qspinlock: Fix deadlock in MCS queue If an interrupt occurs in queued_spin_lock_slowpath() after we increment qnodesp->count and before node->lock is initialized, another CPU might see stale lock values in get_tail_qnode(). If the stale lock value happens to match the lock on that CPU, then we write to the "next" pointer of the wrong qnode. This causes a deadlock as the former CPU, once it becomes the head of the MCS queue, will spin indefinitely until it's "next" pointer is set by its successor in the queue. Running stress-ng on a 16 core (16EC/16VP) shared LPAR, results in occasional lockups similar to the following: $ stress-ng --all 128 --vm-bytes 80% --aggressive \ --maximize --oomable --verify --syslog \ --metrics --times --timeout 5m watchdog: CPU 15 Hard LOCKUP ..... NIP [c0000000000b78f4] queued_spin_lock_slowpath+0x1184/0x1490 LR [c000000001037c5c] _raw_spin_lock+0x6c/0x90 Call Trace: 0xc000002cfffa3bf0 (unreliable) _raw_spin_lock+0x6c/0x90 raw_spin_rq_lock_nested.part.135+0x4c/0xd0 sched_ttwu_pending+0x60/0x1f0 __flush_smp_call_function_queue+0x1dc/0x670 smp_ipi_demux_relaxed+0xa4/0x100 xive_muxed_ipi_action+0x20/0x40 __handle_irq_event_percpu+0x80/0x240 handle_irq_event_percpu+0x2c/0x80 handle_percpu_irq+0x84/0xd0 generic_handle_irq+0x54/0x80 __do_irq+0xac/0x210 __do_IRQ+0x74/0xd0 0x0 do_IRQ+0x8c/0x170 hardware_interrupt_common_virt+0x29c/0x2a0 --- interrupt: 500 at queued_spin_lock_slowpath+0x4b8/0x1490 ..... NIP [c0000000000b6c28] queued_spin_lock_slowpath+0x4b8/0x1490 LR [c000000001037c5c] _raw_spin_lock+0x6c/0x90 --- interrupt: 500 0xc0000029c1a41d00 (unreliable) _raw_spin_lock+0x6c/0x90 futex_wake+0x100/0x260 do_futex+0x21c/0x2a0 sys_futex+0x98/0x270 system_call_exception+0x14c/0x2f0 system_call_vectored_common+0x15c/0x2ec The following code flow illustrates how the deadlock occurs. For the sake of brevity, assume that both locks (A and B) are contended and we call the queued_spin_lock_slowpath() function. CPU0 CPU1 ---- ---- spin_lock_irqsave(A) | spin_unlock_irqrestore(A) | spin_lock(B) | | | ? | id = qnodesp->count++; | (Note that nodes[0].lock == A) | | | ? | Interrupt | (happens before "nodes[0].lock = B") | | | ? | spin_lock_irqsave(A) | | | ? | id = qnodesp->count++ | nodes[1].lock = A | | | ? | Tail of MCS queue | | spin_lock_irqsave(A) ? | Head of MCS queue ? | CPU0 is previous tail ? | Spin indefinitely ? (until	2024-09-18	5.5	CVE-2024-46797 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	"nodes[1].next != NULL") prev = get_tail_qnode(A, CPU0) | ? prev == &qnodes[CPU0].nodes[0] (as qnodes ---truncated---			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: libfs: fix get_stashed_dentry() get_stashed_dentry() tries to optimistically retrieve a stashed dentry from a provided location. It needs to ensure to hold rcu lock before it dereference the stashed location to prevent UAF issues. Use rcu_dereference() instead of READ_ONCE() it's effectively equivalent with some lockdep bells and whistles and it communicates clearly that this expects rcu protection.	2024-09-18	5.5	CVE-2024-46801 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
lyft--confidant	Confidant is a open source secret management service that provides user-friendly storage and access to secrets. The following endpoints are subject to a cross site scripting vulnerability: GET /v1/credentials, GET /v1/credentials/, GET /v1/archive/credentials/, GET /v1/archive/credentials, POST /v1/credentials, PUT /v1/credentials/, PUT /v1/credentials//<to_revision>, GET /v1/services, GET /v1/services/, GET /v1/archive/services/, GET /v1/archive/services, PUT /v1/services/, PUT /v1/services//<to_revision>. The attacker needs to be authenticated and have privileges to create new credentials, but could use this to show information and run scripts to other users into the same Confidant instance. This issue has been patched in version 6.6.2. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-20	4.8	CVE-2024-45793 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
MagePeople Team--Bus Ticket Booking with Seat Reservation	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MagePeople Team Bus Ticket Booking with Seat Reservation allows Stored XSS.This issue affects Bus Ticket Booking with Seat Reservation: from n/a through 5.3.5.	2024-09-17	5.9	CVE-2024-43985 audit@patchstack.com
mattermost -- mattermost_server	Mattermost Desktop App versions <=5.8.0 fail to sufficiently configure Electron Fuses which allows an attacker to gather Chromium cookies or abuse other misconfigurations via remote/local access.	2024-09-16	6.5	CVE-2024-45835 responsibledisclosure@mattermost.com
mattermost -- mattermost_server	Mattermost Desktop App versions <=5.8.0 fail to safeguard screen capture functionality which allows an attacker to silently capture high-quality screenshots via JavaScript APIs.	2024-09-16	5.3	CVE-2024-39772 responsibledisclosure@mattermost.com
Mattermost--Mattermost	Mattermost Mobile Apps versions <=2.18.0 fail to disable autocomplete during login while typing the password and visible password is selected, which allows the password to get saved in the dictionary when the user has Swiftkey as the default keyboard, the masking is off and the password contains a special character..	2024-09-16	4.5	CVE-2024-45833 responsibledisclosure@mattermost.com
