BULLETIN (SB24-337)

VULNERABILITY SUMMARY FOR THE WEEK OF

25TH NOVEMBER, 2024

Bulletin (SB24-337)
Vulnerability Summary for the Week of November 25, 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
1000 Projects--Portfolio Management System MCA	A vulnerability has been found in 1000 Projects Portfolio Management System MCA 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /register.php. The manipulation of the argument name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	2024-11-26	7.3	CVE-2024-11744
1000 Projects--Portfolio Management System MCA	A vulnerability classified as critical was found in 1000 Projects Portfolio Management System MCA 1.0. This vulnerability affects unknown code of the file /forgot_password_process.php. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-27	7.3	CVE-2024-11819
1000projects --beauty_parlour_management_system	A vulnerability classified as critical was found in 1000 Projects Beauty Parlour Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/edit-services.php. The manipulation of the argument sername leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-25	7.3	CVE-2024-11646
1000projects --beauty_parlour_management_system	A vulnerability, which was classified as critical, has been found in 1000 Projects Beauty Parlour Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/view-appointment.php. The manipulation of the argument viewid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-25	7.3	CVE-2024-11647
1000projects --beauty_parlour_management_system	A vulnerability, which was classified as critical, was found in 1000 Projects Beauty Parlour Management System 1.0. This affects an unknown part of the file /admin/add-customer.php. The manipulation of the argument name leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-25	7.3	CVE-2024-11648
1000projects --beauty_parlour_management_system	A vulnerability has been found in 1000 Projects Beauty Parlour Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/search-appointment.php. The manipulation of the argument searchdata leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-25	7.3	CVE-2024-11649
AbsolutePlugins--Absolute Addons For Elementor	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in AbsolutePlugins Absolute Addons For Elementor allows Local Code Inclusion.This issue affects Absolute Addons For Elementor: from n/a through 1.0.14.	2024-11-28	7.5	CVE-2024-52496
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The vulnerability can be exploited by remote unauthenticated users capable of interacting with the default "edgserver" service enabled on the access point and malicious commands are executed with root privileges. No authentication is enabled on the service and the source of the vulnerability resides in processing code associated to the "cfg_cmd_set_eth_conf" operation.	2024-11-26	9.8	CVE-2024-50370
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The vulnerability can be exploited by remote unauthenticated users capable of interacting with the default "edgserver" service enabled on the access point and malicious commands are executed with root privileges. No authentication is enabled on the service and the source of the vulnerability resides in processing code associated to the "wlan_scan" operation.	2024-11-26	9.8	CVE-2024-50371
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The vulnerability can be exploited by remote unauthenticated users capable of interacting with the default "edgserver" service enabled on the access point and malicious commands are executed with root privileges. No authentication is enabled on the service and the source of the vulnerability resides in processing code associated to the "backup_config_to_utility" operation.	2024-11-26	9.8	CVE-2024-50372
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The vulnerability can be exploited by	2024-11-26	9.8	CVE-2024-50373

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote unauthenticated users capable of interacting with the default "edgserver" service enabled on the access point and malicious commands are executed with root privileges. No authentication is enabled on the service and the source of the vulnerability resides in processing code associated to the "restore_config_from_utility" operation.			
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The vulnerability can be exploited by remote unauthenticated users capable of interacting with the default "edgserver" service enabled on the access point and malicious commands are executed with root privileges. No authentication is enabled on the service and the source of the vulnerability resides in processing code associated to the "capture_packages" operation.	2024-11-26	9.8	CVE-2024-50374
Advantech--EKI-6333AC-2G	A CWE-306 "Missing Authentication for Critical Function" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The vulnerability can be exploited by remote unauthenticated users capable of interacting with the default "edgserver" service enabled on the access point.	2024-11-26	9.8	CVE-2024-50375
Advantech--EKI-6333AC-2G	A CWE-15 "External Control of System or Configuration Setting" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The vulnerability can be exploited by authenticated users by restoring a tampered configuration backup.	2024-11-26	7.2	CVE-2024-50358
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The source of the vulnerability relies on multiple parameters belonging to the "scan_ap" API which are not properly sanitized before being concatenated to OS level commands.	2024-11-26	7.2	CVE-2024-50359
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The source of the vulnerability relies on multiple parameters belonging to the "snmp_apply" API which are not properly sanitized before being concatenated to OS level commands.	2024-11-26	7.2	CVE-2024-50360
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The source of the vulnerability relies on multiple parameters belonging to the "certificate_file_remove" API which are not properly sanitized before being concatenated to OS level commands.	2024-11-26	7.2	CVE-2024-50361
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The source of the vulnerability relies on multiple parameters belonging to the "connection_profile_apply" API which are not properly sanitized before being concatenated to OS level commands.	2024-11-26	7.2	CVE-2024-50362
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The source of the vulnerability relies on multiple parameters belonging to the "mp_apply" API which are not properly sanitized before being concatenated to OS level commands.	2024-11-26	7.2	CVE-2024-50363
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The source of the vulnerability relies on multiple parameters belonging to the "export_log" API which are not properly sanitized before being concatenated to OS level commands.	2024-11-26	7.2	CVE-2024-50364
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The source of the vulnerability relies on	2024-11-26	7.2	CVE-2024-50365