Mautic--Mautic	Prior to the patched version, logged in users of Mautic are vulnerable to an SQL injection vulnerability in the Reports bundle. The user could retrieve and alter data like sensitive data, login, and depending on database permission the attacker can manipulate file systems.	2024-09-18	6.6	CVE-2022-25775 security@mautic.org
Mautic--Mautic	Prior to the patched version, an authenticated user of Mautic could read system files and access the internal addresses of the application due to a Server-Side Request Forgery (SSRF) vulnerability.	2024-09-18	6.5	CVE-2022-25777 security@mautic.org

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Mautic--Mautic	Prior to this patch being applied, Mautic's tracking was vulnerable to Cross-Site Scripting through the Page URL variable.	2024-09-18	5.4	CVE-2024-47050 security@mautic.org
Mautic--Mautic	Prior to the patched version, logged in users of Mautic are vulnerable to a self XSS vulnerability in the notifications within Mautic. Users could inject malicious code into the notification when saving Dashboards.	2024-09-18	4.8	CVE-2022-25774 security@mautic.org
Mautic--Mautic	When logging in with the correct username and incorrect weak password, the user receives the notification, that their password is too weak. However when an incorrect username is provided alongside with a weak password, the application responds with 'Invalid credentials' notification. This difference could be used to perform username enumeration.	2024-09-18	4.3	CVE-2024-47059 security@mautic.org
Microsoft--Microsoft Edge (Chromium-based)	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-09-19	6.5	CVE-2024-43489 secure@microsoft.com
Microsoft--Microsoft Edge (Chromium-based)	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-09-19	6.5	CVE-2024-43496 secure@microsoft.com
Microsoft--Microsoft Edge (Chromium-based)	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-09-19	4.3	CVE-2024-38221 secure@microsoft.com
Microsoft--Windows 11 version 22H2	Windows Kernel Information Disclosure Vulnerability	2024-09-17	5.9	CVE-2024-37985 secure@microsoft.com
Millbeck Communications--Proroute H685t-w	This vulnerability occurs when user-supplied input is improperly sanitized and then reflected back to the user's browser, allowing an attacker to execute arbitrary JavaScript in the context of the victim's browser session.	2024-09-17	5.5	CVE-2024-38380 ics-cert@hq.dhs.gov
Moxa--MXview One Series	The vulnerability allows an attacker to craft MQTT messages that include relative path traversal sequences, enabling them to read arbitrary files on the system. This could lead to the disclosure of sensitive information, such as configuration files and JWT signing secrets.	2024-09-21	6.5	CVE-2024-6786 psirt@moxa.com
Moxa--MXview One Series	The configuration file stores credentials in cleartext. An attacker with local access rights can read or modify the configuration file, potentially resulting in the service being abused due to sensitive information exposure.	2024-09-21	5.5	CVE-2024-6785 psirt@moxa.com
Moxa--MXview One Series	This vulnerability occurs when an attacker exploits a race condition between the time a file is checked and the time it is used (TOCTOU). By exploiting this race condition, an attacker can write arbitrary files to the system. This could allow the attacker to execute malicious code and potentially cause file losses.	2024-09-21	5.3	CVE-2024-6787 psirt@moxa.com
n/a--DedeCMS	A vulnerability was found in DedeCMS up to 5.7.115. It has been rated as critical. This issue affects some unknown processing of the file article_string_mix.php. The manipulation leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-09-22	6.3	CVE-2024-9076 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--Intel(R) Processors with Intel(R) SGX	Improper conditions check in some Intel(R) Processors with Intel(R) SGX may allow a privileged user to potentially enable information disclosure via local access.	2024-09-16	5.3	CVE-2023-43753 secure@intel.com
n/a--Intel(R) Processors	Observable discrepancy in RAPL interface for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	2024-09-16	5.3	CVE-2024-23984 secure@intel.com
n/a--Intel(R) Processors	Improper finite state machines (FSMs) in hardware logic in some Intel(R) Processors may allow an privileged user to potentially enable a denial of service via local access.	2024-09-16	5.3	CVE-2024-24968 secure@intel.com
n/a--Intel(R) RAID Web Console software	Improper access control in Intel(R) RAID Web Console software for all versions may allow an authenticated user to potentially enable denial of service via adjacent access.	2024-09-16	6.5	CVE-2024-32940 secure@intel.com
n/a--Intel(R) RAID Web Console software	Uncaught exception in Intel(R) RAID Web Console software all versions may allow an authenticated user to potentially enable denial of service via local access.	2024-09-16	6.5	CVE-2024-33848 secure@intel.com
n/a--Intel(R) RAID Web Console software	Uncontrolled search path element in Intel(R) RAID Web Console software for all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-09-16	6.7	CVE-2024-34153 secure@intel.com
n/a--Intel(R) RAID Web Console software	Improper access control in Intel(R) RAID Web Console software for all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-09-16	6.7	CVE-2024-34543 secure@intel.com