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	multiple parameters belonging to the "lan_apply" API which are not properly sanitized before being concatenated to OS level commands.			
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The source of the vulnerability relies on multiple parameters belonging to the "applications_apply" API which are not properly sanitized before being concatenated to OS level commands.	2024-11-26	7.2	CVE-2024-50366
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The source of the vulnerability relies on multiple parameters belonging to the "sta_log_htm" API which are not properly sanitized before being concatenated to OS level commands.	2024-11-26	7.2	CVE-2024-50367
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The source of the vulnerability relies on multiple parameters belonging to the "basic_htm" API which are not properly sanitized before being concatenated to OS level commands.	2024-11-26	7.2	CVE-2024-50368
Advantech--EKI-6333AC-2G	A CWE-78 "Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The source of the vulnerability relies on multiple parameters belonging to the "multiple_ssid_htm" API which are not properly sanitized before being concatenated to OS level commands.	2024-11-26	7.2	CVE-2024-50369
Advantech--EKI-6333AC-2G	A CWE-79 "Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The vulnerability can be exploited remotely leveraging a rogue Wi-Fi access point with a malicious SSID.	2024-11-26	7.3	CVE-2024-50376
Anzia--Ni WooCommerce Cost Of Goods	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Anzia Ni WooCommerce Cost Of Goods allows SQL Injection.This issue affects Ni WooCommerce Cost Of Goods: from n/a through 3.2.8.	2024-11-30	7.6	CVE-2024-53783
Apache Software Foundation--Apache Arrow R package	Deserialization of untrusted data in IPC and Parquet readers in the Apache Arrow R package versions 4.0.0 through 16.1.0 allows arbitrary code execution. An application is vulnerable if it reads Arrow IPC, Feather or Parquet data from untrusted sources (for example, user-supplied input files). This vulnerability only affects the arrow R package, not other Apache Arrow implementations or bindings unless those bindings are specifically used via the R package (for example, an R application that embeds a Python interpreter and uses PyArrow to read files from untrusted sources is still vulnerable if the arrow R package is an affected version). It is recommended that users of the arrow R package upgrade to 17.0.0 or later. Similarly, it is recommended that downstream libraries upgrade their dependency requirements to arrow 17.0.0 or later. If using an affected version of the package, untrusted data can read into a Table and its internal to_data_frame() method can be used as a workaround (e.g., read_parquet(..., as_data_frame = FALSE)$to_data_frame()). This issue affects the Apache Arrow R package: from 4.0.0 through 16.1.0. Users are recommended to upgrade to version 17.0.0, which fixes the issue.	2024-11-28	9.8	CVE-2024-52338
Apache Software Foundation--Apache NimBLE	Out-of-bounds Read vulnerability in Apache NimBLE. Missing proper validation of HCI Number Of Completed Packets could lead to out-of-bound access when parsing HCI event and invalid read from HCI transport memory. This issue requires broken or bogus Bluetooth controller and thus severity is considered low. This issue affects Apache NimBLE: through 1.7.0. Users are recommended to upgrade to version 1.8.0, which fixes the issue.	2024-11-26	7.5	CVE-2024-51569
Astoundify--Jobify - Job Board WordPress Theme	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Astoundify Jobify - Job Board WordPress Theme allows Relative Path Traversal.This issue affects Jobify - Job Board WordPress Theme: from n/a through 4.2.3.	2024-11-28	7.5	CVE-2024-52481
Automation Web Platform--Wawp	Authentication Bypass Using an Alternate Path or Channel vulnerability in Automation Web Platform Wawp allows Authentication Bypass.This issue affects Wawp: from n/a before 3.0.18.	2024-11-28	9.8	CVE-2024-52475

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Axis Communications AB--AXIS Q6128-E PTZ Network Camera	Florent ThiÃ©ry has found that selected Axis devices were vulnerable to handling certain ethernet frames which could lead to the Axis device becoming unavailable in the network. Axis has released patched AXIS OS versions for the highlighted flaw for products that are still under AXIS OS software support. Please refer to the Axis security advisory for more information and solution.	2024-11-26	7.5	CVE-2024-47257
Billion Electric--M100	Certain modes of routers from Billion Electric have a Missing Authentication vulnerability, allowing unauthenticated remote attackers to directly access the specific functionality to obtain partial device information, modify the WiFi SSID, and restart the device.	2024-11-29	8.6	CVE-2024-11980
Billion Electric--M100	Certain models of routers from Billion Electric has an Authentication Bypass vulnerability, allowing unautheticated attackers to retrive contents of arbitrary web pages.	2024-11-29	7.5	CVE-2024-11981
Billion Electric--M100	Certain models of routers from Billion Electric has a Plaintext Storage of a Password vulnerability. Remote attackers with administrator privileges can access the user settings page to retrieve plaintext passwords.	2024-11-29	7.2	CVE-2024-11982
Billion Electric--M100	Certain models of routers from Billion Electric has an OS Command Injection vulnerability, allowing remote attackers with administrator privileges to inject arbitrary system commands into a specific SSH function and execute them on the device.	2024-11-29	7.2	CVE-2024-11983
boldgrid--Total Upkeep WordPress Backup Plugin plus Restore & Migrate by BoldGrid	The Total Upkeep - WordPress Backup Plugin plus Restore & Migrate by BoldGrid plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.16.6 via the cron_interval parameter. This is due to missing input validation and sanitization. This makes it possible for authenticated attackers, with Administrator-level access and above, to execute code on the server.	2024-11-26	7.2	CVE-2024-9461
cleantalk--Security & Malware scan by CleanTalk	The Security & Malware scan by CleanTalk plugin for WordPress is vulnerable to unauthorized SQL Injection due to an authorization bypass via reverse DNS spoofing on the checkWithoutToken function in all versions up to, and including, 2.145, as well as insufficient input sanitization and validation. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-11-26	7.5	CVE-2024-10570
cleantalk--Spam protection, Anti-Spam, FireWall by CleanTalk	The Spam protection, Anti-Spam, FireWall by CleanTalk plugin for WordPress is vulnerable to unauthorized Arbitrary Plugin Installation due to an authorization bypass via reverse DNS spoofing on the checkWithoutToken function in all versions up to, and including, 6.43.2. This makes it possible for unauthenticated attackers to install and activate arbitrary plugins which can be leveraged to achieve remote code execution if another vulnerable plugin is installed and activated.	2024-11-26	9.8	CVE-2024-10542
cleantalk--Spam protection, Anti-Spam, FireWall by CleanTalk	The Spam protection, Anti-Spam, FireWall by CleanTalk plugin for WordPress is vulnerable to unauthorized Arbitrary Plugin Installation due to an missing empty value check on the 'api_key' value in the 'perform' function in all versions up to, and including, 6.44. This makes it possible for unauthenticated attackers to install and activate arbitrary plugins which can be leveraged to achieve remote code execution if another vulnerable plugin is installed and activated.	2024-11-26	8.1	CVE-2024-10781
code-projects--Concert Ticket Ordering System	A vulnerability classified as critical has been found in code-projects Concert Ticket Ordering System 1.0. Affected is an unknown function of the file /tour(cor).php. The manipulation of the argument mai leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-28	7.3	CVE-2024-11970
code-projects--Simple Car Rental System	A vulnerability classified as critical was found in code-projects Simple Car Rental System 1.0. Affected by this vulnerability is an unknown functionality of the file /login.php. The manipulation of the argument uname leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-28	7.3	CVE-2024-11962
Codezips--E-Commerce Site	A vulnerability classified as critical was found in Codezips E-Commerce Site 1.0. Affected by this vulnerability is an unknown functionality of the file search.php. The manipulation of the argument keywords leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-25	7.3	CVE-2024-11663
contest-gallery--Photos, Files, YouTube, Twitter, Instagram, TikTok, Ecommerce Contest Gallery	The Contest Gallery plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 24.0.7. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gain access to their account.	2024-11-28	9.8	CVE-2024-11103