n/a--Intel(R) RAID Web Console software	Improper input validation in some Intel(R) RAID Web Console software all versions may allow an authenticated user to potentially enable information disclosure via adjacent access.	2024-09-16	5.2	CVE-2024-34545 secure@intel.com
n/a--Intel(R) RAID Web Console software	NULL pointer dereference in Intel(R) RAID Web Console software for all versions may allow an authenticated user to potentially enable denial of service via local access.	2024-09-16	4.7	CVE-2024-32666 secure@intel.com
n/a--Intel(R) RAID Web Console	Improper access control in Intel(R) RAID Web Console all versions may allow an authenticated user to potentially enable denial of service via adjacent access.	2024-09-16	4.6	CVE-2024-36247 secure@intel.com
n/a--MicroPython	A vulnerability was found in MicroPython 1.22.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file py/objarray.c. The manipulation leads to use after free. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. Upgrading to version 1.23.0 is able to address this issue. The identifier of the patch is 4bed614e707c0644c06e117f848fa12605c711cd. It is recommended to upgrade the affected component. In micropython objarray component, when a bytes object is resized and copied into itself, it may reference memory that has already been freed.	2024-09-17	5.6	CVE-2024-8947 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
n/a--n/a	Cross Site Scripting vulnerability in Leotheme Leo Product Search Module v.2.1.6 and earlier allows a remote attacker to execute arbitrary code via the q parameter of the product search function.	2024-09-20	6.1	CVE-2024-42697 cve@mitre.org

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	A SQL injection vulnerability in linlinjava litemall 1.8.0 allows a remote attacker to obtain sensitive information via the goodsId, goodsSn, and name parameters in AdminGoodscontroller.java.	2024-09-19	6.5	CVE-2024-46382 cve@mitre.org
n/a--n/a	runofast Indoor Security Camera for Baby Monitor has a default password of password for the root account. This allows access to the /stream1 URI via the rtsp:// protocol to receive the video and audio stream.	2024-09-18	6.5	CVE-2024-46959 cve@mitre.org
n/a--n/a	An Incorrect Access Control vulnerability was found in /music/ajax.php?action=delete_genre in Kashipara Music Management System v1.0. This vulnerability allows an unauthenticated attacker to delete the valid music genre entries.	2024-09-16	5.9	CVE-2024-42796 cve@mitre.org cve@mitre.org
n/a--n/a	Kashipara Music Management System v1.0 is vulnerable to Incorrect Access Control via /music/ajax.php?action=save_user.	2024-09-16	4.7	CVE-2024-42794 cve@mitre.org cve@mitre.org
n/a--n/a	An Incorrect Access Control vulnerability was found in /music/view_user.php?id=3 and /music/controller.php?page=edit_user&id=3 in Kashipara Music Management System v1.0. This vulnerability allows an unauthenticated attacker to view valid user details.	2024-09-16	4.2	CVE-2024-42795 cve@mitre.org cve@mitre.org
n/a--n/a	A stored cross-site scripting (XSS) vulnerability in the Add Scheduled Task module of Maccms10 v2024.1000.4040 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	2024-09-20	4.8	CVE-2024-46654 cve@mitre.org
n/a--UEFI firmware for some Intel(R) Processors	Out-of-bounds write in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	2024-09-16	6.1	CVE-2023-22351 secure@intel.com
n/a--UEFI firmware for some Intel(R) Processors	NULL pointer dereference in the UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	2024-09-16	6.1	CVE-2023-23904 secure@intel.com
Pagelayer Team--PageLayer	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pagelayer Team PageLayer allows Stored XSS.This issue affects PageLayer: from n/a through 1.8.7.	2024-09-18	5.9	CVE-2024-43972 audit@patchstack.com
Podlove--Podlove Podcast Publisher	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Podlove Podlove Podcast Publisher allows Stored XSS.This issue affects Podlove Podcast Publisher: from n/a through 4.1.13.	2024-09-18	6.5	CVE-2024-43983 audit@patchstack.com
POSIMYTH--The Plus Addons for Elementor Page Builder Lite	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in POSIMYTH The Plus Addons for Elementor Page Builder Lite allows Stored XSS.This issue affects The Plus Addons for Elementor Page Builder Lite: from n/a through 5.6.2.	2024-09-17	6.5	CVE-2024-43977 audit@patchstack.com
puma--puma	Puma is a Ruby/Rack web server built for parallelism. In affected versions clients could clobber values set by intermediate proxies (such as X-Forwarded-For) by providing a underscore version of the same header (X-Forwarded_For). Any users relying on proxy set variables is affected. v6.4.3/v5.6.9 now discards any headers using underscores if the non-underscore version also exists. Effectively, allowing the proxy defined headers to always win. Users are advised to upgrade. Nginx has a underscores_in_headers configuration variable to discard these headers at the proxy level as a mitigation. Any users that are implicitly trusting the proxy defined	2024-09-19	5.4	CVE-2024-45614 security-advisories@github.com security-advisories@github.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	headers for security should immediately cease doing so until upgraded to the fixed versions.			
Red Hat--Red Hat Build of Keycloak	A misconfiguration flaw was found in Keycloak. This issue can allow an attacker to redirect users to an arbitrary URL if a 'Valid Redirect URI' is set to http://localhost or http://127.0.0.1, enabling sensitive information such as authorization codes to be exposed to the attacker, potentially leading to session hijacking.	2024-09-19	6.8	CVE-2024-8883 secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in QEMU. An assertion failure was present in the usb_ep_get() function in hw/net/core.c when trying to get the USB endpoint from a USB device. This flaw may allow a malicious unprivileged guest user to crash the QEMU process on the host and cause a denial of service condition.	2024-09-19	4.7	CVE-2024-8354 secalert@redhat.com secalert@redhat.com
Red Hat--Red Hat Enterprise Linux 8	A vulnerability was found in Performance Co-Pilot (PCP). This flaw allows an attacker to send specially crafted data to the system, which could cause the program to misbehave or crash.	2024-09-19	5.5	CVE-2024-45769 secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Enterprise Linux 8	A vulnerability was found in Performance Co-Pilot (PCP). This flaw can only be exploited if an attacker has access to a compromised PCP system account. The issue is related to the pmpost tool, which is used to log messages in the system. Under certain conditions, it runs with high-level privileges.	2024-09-19	4.4	CVE-2024-45770 secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com
Red Hat--Red Hat Enterprise Linux AI (RHEL AI)	A vulnerability was found in the ilab model serve component, where improper handling of the best_of parameter in the vllm JSON web API can lead to a Denial of Service (DoS). The API used for LLM-based sentence or chat completion accepts a best_of parameter to return the best completion from several options. When this parameter is set to a large value, the API does not handle timeouts or resource exhaustion properly, allowing an attacker to cause a DoS by consuming excessive system resources. This leads to the API becoming unresponsive, preventing legitimate users from accessing the service.	2024-09-17	6.2	CVE-2024-8939 secalert@redhat.com secalert@redhat.com
requarks--wiki	Wiki.js is an open source wiki app built on Node.js. A disabled user can still gain access to a wiki by abusing the password reset function. While setting up SMTP e-mail's on my server, I tested said e-mails by performing a password reset with my test user. To my shock, not only did it let me reset my password, but after resetting my password I can get into the wiki I was locked out of. The ramifications of this bug is a user can **bypass an account disabling by requesting their password be reset**. All users of wiki.js version `2.5.303` who use any account restrictions and have disabled user are affected. This issue has been addressed in version 2.5.304 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-18	4.3	CVE-2024-45298 security-advisories@github.com security-advisories@github.com
rfideas --micard_plus_ci_firmware	The MiCard PLUS Ci and MiCard PLUS BLE reader products developed by rf IDEAS and rebranded by NT-ware have a firmware fault that may result in characters randomly being dropped from some ID card reads, which would result in the wrong ID card number being assigned during ID card self-registration and might result in failed login attempts for end-users. Random characters being dropped from ID card numbers compromises the uniqueness of ID cards that can, therefore, result in a security issue if the users are using the 'ID card self-registration' function.	2024-09-16	5.3	CVE-2024-1578 4586e0a2-224d-4f8a-9cb4-8882b208c0b3 4586e0a2-224d-4f8a-9cb4-8882b208c0b3
Saturday Drive--Ninja Forms	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Saturday Drive Ninja Forms allows Stored XSS.This issue affects Ninja Forms: from n/a through 3.8.11.	2024-09-18	5.9	CVE-2024-43999 audit@patchstack.com
sonalsinha21--Posterity	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in sonalsinha21 Posterity allows Stored XSS.This issue affects Posterity: from n/a through 3.6.	2024-09-18	6.5	CVE-2024-43995 audit@patchstack.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				com
SourceCodester--Best House Rental Management System	A vulnerability has been found in SourceCodester Best House Rental Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /ajax.php?action=update_account. The manipulation of the argument firstname/lastname/email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-09-20	6.3	CVE-2024-9041 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Online Eyewear Shop	A vulnerability classified as critical has been found in SourceCodester Online Eyewear Shop 1.0. This affects an unknown part of the file /classes/Master.php of the component Cart Content Handler. The manipulation of the argument cart_id/id leads to improper ownership management. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-09-17	6.3	CVE-2024-8949 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Online Eyewear Shop	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file view_category.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.	2024-09-22	6.3	CVE-2024-9081 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Online Eyewear Shop	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /Users.phpf=save of the component User Creation Handler. The manipulation of the argument type with the input 1 leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-09-22	6.3	CVE-2024-9082 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Telecom Billing Management System	A vulnerability has been found in SourceCodester Telecom Billing Management System 1.0 and classified as critical. This vulnerability affects the function login. The manipulation of the argument uname leads to buffer overflow. The exploit has been disclosed to the public and may be used.	2024-09-22	6.3	CVE-2024-9088 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