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Upload, Vote, Sell via PayPal, Social Share Buttons				
contiki-ng--contiki-ng	Contiki-NG is an open-source, cross-platform operating system for IoT devices. An out-of-bounds read of 1 byte can be triggered when sending a packet to a device running the Contiki-NG operating system with SNMP enabled. The SNMP module is disabled in the default Contiki-NG configuration. The vulnerability exists in the os/net/app-layer/snmp/snmp-ber.c module, where the function snmp_ber_decode_string_len_buffer decodes the string length from a received SNMP packet. In one place, one byte is read from the buffer, without checking that the buffer has another byte available, leading to a possible out-of-bounds read. The problem has been patched in Contiki-NG pull request #2936. It will be included in the next release of Contiki-NG. Users are advised to apply the patch manually or to wait for the next release. A workaround is to disable the SNMP module in the Contiki-NG build configuration.	2024-11-27	8.3	CVE-2024-41125
contiki-ng--contiki-ng	Contiki-NG is an open-source, cross-platform operating system for IoT devices. An out-of-bounds read of 1 byte can be triggered when sending a packet to a device running the Contiki-NG operating system with SNMP enabled. The SNMP module is disabled in the default Contiki-NG configuration. The vulnerability exists in the os/net/app-layer/snmp/snmp-message.c module, where the snmp_message_decode function fails to check the boundary of the message buffer when reading a byte from it immediately after decoding an object identifier (OID). The problem has been patched in Contiki-NG pull request 2937. It will be included in the next release of Contiki-NG. Users are advised to either apply the patch manually or to wait for the next release. A workaround is to disable the SNMP module in the Contiki-NG build configuration.	2024-11-27	8.3	CVE-2024-41126
contiki-ng--contiki-ng	Contiki-NG is an open-source, cross-platform operating system for IoT devices. An unaligned memory access can be triggered in the two RPL implementations of the Contiki-NG operating system. The problem can occur when either one of these RPL implementations is enabled and connected to an RPL instance. If an IPv6 packet containing an odd number of padded bytes before the RPL option, it can cause the rpl_ext_header_hbh_update function to read a 16-bit integer from an odd address. The impact of this unaligned read is architecture-dependent, but can potentially cause the system to crash. The problem has not been patched as of release 4.9, but will be included in the next release. One can apply the changes in Contiki-NG pull request #2962 to patch the system or wait for the next release.	2024-11-27	7.5	CVE-2024-47181
Cool Plugins--Cryptocurrency Widgets For Elementor	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Cool Plugins Cryptocurrency Widgets For Elementor allows PHP Local File Inclusion.This issue affects Cryptocurrency Widgets For Elementor: from n/a through 1.6.4.	2024-11-30	8.1	CVE-2024-53739
Cradlepoint--NetCloud Exchange Client	The NetCloud Exchange client for Windows, version 1.110.50, contains an insecure file and folder permissions vulnerability. A normal (non-admin) user could exploit the weakness in file and folder permissions to escalate privileges, execute arbitrary code and maintain persistence on the compromised machine. It has been identified that full control permissions exist on the 'Everyone' group (i.e. any user who has local access to the operating system regardless of their privileges).	2024-11-28	8.8	CVE-2024-11969
D-Link--DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01. It has been classified as critical. This affects the function formResetStatistic of the file /goform/formResetStatistic. 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.	2024-11-28	8.8	CVE-2024-11959
D-Link--DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01. It has been declared as critical. This vulnerability affects the function formSetPortTr of the file /goform/formSetPortTr. 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.	2024-11-28	8.8	CVE-2024-11960
DapperDuckling--keycloak-connector	@dapperduckling/keycloak-connector-server is an opinionated series of libraries for Node.js applications and frontend clients to interface with keycloak. A Reflected Cross-Site Scripting (XSS) vulnerability was discovered in the authentication flow of the application. This issue arises due to improper sanitization of the URL parameters, allowing the URL bar's contents to be injected and reflected into the HTML page. An attacker could craft a malicious URL to execute arbitrary JavaScript in the browser of a victim who visits the link. Any application utilizing this	2024-11-26	8.1	CVE-2024-53843

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authentication library is vulnerable. Users of the application are at risk if they can be lured into clicking on a crafted malicious link. The vulnerability has been patched in version 2.5.5 by ensuring proper sanitization and escaping of user input in the affected URL parameters. Users are strongly encouraged to upgrade. If upgrading is not immediately possible, users can implement the following workarounds: 1. Employ a Web Application Firewall (WAF) to block malicious requests containing suspicious URL parameters. or 2. Apply input validation and escaping directly within the application's middleware or reverse proxy layer, specifically targeting the affected parameters.			
Dell--Wyse Management Suite	Dell Wyse Management Suite, version WMS 4.4 and before, contain an Authentication Bypass by Capture-replay vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Denial of service.	2024-11-26	7.6	CVE-2024-49595
Dell--Wyse Management Suite	Dell Wyse Management Suite, versions WMS 4.4 and prior, contain an Improper Restriction of Excessive Authentication Attempts vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Protection mechanism bypass.	2024-11-26	7.6	CVE-2024-49597
Eniture Technology--Distance Based Shipping Calculator	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Eniture Technology Distance Based Shipping Calculator allows SQL Injection.This issue affects Distance Based Shipping Calculator: from n/a through 2.0.21.	2024-11-28	8.5	CVE-2024-52495
Essential Marketer--Essential Breadcrumbs	Cross-Site Request Forgery (CSRF) vulnerability in Essential Marketer Essential Breadcrumbs allows Stored XSS.This issue affects Essential Breadcrumbs: from n/a through 1.1.1.	2024-11-30	7.1	CVE-2024-53778
FUJI ELECTRIC CO., LTD. and Hakko Electronics Co., Ltd.--TELLUS	There is an Out-of-bounds read vulnerability in TELLUS (v4.0.19.0 and earlier) and TELLUS Lite (v4.0.19.0 and earlier). If a user opens a specially crafted file, information may be disclosed and/or arbitrary code may be executed.	2024-11-28	7.8	CVE-2024-38389
FUJI ELECTRIC CO., LTD. and Hakko Electronics Co., Ltd.--V-Server	There is an Out-of-bounds read vulnerability in V-Server (v4.0.19.0 and earlier) and V-Server Lite (v4.0.19.0 and earlier). If a user opens a specially crafted file, information may be disclosed and/or arbitrary code may be executed.	2024-11-28	7.8	CVE-2024-38658
FUJI ELECTRIC CO., LTD. and Hakko Electronics Co., Ltd.--V-SFT	There are multiple stack-based buffer overflow vulnerabilities in V-SFT (v6.2.2.0 and earlier), TELLUS (v4.0.19.0 and earlier), and TELLUS Lite (v4.0.19.0 and earlier). If a user opens a specially crafted file, information may be disclosed and/or arbitrary code may be executed.	2024-11-28	7.8	CVE-2024-38309
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 8.12 before 17.4.5, 17.5 before 17.5.3, and 17.6 before 17.6.1. This issue allows an attacker with access to a victim's Personal Access Token (PAT) to escalate privileges.	2024-11-26	8.2	CVE-2024-8114
Google--Android	In checkPermissions of RecognitionService.java, there is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-27	8.4	CVE-2017-13316
Google--Android	In String16 of String16.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-27	8.4	CVE-2017-13323
Google--Android	In pvmp3_get_main_data_size of pvmp3_get_main_data_size.cpp, there is a possible buffer overread due to a missing bounds check. This could lead to remote information disclosure of global static variables with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-27	7.5	CVE-2017-13319
Google--Android	In installPackageLI of PackageManagerService.java, there is a possible permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	2024-11-28	7.8	CVE-2018-9374
Google--Chrome	Integer overflow in Layout in Google Chrome prior to 129.0.6668.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-11-27	8.8	CVE-2024-7025

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Hewlett Packard Enterprise (HPE)--HPE Insight Remote Support	A directory traversal vulnerability in Hewlett Packard Enterprise Insight Remote Support may allow remote code execution.	2024-11-27	9.8	CVE-2024-53676
Hewlett Packard Enterprise (HPE)--HPE Insight Remote Support	An XML external entity injection (XXE) vulnerability in HPE Insight Remote Support may allow remote users to disclose information in certain cases.	2024-11-26	7.3	CVE-2024-11622
Hewlett Packard Enterprise (HPE)--HPE Insight Remote Support	An XML external entity injection (XXE) vulnerability in HPE Insight Remote Support may allow remote users to disclose information in certain cases.	2024-11-26	7.3	CVE-2024-53674
Hewlett Packard Enterprise (HPE)--HPE Insight Remote Support	An XML external entity injection (XXE) vulnerability in HPE Insight Remote Support may allow remote users to disclose information in certain cases.	2024-11-26	7.3	CVE-2024-53675
Hewlett Packard Enterprise (HPE)--Insight Remote Support	A java deserialization vulnerability in HPE Remote Insight Support may allow an unauthenticated attacker to execute code.	2024-11-26	8.1	CVE-2024-53673
https://codecanyon.net/item/jobsearch-wp-job-board-wordpress-plugin/21066856--JobSearch WP Job Board	The JobSearch WP Job Board plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 2.6.7. This is due to the plugin not properly verifying a users identity when verifying an email address through the user_account_activation function. This makes it possible for unauthenticated attackers to log in as any user, including site administrators if the users email is known.	2024-11-28	9.8	CVE-2024-11925
IBM--Data Virtualization Manager for z/OS	IBM Data Virtualization Manager for z/OS 1.1 and 1.2 could allow an authenticated user to inject malicious JDBC URL parameters and execute code on the server.	2024-11-26	8.5	CVE-2024-52899
IBM--Security Verify Access	IBM Security Verify Access Appliance 10.0.0 through 10.0.8 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request.	2024-11-29	9.8	CVE-2024-49803
IBM--Security Verify Access	IBM Security Verify Access Appliance 10.0.0 through 10.0.8 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.	2024-11-29	9.4	CVE-2024-49805
IBM--Security Verify Access	IBM Security Verify Access Appliance 10.0.0 through 10.0.8 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.	2024-11-29	9.4	CVE-2024-49806
IBM--Security Verify Access	IBM Security Verify Access Appliance 10.0.0 through 10.0.8 could allow a locally authenticated non-administrative user to escalate their privileges due to unnecessary permissions used to perform certain tasks.	2024-11-29	7.8	CVE-2024-49804
IBM--Watson Speech Services Cartridge for IBM Cloud Pak for Data	IBM Watson Speech Services Cartridge for IBM Cloud Pak for Data 4.0.0 through 5.0.2 does not properly check inputs to resources that are used concurrently, which might lead to unexpected states, possibly resulting in a crash.	2024-11-26	7.5	CVE-2024-49353
Idealien Studios--Idealien Category Enhancements	Cross-Site Request Forgery (CSRF) vulnerability in Idealien Studios Idealien Category Enhancements allows Stored XSS.This issue affects Idealien Category Enhancements: from n/a through 1.2.	2024-11-28	7.1	CVE-2024-53734
Imagination Technologies--Graphics DDK	Software installed and run as a non-privileged user may conduct improper GPU system calls to allow unprivileged access to arbitrary physical memory page.	2024-11-30	8.1	CVE-2024-43702