syscomgo -- omflow	OMFLOW from The SYSCOM Group does not properly validate user input of the download functionality, allowing remote attackers with regular privileges to read arbitrary system files.	2024-09-16	6.5	CVE-2024-8778 twcert@cert.org.tw twcert@cert.org.tw
syscomgo -- omflow	OMFLOW from The SYSCOM Group does not properly restrict the query range of its data query functionality, allowing remote attackers with regular privileges to obtain accounts and password hashes of other users.	2024-09-16	6.5	CVE-2024-8780 twcert@cert.org.tw twcert@cert.org.tw
The SYSCOM Group--OMFLOW	OMFLOW from The SYSCOM Group has a vulnerability involving the exposure of sensitive data. This allows remote attackers who have logged into the system to obtain password hashes of all users and administrators.	2024-09-18	6.5	CVE-2024-8969 twcert@cert.org.tw twcert@cert.org.t

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				w
the-djmaze--snappymail	Snappymail is an open source web-based email client. SnappyMail uses the `cleanHtml()` function to cleanup HTML and CSS in emails. Research discovered that the function has a few bugs which cause an mXSS exploit. Because the function allowed too many (invalid) HTML elements, it was possible (with incorrect markup) to trick the browser to "fix" the broken markup into valid markup. As a result a motivated attacker may be able to inject javascript. However, due to the default Content Security Policy the impact of the exploit is minimal. It could be possible to create an attack which leaks some data when loading images through the proxy. This way it might be possible to use the proxy to attack the local system, like with `http://localhost:5000/leak`. Another attack could be to load a JavaScript attachment of the email. This is very tricky as the email must link to every possible UID as each email has a unique UID which has a value between 1 and 18446744073709551615 **v2.38.0** and up now remove unsupported HTML elements which mitigates the issue. Users are advised to upgrade. Older versions can install an extension named "Security mXSS" as a mitigation. This will be available at the administration area at `/?admin#/packages`. **NOTE:** this extension can not "fix" malicious code in encrypted messages or (html) attachments as it can't manipulate the JavaScript code for this. It only protects normal message HTML.	2024-09-16	5	CVE-2024-45800 security-advisories@github.com security-advisories@github.com security-advisories@github.com
ThemeHunk--Gutenberg Blocks Unlimited blocks For Gutenberg	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeHunk Gutenberg Blocks - Unlimited blocks For Gutenberg allows Stored XSS.This issue affects Gutenberg Blocks - Unlimited blocks For Gutenberg: from n/a through 1.2.7.	2024-09-17	6.5	CVE-2024-44049 audit@patchstack.com
TOTOLINK--T10	A vulnerability was found in TOTOLINK T10 4.1.8cu.5207. It has been declared as critical. This vulnerability affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-09-19	6.3	CVE-2024-9001 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Unknown--Accordion Image Menu	The Accordion Image Menu WordPress plugin through 3.1.3 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	2024-09-17	5.4	CVE-2024-8092 contact@wpscan.com
Unknown--Enhanced Search Box	The Enhanced Search Box WordPress plugin through 0.6.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	2024-09-17	4.8	CVE-2024-8091 contact@wpscan.com
Unknown--infolinks Ad Wrap	The infolinks Ad Wrap WordPress plugin through 1.0.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	2024-09-17	5.7	CVE-2024-8044 contact@wpscan.com
Unknown--Logo Manager For Enamad	The Logo Manager For Enamad WordPress plugin through 0.7.1 does not sanitise and escape in its widgets settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2024-09-17	5.7	CVE-2024-5170 contact@wpscan.com
Unknown--Posts reminder	The Posts reminder WordPress plugin through 0.20 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	2024-09-17	4.8	CVE-2024-8093 contact@wpscan.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Unknown--Review Ratings	The Review Ratings WordPress plugin through 1.6 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	2024-09-17	4.8	CVE-2024-8052 contact@wpscan.com
Unknown--Special Feed Items	The Special Feed Items WordPress plugin through 1.0.1 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	2024-09-17	5.7	CVE-2024-8051 contact@wpscan.com
Unknown--Vikinghammer Tweet	The Vikinghammer Tweet WordPress plugin through 0.2.4 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	2024-09-17	5.7	CVE-2024-8043 contact@wpscan.com
Unknown--Visual Sound (old)	The Visual Sound (old) WordPress plugin through 1.06 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	2024-09-17	5.7	CVE-2024-8047 contact@wpscan.com
vitejs--vite	Vite a frontend build tooling framework for javascript. Affected versions of vite were discovered to contain a DOM Clobbering vulnerability when building scripts to `cjs`/`iife`/`umd` output format. The DOM Clobbering gadget in the module can lead to cross-site scripting (XSS) in web pages where scriptless attacker-controlled HTML elements (e.g., an img tag with an unsanitized name attribute) are present. DOM Clobbering is a type of code-reuse attack where the attacker first embeds a piece of non-script, seemingly benign HTML markups in the webpage (e.g. through a post or comment) and leverages the gadgets (pieces of js code) living in the existing javascript code to transform it into executable code. We have identified a DOM Clobbering vulnerability in Vite bundled scripts, particularly when the scripts dynamically import other scripts from the assets folder and the developer sets the build output format to `cjs`, `iife`, or `umd`. In such cases, Vite replaces relative paths starting with `__VITE_ASSET__` using the URL retrieved from `document.currentScript`. However, this implementation is vulnerable to a DOM Clobbering attack. The `document.currentScript` lookup can be shadowed by an attacker via the browser's named DOM tree element access mechanism. This manipulation allows an attacker to replace the intended script element with a malicious HTML element. When this happens, the src attribute of the attacker-controlled element is used as the URL for importing scripts, potentially leading to the dynamic loading of scripts from an attacker-controlled server. This vulnerability can result in cross-site scripting (XSS) attacks on websites that include Vite-bundled files (configured with an output format of `cjs`, `iife`, or `umd`) and allow users to inject certain scriptless HTML tags without properly sanitizing the name or id attributes. This issue has been patched in versions 5.4.6, 5.3.6, 5.2.14, 4.5.5, and 3.2.11. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-17	6.4	CVE-2024-45812 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