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Imagination Technologies--Graphics DDK	Software installed and run as a non-privileged user may conduct improper GPU system calls to achieve unauthorised reads and writes of physical memory from the GPU HW.	2024-11-30	8.1	CVE-2024-43703
Interinfo--DreamMaker	DreamMaker from Interinfo has a Path Traversal vulnerability and does not restrict the types of uploaded files. This allows unauthenticated remote attackers to upload arbitrary files to any directory, leading to arbitrary code execution by uploading webshells.	2024-11-29	9.8	CVE-2024-11979
Interinfo--DreamMaker	DreamMaker from Interinfo has a Path Traversal vulnerability, allowing unauthenticated remote attackers to exploit this vulnerability to read arbitrary system files.	2024-11-29	7.5	CVE-2024-11978
Jason Grim--Custom Shortcode Sidebars	Cross-Site Request Forgery (CSRF) vulnerability in Jason Grim Custom Shortcode Sidebars allows Stored XSS.This issue affects Custom Shortcode Sidebars: from n/a through 1.2.	2024-11-28	7.1	CVE-2024-53736
Jenkins Project--Jenkins Simple Queue Plugin	Jenkins Simple Queue Plugin 1.4.4 and earlier does not escape the view name, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with View/Create permission.	2024-11-27	8	CVE-2024-54003
Kardi--Pricing table addon for elementor	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Kardi Pricing table addon for elementor allows PHP Local File Inclusion.This issue affects Pricing table addon for elementor: from n/a through 1.0.0.	2024-11-28	7.5	CVE-2024-52499
laurent22--joplin	Joplin is an open source, privacy-focused note taking app with sync capabilities for Windows, macOS, Linux, Android and iOS. In affected versions attackers are able to abuse the fact that openExternal is used without any filtering of URI schemes to obtain remote code execution in Windows environments. This issue has been addressed in version 3.0.3 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-11-25	7.2	CVE-2024-53268
lfprojects--mlflow	Excessive directory permissions in MLflow leads to local privilege escalation when using spark_udf. This behavior can be exploited by a local attacker to gain elevated permissions by using a ToCToU attack. The issue is only relevant when the spark_udf() MLflow API is called.	2024-11-25	7	CVE-2024-27134
LLC Â«TriIncom--Express Payments Module	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in LLC Â«TriIncomÂ» Express Payments Module allows Blind SQL Injection.This issue affects Express Payments Module: from n/a through 1.1.8.	2024-11-28	9.3	CVE-2024-52474
lobehub--lobe-chat	Lobe Chat is an open-source, AI chat framework. Versions of lobe-chat prior to 1.19.13 have an unauthorized ssrf vulnerability. An attacker can construct malicious requests to cause SSRF without logging in, attack intranet services, and leak sensitive information. The jwt token header X-Lobe-Chat-Auth strored proxy address and OpenAI API Key, can be modified to scan an internal network in the target lobe-web environment. This issue has been addressed in release version 1.19.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-11-26	8.1	CVE-2024-32965
Maeve Lander--PayPal Responder	Cross-Site Request Forgery (CSRF) vulnerability in Maeve Lander PayPal Responder allows Stored XSS.This issue affects PayPal Responder: from n/a through 1.2.	2024-12-01	7.1	CVE-2024-53750
ManageEngine--Analytics Plus	Zohocorp ManageEngine Analytics Plus versions below 6100 are vulnerable to authenticated sensitive data exposure which allows the users to retrieve sensitive tokens associated to the org-admin account.	2024-11-27	8.1	CVE-2024-52323
marketingfire--Widget Options The #1 WordPress Widget & Block Control Plugin	The Widget Options - The #1 WordPress Widget & Block Control Plugin plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.0.7 via the display logic functionality that extends several page builders. This is due to the plugin allowing users to supply input that will be passed through eval() without any filtering or capability checks. This makes it possible for authenticated attackers, with contributor-level access and above, to execute code on the server. Special note: We suggested the vendor implement an allowlist of functions and limit the ability to execute commands to just administrators, however, they did not take our advice. We are considering this patched, however, we believe it could still be further hardened and there may be residual risk with how the issue is currently patched.	2024-11-28	9.9	CVE-2024-8672
Mattermost--Mattermost	Mattermost versions 10.0.x <= 10.0.1, 10.1.x <= 10.1.1, 9.11.x <= 9.11.3, 9.5.x <= 9.5.11 fail to properly validate email addresses which allows an unauthenticated	2024-11-28	8.2	CVE-2024-11599

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	user to bypass email domain restrictions via carefully crafted input on email registration.			
Microsoft--Dynamics 365 Sales for Android	Microsoft Dynamics 365 Sales Spoofing Vulnerability	2024-11-26	7.6	CVE-2024-49053
Microsoft--Microsoft Azure Functions	Missing authentication for critical function in Microsoft Azure PolicyWatch allows an unauthorized attacker to elevate privileges over a network.	2024-11-26	8.2	CVE-2024-49052
Microsoft--Microsoft Copilot Studio	Improper neutralization of input during web page generation ('Cross-site Scripting') in Copilot Studio by an unauthorized attacker leads to elevation of privilege over a network.	2024-11-26	9.3	CVE-2024-49038
Microsoft--Microsoft Partner Center	An improper access control vulnerability in Partner.Microsoft.com allows an a unauthenticated attacker to elevate privileges over a network.	2024-11-26	8.7	CVE-2024-49035
Mitsubishi Electric Corporation--GENESIS64	Uncontrolled Search Path Element vulnerability in ICONICS GENESIS64 all versions, Mitsubishi Electric GENESIS64 all versions and Mitsubishi Electric MC Works64 all versions allows a local authenticated attacker to execute a malicious code by storing a specially crafted DLL in a specific folder. This could lead to disclose, tamper with, destroy, or delete information in the affected products, or cause a denial of service (DoS) condition on the products.	2024-11-28	7.8	CVE-2024-8299
Mitsubishi Electric Corporation--GENESIS64	Dead Code vulnerability in ICONICS GENESIS64 Version 10.97.2, 10.97.2 CFR1, 10.97.2 CRF2 and 10.97.3 and Mitsubishi Electric GENESIS64 Version 10.97.2, 10.97.2 CFR1, 10.97.2 CRF2 and 10.97.3 allows a local authenticated attacker to execute a malicious code by tampering with a specially crafted DLL. This could lead to disclose, tamper with, destroy, or delete information in the affected products, or cause a denial of service (DoS) condition on the products.	2024-11-28	7	CVE-2024-8300
Mitsubishi Electric Corporation--GENESIS64	Uncontrolled Search Path Element vulnerability in ICONICS GENESIS64 all versions, Mitsubishi Electric GENESIS64 all versions and Mitsubishi Electric MC Works64 all versions allows a local authenticated attacker to execute a malicious code by storing a specially crafted DLL in a specific folder. This could lead to disclose, tamper with, destroy, or delete information in the affected products, or cause a denial of service (DoS) condition on the products.	2024-11-28	7.8	CVE-2024-9852
Mozilla--Convict	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') vulnerability in Mozilla Convict. This allows an attacker to inject attributes that are used in other components, or to override existing attributes with ones that have incompatible type, which may lead to a crash. The main use case of Convict is for handling server-side configurations written by the admins owning the servers, and not random users. So it's unlikely that an admin would deliberately sabotage their own server. Still, a situation can happen where an admin not knowledgeable about JavaScript could be tricked by an attacker into writing the malicious JavaScript code into some config files. This issue affects Convict: before 6.2.4.	2024-11-26	8.4	CVE-2023-0163
Mozilla--Firefox	The executable file warning was not presented when downloading .library-ms files. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	9.8	CVE-2024-11693
Mozilla--Firefox	A flaw in handling fullscreen transitions may have inadvertently caused the application to become stuck in fullscreen mode when a modal dialog was opened during the transition. This issue left users unable to exit fullscreen mode using standard actions like pressing "Esc" or accessing right-click menus, resulting in a disrupted browsing experience until the browser is restarted. *This bug only affects the application when running on macOS. Other operating systems are unaffected.* This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	9.8	CVE-2024-11698
Mozilla--Firefox	A double-free issue could have occurred in `sec_pkcs7_decoder_start_decrypt()` when handling an error path. Under specific conditions, the same symmetric key could have been freed twice, potentially leading to memory corruption. This vulnerability affects Firefox < 133 and Thunderbird < 133.	2024-11-26	9.8	CVE-2024-11704
Mozilla--Firefox	`NSC_DeriveKey` inadvertently assumed that the `phKey` parameter is always non-NULL. When it was passed as NULL, a segmentation fault (SEGV) occurred, leading to crashes. This behavior conflicted with the PKCS#11 v3.0 specification, which	2024-11-26	9.1	CVE-2024-11705

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows `phKey` to be NULL for certain mechanisms. This vulnerability affects Firefox < 133 and Thunderbird < 133.			
Mozilla--Firefox	Certain WebGL operations on Apple silicon M series devices could have lead to an out-of-bounds write and memory corruption due to a flaw in Apple's GPU driver. *This bug only affected the application on Apple M series hardware. Other platforms were unaffected.* This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Firefox ESR < 115.18, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	8.8	CVE-2024-11691
Mozilla--Firefox	When handling keypress events, an attacker may have been able to trick a user into bypassing the "Open Executable File?" confirmation dialog. This could have led to malicious code execution. This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	8.8	CVE-2024-11697
Mozilla--Firefox	Memory safety bugs present in Firefox 132, Firefox ESR 128.4, and Thunderbird 128.4. 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 < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	8.8	CVE-2024-11699
Mozilla--Firefox	Malicious websites may have been able to user intent confirmation through tapjacking. This could have led to users unknowingly approving the launch of external applications, potentially exposing them to underlying vulnerabilities. This vulnerability affects Firefox < 133 and Thunderbird < 133.	2024-11-26	8.1	CVE-2024-11700
Mozilla--Firefox	Copying sensitive information from Private Browsing tabs on Android, such as passwords, may have inadvertently stored data in the cloud-based clipboard history if enabled. This vulnerability affects Firefox < 133 and Thunderbird < 133.	2024-11-26	7.5	CVE-2024-11702
Mozilla--sccache	On Linux the sccache client can execute arbitrary code with the privileges of a local sccache server, by preloading the code in a shared library passed to LD_PRELOAD. If the server is run as root (which is the default when installing the snap package https://snapcraft.io/sccache), this means a user running the sccache client can get root privileges.	2024-11-26	7.8	CVE-2023-1521
n/a--eNMS	A vulnerability, which was classified as critical, has been found in eNMS up to 4.2. Affected by this issue is the function multiselect_filtering of the file eNMS/controller.py of the component TGZ File Handler. The manipulation leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The patch is identified as 22b0b443acca740fc83b5544165c1f53eff3f529. It is recommended to apply a patch to fix this issue.	2024-11-25	8.8	CVE-2024-11664
n/a--n/a	A NoSQL injection vulnerability in Adapt Learning Adapt Authoring Tool <= 0.11.3 allows unauthenticated attackers to reset user and administrator account passwords via the "Reset password" feature. The vulnerability occurs due to insufficient validation of user input, which is used as a query in Mongoose's find() function. This makes it possible for attackers to perform a full takeover of the administrator account. Attackers can then use the newly gained administrative privileges to upload a custom plugin to perform remote code execution (RCE) on the server hosting the web application.	2024-11-25	9.8	CVE-2024-50672
n/a--n/a	DCME-320 <=7.4.12.90, DCME-520 <=9.25.5.11, DCME-320-L, <=9.3.5.26, and DCME-720 <=9.1.5.11 are vulnerable to Remote Code Execution via /function/system/basic/license_update.php.	2024-11-29	9.8	CVE-2024-52777
n/a--n/a	DCME-320 <=7.4.12.90, DCME-520 <=9.25.5.11, DCME-320-L <=9.3.5.26, and DCME-720 <=9.1.5.11 are vulnerable to Remote Code Execution via /function/audit/newstatistics/mon_stat_hist.php.	2024-11-29	9.8	CVE-2024-52778
n/a--n/a	DCME-320 <=7.4.12.90, DCME-520 <=9.25.5.11, DCME-320-L <=9.3.5.26, and DCME-720 <=9.1.5.11 are vulnerable to Remote Code Execution via /function/audit/newstatistics/mon_stat_top10.php.	2024-11-29	9.8	CVE-2024-52779
n/a--n/a	DCME-320 <=7.4.12.90, DCME-520 <=9.25.5.11, DCME-320-L <=9.3.5.26, and DCME-720 <=9.1.5.11 are vulnerable to Remote Code Execution via /function/system/basic/mgmt_edit.php.	2024-11-29	9.8	CVE-2024-52780
n/a--n/a	DCME-320 <=7.4.12.90, DCME-520 <=9.25.5.11, DCME-320-L <=9.3.5.26, and DCME-720 <=9.1.5.11 are vulnerable to Remote Code Execution via /function/system/tool/traceroute.php.	2024-11-29	9.8	CVE-2024-52781
n/a--n/a	DCME-320 <=7.4.12.90, DCME-520 <=9.25.5.11, DCME-320-L <=9.3.5.26, and DCME-720 <=9.1.5.11 are vulnerable to Remote Code Execution via /function/audit/newstatistics/mon_stat_hist_new.php.	2024-11-29	9.8	CVE-2024-52782
n/a--n/a	An issue in the upload_documents method of libre-chat v0.0.6 allows attackers to execute a path traversal via supplying a crafted filename in an uploaded file.	2024-11-25	9.1	CVE-2024-52787