vitejs--vite	Vite a frontend build tooling framework for javascript. In affected versions the contents of arbitrary files can be returned to the browser. `@fs` denies access to files outside of Vite serving allow list. Adding `?import&raw` to the URL bypasses this limitation and returns the file content if it exists. This issue has been patched in versions 5.4.6, 5.3.6, 5.2.14, 4.5.5, and 3.2.11. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-09-17	4.8	CVE-2024-45811 security-advisories@github.com security-advisories@github.com
wayneconnor--Sliding Door	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in wayneconnor Sliding Door allows Stored XSS.This issue affects Sliding Door: from n/a through 3.6.	2024-09-18	6.5	CVE-2024-43987 audit@patchstack.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
webdzier--Hotel Galaxy	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in webdzier Hotel Galaxy allows Stored XSS.This issue affects Hotel Galaxy: from n/a through 4.4.24.	2024-09-18	6.5	CVE-2024-43991 audit@patchstack.com
WP Royal--Royal Elementor Addons	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Royal Royal Elementor Addons allows Stored XSS.This issue affects Royal Elementor Addons: from n/a through 1.3.982.	2024-09-18	6.5	CVE-2024-44001 audit@patchstack.com
Wpsoul--Greenshift animation and page builder blocks	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wpsoul Greenshift - animation and page builder blocks allows Stored XSS.This issue affects Greenshift - animation and page builder blocks: from n/a through 9.3.7.	2024-09-18	6.5	CVE-2024-44005 audit@patchstack.com
xwiki--xwiki-platform	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible for any user knowing the ID of a notification filter preference of another user, to enable/disable it or even delete it. The impact is that the target user might start loosing notifications on some pages because of this. This vulnerability is present in XWiki since 13.2-rc-1. This vulnerability has been patched in XWiki 14.10.21, 15.5.5, 15.10.1, 16.0-rc-1. The patch consists in checking properly the rights of the user before performing any action on the filters. Users are advised to upgrade. It's possible to fix manually the vulnerability by editing the document `XWiki.Notifications.Code.NotificationPreferenceService` to apply the changes performed in commit e8acc9d8e6af7dfbfe70716ded431642ae4a6dd4.	2024-09-18	6.5	CVE-2024-46978 security-advisories@github.com security-advisories@github.com security-advisories@github.com
xwiki--xwiki-platform	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible to get access to notification filters of any user by using a URL such as `<hostname>xwiki/bin/get/XWiki/Notifications/Code/NotificationFilterPreferenceLivetableResults?outputSyntax=plain&type=custom&user=<username>`. This vulnerability impacts all versions of XWiki since 13.2-rc-1. The filters do not provide much information (they mainly contain references which are public data in XWiki), though some info could be used in combination with other vulnerabilities. This vulnerability has been patched in XWiki 14.10.21, 15.5.5, 15.10.1, 16.0RC1. The patch consists in checking the rights of the user when sending the data. Users are advised to upgrade. It's possible to workaround the vulnerability by applying manually the patch: it's possible for an administrator to edit directly the document `XWiki.Notifications.Code.NotificationFilterPreferenceLivetableResults` to apply the same changes as in the patch. See commit c8c6545f9bde6f5aade994aa5b5903a67b5c2582.	2024-09-18	5.3	CVE-2024-46979 security-advisories@github.com security-advisories@github.com security-advisories@github.com
Yordam Information Technology--Yordam Library Automation System	Improper Restriction of Excessive Authentication Attempts vulnerability in Yordam Information Technology Yordam Library Automation System allows Interface Manipulation.This issue affects Yordam Library Automation System: before 20.1.	2024-09-18	6.5	CVE-2024-5682 iletisim@usom.gov.tr
zitadel--zitadel	Zitadel is an open source identity management platform. In Zitadel, even after an organization is deactivated, associated projects, respectively their applications remain active. Users across other organizations can still log in and access through these applications, leading to unauthorized access. Additionally, if a project was deactivated access to applications was also still possible. The issue stems from the fact that when an organization is deactivated in Zitadel, the applications associated with it do not automatically deactivate. The application lifecycle is not tightly coupled with the organization's lifecycle, leading to a situation where the organization or project is marked as inactive, but its resources remain accessible.	2024-09-20	4.3	CVE-2024-47060 security-advisories@github.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This vulnerability allows for unauthorized access to projects and their resources, which should have been restricted post-organization deactivation. Versions 2.62.1, 2.61.1, 2.60.2, 2.59.3, 2.58.5, 2.57.5, 2.56.6, 2.55.8, and 2.54.10 have been released which address this issue. Users are advised to upgrade. Users unable to upgrade may explicitly disable the application to make sure the client is not allowed anymore.			
ZTE--MF296R	There is a buffer overflow vulnerability in ZTE MF296R. Due to insufficient validation of the SMS parameter length, an authenticated attacker could use the vulnerability to perform a denial of service attack.	2024-09-18	4.5	CVE-2022-39068 psirt@zte.com.cn

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
HCL Software--Nomad server on Domino	HCL Nomad server on Domino did not configure certain HTTP Security headers by default which could allow an attacker to obtain sensitive information via unspecified vectors.	2024-10-01	3.7	CVE-2024-30132 psirt@hcl.com
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Self Cross-Site Scripting (Self-XSS) vulnerability in the "Alert Templates" feature allows users to inject arbitrary JavaScript into the alert template's name. This script executes immediately upon submission but does not persist after a page refresh.	2024-10-01	3.5	CVE-2024-47526 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
miraheze--DataDump	DataDump is a MediaWiki extension that provides dumps of wikis. Several interface messages are unescaped (more specifically, (datadump-table-column-queued), (datadump-table-column-in-progress), (datadump-table-column-completed), (datadump-table-column-failed)). If these messages are edited (which requires the (editinterface) right by default), anyone who can view Special:DataDump (which requires the (view-dump) right by default) can be XSSed. This vulnerability is fixed with 601688ee8e8808a23b102fa305b178f27cbd226d.	2024-10-02	3.5	CVE-2024-47612 security-advisories@github.com security-advisories@github.com security-advisories@github.com
n/a--OFCMS	A vulnerability classified as problematic has been found in OFCMS 1.1.2. This affects the function add of the file /admin/system/dict/add.json?sqlid=system.dict.save. The manipulation of the argument dict_value 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.	2024-10-01	3.5	CVE-2024-9411 cna@vuldb.com cna@vuldb.com cna@vuldb.com
Netadmin Software--NetAdmin IAM	A vulnerability was found in Netadmin Software NetAdmin IAM up to 3.5 and classified as problematic. Affected by this issue is some unknown functionality of the file /controller/api/Answer/ReturnUserQuestionsFilled of the component HTTP POST Request Handler. The manipulation of the argument username leads to information exposure through discrepancy. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-04	3.7	CVE-2024-9513 cna@vuldb.com cna@vuldb.com cna@vuldb.com
NVIDIA--CUDA Toolkit	NVIDIA CUDA toolkit for Windows and Linux contains a vulnerability in the nvdisasm command line tool where an attacker may cause an improper validation in input issue by tricking the user into running nvdisasm on a malicious ELF file. A successful exploit of this vulnerability may lead to denial of service.	2024-10-03	3.3	CVE-2024-0123 psirt@nvidia.com
NVIDIA--CUDA Toolkit	NVIDIA CUDA Toolkit for Windows and Linux contains a vulnerability in the nvdisam command line tool, where a user can cause nvdisasm to read freed memory by running it on a malformed ELF file. A successful exploit of this vulnerability might lead to a limited denial of service.	2024-10-03	3.3	CVE-2024-0124 psirt@nvidia.com

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
NVIDIA--CUDA Toolkit	NVIDIA CUDA Toolkit for Windows and Linux contains a vulnerability in the nvdisam command line tool, where a user can cause a NULL pointer dereference by running nvdisasm on a malformed ELF file. A successful exploit of this vulnerability might lead to a limited denial of service.	2024-10-03	3.3	CVE-2024-0125 psirt@nvidia.com
Sovell--Smart Canteen System	A vulnerability classified as problematic was found in Sovell Smart Canteen System up to 3.0.7303.30513. Affected by this vulnerability is the function Check_ET_CheckPwdz201 of the file suanfa.py of the component Password Reset Handler. The manipulation leads to authorization bypass. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.	2024-10-06	3.7	CVE-2024-9554 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
authzed--spicedb	spicedb is an Open Source, Google Zanzibar-inspired permissions database to enable fine-grained authorization for customer applications. Multiple caveats over the same indirect subject type on the same relation can result in no permission being returned when permission is expected. If the resource has multiple groups, and each group is caveated, it is possible for the returned permission to be "no permission" when permission is expected. Permission is returned as NO_PERMISSION when PERMISSION is expected on the CheckPermission API. This issue has been addressed in release version 1.35.3. Users are advised to upgrade. Users unable to upgrade should not use caveats or avoid the use of caveats on an indirect subject type with multiple entries.	2024-09-18	3.7	CVE-2024-46989 security-advisories@github.com security-advisories@github.com
code-projects--Blood Bank Management System	A vulnerability, which was classified as problematic, was found in code-projects Blood Bank Management System 1.0. This affects an unknown part of the component Password Handler. The manipulation leads to cleartext storage in a file or on disk. An attack has to be approached locally.	2024-09-20	2.3	CVE-2024-9040 cna@vuldb.com cna@vuldb.com cna@vuldb.com
code-projects--Blood Bank System	A vulnerability classified as problematic was found in code-projects Blood Bank System 1.0. This vulnerability affects unknown code of the file bbms.php. The manipulation of the argument fullname/age/bloodgroup/city/phno/gender as part of String leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-09-22	3.5	CVE-2024-9084 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