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	A SQL Injection vulnerability was found in /covid-tms/check_availability.php in PHPGurukul COVID 19 Testing Management System v1.0, which allows remote attackers to execute arbitrary code via the mobnumber POST request parameter.	2024-11-27	9.8	CVE-2024-53604
n/a--n/a	EnGenius EWS356-FIR 1.1.30 and earlier devices allow a remote attacker to execute arbitrary OS commands via the Controller connectivity parameter.	2024-11-27	8	CVE-2024-31976
n/a--n/a	Stored Cross-Site Scripting in the Access Request History in Omada Identity before version 15 update 1 allows an authenticated attacker to execute arbitrary code in the browser of a victim via a specially crafted link or by viewing a manipulated Access Request History	2024-11-27	8	CVE-2024-52951
n/a--n/a	A Client-Side Template Injection (CSTI) vulnerability in the component /project/new/scrum of Taiga v 8.6.1 allows remote attackers to execute arbitrary code by injecting a malicious payload within the new project details.	2024-11-25	8	CVE-2024-53554
n/a--n/a	A CSV injection vulnerability in Taiga v6.8.1 allows attackers to execute arbitrary code via uploading a crafted CSV file.	2024-11-26	8.8	CVE-2024-53555
n/a--n/a	In Click Studios Passwordstate before build 9920, there is a potential permission escalation on the edit folder screen.	2024-11-29	8.8	CVE-2024-54124
n/a--n/a	An issue was discovered in Centreon centreon-dsm-server 24.10.x before 24.10.0, 24.04.x before 24.04.3, 23.10.x before 23.10.1, 23.04.x before 23.04.3, and 22.10.x before 22.10.2. SQL injection can occur in the form to configure Centreon DSM slots. Exploitation is only accessible to authenticated users with high-privileged access.	2024-11-25	7.2	CVE-2024-45755
n/a--n/a	An issue was discovered in Centreon centreon-open-tickets 24.10.x before 24.10.0, 24.04.x before 24.04.2, 23.10.x before 23.10.1, 23.04.x before 23.04.3, and 22.10.x before 22.10.2. SQL injection can occur in the form to create a ticket. Exploitation is only accessible to authenticated users with high-privileged access.	2024-11-25	7.2	CVE-2024-45756
n/a--n/a	In ProFTPD through 1.3.8b before cec01cc, supplemental group inheritance grants unintended access to GID 0 because of the lack of supplemental groups from mod_sql.	2024-11-29	7.5	CVE-2024-48651
n/a--n/a	A SQL Injection vulnerability was found in /covid-tms/password-recovery.php in PHPGurukul COVID 19 Testing Management System v1.0, which allows remote attackers to execute arbitrary code via the contactno POST request parameter.	2024-11-27	7.3	CVE-2024-53603
n/a--n/a	In OpenStack Neutron through 25.0.0, neutron/extensions/tagging.py can use an incorrect ID during policy enforcement. NOTE: 935883 has the "Work in Progress" status as of 2024-11-24.	2024-11-25	7.5	CVE-2024-53916
NEC Corporation--UNIVERGE IX	Command Injection vulnerability in NEC Corporation UNIVERGE IX from Ver9.2 to Ver10.10.21, for Ver10.8 up to Ver10.8.27, for Ver10.9 up to Ver10.9.14 and UNIVERGE IX-R/IX-V Ver1.2.15 and earlier allows a attacker to inject an arbitrary CLI commands to be executed on the device via the management interface.	2024-11-29	7.2	CVE-2024-11013
ngtcp2--ngtcp2	The ngtcp2 project is an effort to implement IETF QUIC protocol in C. In affected versions acks are not validated before being written to the qlog leading to a buffer overflow. In `ngtcp2_conn::conn_recv_pkt` for an ACK, there was new logic that got added to skip `conn_recv_ack` if an ack has already been processed in the payload. However, this causes us to also skip `ngtcp2_pkt_validate_ack`. The ack which was skipped still got written to qlog. The bug occurs in `ngtcp2_qlog::write_ack_frame`. It is now possible to reach this code with an invalid ack, suppose `largest_ack=0` and `first_ack_range=15`. Subtracting `largest_ack - first_ack_range` will lead to an integer underflow which is 20 chars long. However, the ngtcp2 qlog code assumes the number written is a signed integer and only accounts for 19 characters of overhead (see `NGTCP2_QLOG_ACK_FRAME_RANGE_OVERHEAD`). Therefore, we overwrite the buffer causing a heap overflow. This is high priority and could potentially impact many users if they enable qlog. qlog is disabled by default. Due to its overhead, it is most likely used for debugging purpose, but the actual use is unknown. ngtcp2 v1.9.1 fixes the bug and users are advised to upgrade. Users unable to upgrade should not turn on qlog.	2024-11-25	8.2	CVE-2024-52811
ninjateam--File Manager Pro Filester	The File Manager Pro - Filester plugin for WordPress is vulnerable to arbitrary file uploads due to missing validation in the 'fsConnector' function in all versions up to, and including, 1.8.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, and granted permissions by an Administrator, to upload a new .htaccess file allowing them to subsequently upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-11-28	7.5	CVE-2024-8066
ninjateam--File Manager Pro Filester	The File Manager Pro - Filester plugin for WordPress is vulnerable to Local JavaScript File Inclusion in all versions up to, and including, 1.8.5 via the 'fm_locale' parameter. This makes it possible for authenticated attackers, with Administrator-level access and above, to include and execute arbitrary files on the server,	2024-11-28	7.2	CVE-2024-9669