CodeCanyon--CRMGo SaaS	A vulnerability classified as problematic was found in CodeCanyon CRMGo SaaS 7.2. This vulnerability affects unknown code of the file /deal/{note_id}/note. The manipulation of the argument notes leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-09-20	3.5	CVE-2024-9030 cna@vuldb.com cna@vuldb.com cna@vuldb.com
CodeCanyon--CRMGo SaaS	A vulnerability, which was classified as problematic, has been found in CodeCanyon CRMGo SaaS up to 7.2. This issue affects some unknown processing of the file /project/task/{task_id}/show. The manipulation of the argument comment leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-09-20	3.5	CVE-2024-9031 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
GitLab--GitLab	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.7 prior to 17.1.7, 17.2 prior to 17.2.5, and 17.3 prior to 17.3.2, where group runners information was disclosed to unauthorised group members.	2024-09-16	3.1	CVE-2024-6685 cve@gitlab.com cve@gitlab.com
jeanmarc77--123solar	A vulnerability classified as problematic has been found in jeanmarc77 123solar 1.8.4.5. This affects an unknown part of the file /detailed.php. The manipulation of the argument date1 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 patch	2024-09-19	3.5	CVE-2024-9007 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	is named 94bf9ab7ad0ccb7fbdc02f172f37f0e2ea08d48f. It is recommended to apply a patch to fix this issue.			cna@vuldb.com cna@vuldb.com
Mautic--Mautic	With access to edit a Mautic form, the attacker can add Cross-Site Scripting stored in the html filed. This could be used to steal sensitive information from the user's current session.	2024-09-18	2.9	CVE-2024-47058 security@mautic.org
n/a--dingfangzu	A vulnerability classified as problematic has been found in dingfangzu up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. Affected is an unknown function of the file scripts/order.js of the component Order Checkout. The manipulation of the argument address-name 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. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	2024-09-22	3.5	CVE-2024-9077 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
n/a--Intel(R) RAID Web Console software	Improper access control in Intel(R) RAID Web Console software all versions may allow an authenticated user to potentially enable denial of service via adjacent access.	2024-09-16	3.5	CVE-2024-36261 secure@intel.com
n/a--Intel(R) RAID Web Console	Improper access control in Intel(R) RAID Web Console all versions may allow an authenticated user to potentially enable information disclosure via local access.	2024-09-16	3.3	CVE-2024-28170 secure@intel.com
n/a--UEFI firmware for some Intel(R) Processors	Out-of-bounds read in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable denial of service via local access.	2024-09-16	2.5	CVE-2023-25546 secure@intel.com
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in QEMU, in the virtio-scsi, virtio-blk, and virtio-crypto devices. The size for virtqueue_push as set in virtio_scsi_complete_req / virtio_blk_req_complete / virito_crypto_req_complete could be larger than the true size of the data which has been sent to guest. Once virtqueue_push() finally calls dma_memory_unmap to ummap the in_iov, it may call the address_space_write function to write back the data. Some uninitialized data may exist in the bounce.buffer, leading to an information leak.	2024-09-20	3.8	CVE-2024-8612 secalert@redhat.com secalert@redhat.com
SourceCodester--Best House Rental Management System	A vulnerability has been found in SourceCodester Best House Rental Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=save_category. The manipulation of the argument name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-09-20	3.5	CVE-2024-9033 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Employee Management System	A vulnerability classified as problematic has been found in SourceCodester Employee Management System 1.0. This affects an unknown part of the file /Admin/add-admin.php. The manipulation of the argument txtfullname 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.	2024-09-22	2.4	CVE-2024-9083 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Resort Reservation System	A vulnerability classified as problematic was found in SourceCodester Resort Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file manage_fee.php. The manipulation of the argument toview leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-09-17	3.5	CVE-2024-8951 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				cna@vuldb.com
Stirling-Tools--Stirling-PDF	A vulnerability was found in Stirling-Tools Stirling-PDF up to 0.28.3. It has been declared as problematic. This vulnerability affects unknown code of the component Markdown-to-PDF. The manipulation leads to cross site scripting. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. Upgrading to version 0.29.0 is able to address this issue. It is recommended to upgrade the affected component. The vendor explains that "this functionality was removed in 0.29.0 already" and "we plan to re-add at later date with issue resolved".	2024-09-21	2.6	CVE-2024-9075 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
y_project--RuoYi	A vulnerability was found in y_project RuoYi up to 4.7.9. It has been declared as problematic. Affected by this vulnerability is the function SysUserServiceImpl of the file ruoyi-system/src/main/java/com/ruoyi/system/service/impl/SysUserServiceImpl.java of the component Backend User Import. The manipulation of the argument loginName leads to cross site scripting. 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 patch is named 9b68013b2af87b9c809c4637299abd929bc73510. It is recommended to apply a patch to fix this issue.	2024-09-21	3.1	CVE-2024-9048 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com