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included. The vulnerability was partially patched in version 1.8.5.			
Pathomation--Pathomation	Unrestricted Upload of File with Dangerous Type vulnerability in Pathomation allows Upload a Web Shell to a Web Server.This issue affects Pathomation: from n/a through 2.5.1.	2024-11-28	10	CVE-2024-52490
PHPGurukul--Complaint Management system	A vulnerability, which was classified as critical, was found in PHPGurukul Complaint Management system 1.0. This affects an unknown part of the file /user/index.php. The manipulation of the argument emailid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-28	7.3	CVE-2024-11964
PHPGurukul--Complaint Management system	A vulnerability has been found in PHPGurukul Complaint Management system 1.0 and classified as critical. This vulnerability affects unknown code of the file /user/reset-password.php. The manipulation of the argument email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-28	7.3	CVE-2024-11965
PHPGurukul--Complaint Management system	A vulnerability was found in PHPGurukul Complaint Management system 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/index.php. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-28	7.3	CVE-2024-11966
PHPGurukul--Complaint Management system	A vulnerability was found in PHPGurukul Complaint Management system 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/reset-password.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-28	7.3	CVE-2024-11967
PHPGurukul--User Registration & Login and User Management System	A vulnerability was found in PHPGurukul User Registration & Login and User Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/index.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.	2024-11-26	7.3	CVE-2024-11817
PHPGurukul--User Registration & Login and User Management System	A vulnerability classified as critical has been found in PHPGurukul User Registration & Login and User Management System 1.0. This affects an unknown part of the file /signup.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.	2024-11-27	7.3	CVE-2024-11818
Prism I.T. Systems--Multilevel Referral Affiliate Plugin for WooCommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Prism I.T. Systems Multilevel Referral Affiliate Plugin for WooCommerce allows Reflected XSS.This issue affects Multilevel Referral Affiliate Plugin for WooCommerce: from n/a through 2.27.	2024-12-01	7.1	CVE-2024-53742
ProjectSend--ProjectSend	ProjectSend versions prior to r1720 are affected by an improper authentication vulnerability. Remote, unauthenticated attackers can exploit this flaw by sending crafted HTTP requests to options.php, enabling unauthorized modification of the application's configuration. Successful exploitation allows attackers to create accounts, upload webshells, and embed malicious JavaScript.	2024-11-26	9.8	CVE-2024-11680
python-jsonschema--check-jsonschema	check-jsonschema is a CLI and set of pre-commit hooks for jsonschema validation. The default cache strategy uses the basename of a remote schema as the name of the file in the cache, e.g. `https://example.org/schema.json` will be stored as `schema.json`. This naming allows for conflicts. If an attacker can get a user to run `check-jsonschema` against a malicious schema URL, e.g., `https://example.evil.org/schema.json`, they can insert their own schema into the cache and it will be picked up and used instead of the appropriate schema. Such a cache confusion attack could be used to allow data to pass validation which should have been rejected. This issue has been patched in version 0.30.0. All users are advised to upgrade. A few workarounds exist: 1. Users can use `--no-cache` to disable caching. 2. Users can use `--cache-filename` to select filenames for use in the cache, or to ensure that other usages do not overwrite the cached schema. (Note: this flag is being deprecated as part of the remediation effort.) 3. Users can explicitly download the schema before use as a local file, as in `curl -LOs https://example.org/schema.json; check-jsonschema --schemafile ./schema.json`	2024-11-29	7.1	CVE-2024-53848

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Qualcomm, Inc.--Snapdragon	On some hardware revisions where VP9 decoding is hardware-accelerated, the frame size is not programmed correctly into the decoder hardware which can lead to an invalid memory access by the decoder.	2024-11-26	9.8	CVE-2017-11076
Qualcomm, Inc.--Snapdragon	In multiple functions that process 802.11 frames, out-of-bounds reads can occur due to insufficient validation.	2024-11-26	9.8	CVE-2017-17772
Qualcomm, Inc.--Snapdragon	Wrong configuration in Touch Pal application can collect user behavior data without awareness by the user.	2024-11-26	9.8	CVE-2018-11922
Qualcomm, Inc.--Snapdragon	Initial xbl_sec revision does not have all the debug policy features and critical checks.	2024-11-26	8.4	CVE-2016-10394
Qualcomm, Inc.--Snapdragon	QSEE will randomly experience a fatal error during execution due to speculative instruction fetches from device memory. Device memory is not valid executable memory.	2024-11-26	8.4	CVE-2016-10408
Qualcomm, Inc.--Snapdragon	Buffer overwrite in the WLAN host driver by leveraging a compromised WLAN FW	2024-11-26	8.4	CVE-2017-15832
Qualcomm, Inc.--Snapdragon	A race condition exists in a driver potentially leading to a use-after-free condition.	2024-11-26	8.4	CVE-2017-18153
Qualcomm, Inc.--Snapdragon	Information disclosure due to uninitialized variable.	2024-11-26	8.4	CVE-2017-18306
Qualcomm, Inc.--Snapdragon	Information disclosure possible while audio playback.	2024-11-26	8.4	CVE-2017-18307
Qualcomm, Inc.--Snapdragon	An image with a version lower than the fuse version may potentially be booted lead to improper authentication.	2024-11-26	8.4	CVE-2018-11952
Qualcomm, Inc.--Snapdragon	An unsigned integer underflow vulnerability in IPA driver result into a buffer over-read while reading NAT entry using debugfs command 'cat /sys/kernel/debug/ipa/ip4_nat'	2024-11-26	8.4	CVE-2018-5852
Qualcomm, Inc.--Snapdragon	Crafted Binder Request Causes Heap UAF in MediaServer	2024-11-26	7.8	CVE-2018-11816
Quick.CMS--Quick.CMS	Absolute path traversal vulnerability in Quick.CMS, version 6.7, the exploitation of which could allow remote users to bypass the intended restrictions and download any file if it has the appropriate permissions outside of documentroot configured on the server via the aDirFiles%5B0%5D parameter in the admin.php page. This vulnerability allows an attacker to delete files stored on the server due to a lack of proper verification of user-supplied input.	2024-11-29	9.1	CVE-2024-11992
quomodosoft--Shopready	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in quomodosoft Shopready allows PHP Local File Inclusion.This issue affects Shopready: from n/a through 3.5.	2024-11-28	7.5	CVE-2024-52497
Rank Math SEO--Rank Math SEO	Improper Control of Generation of Code ('Code Injection') vulnerability in Rank Math SEO allows Code Injection.This issue affects Rank Math SEO: from n/a through 1.0.231.	2024-11-28	7.2	CVE-2024-11620
Red Hat--Red Hat Enterprise Linux 8	A vulnerability was found in CRI-O, where it can be requested to take a checkpoint archive of a container and later be asked to restore it. When it does that restoration, it attempts to restore the mounts from the restore archive instead of the pod request. As a result, the validations run on the pod spec, verifying that the pod has access to the mounts it specifies are not applicable to a restored container. This flaw allows a malicious user to trick CRI-O into restoring a pod that doesn't have access to host mounts. The user needs access to the kubelet or cri-o socket to call the restore endpoint and trigger the restore.	2024-11-26	7.4	CVE-2024-8676
Red Hat--Red Hat Enterprise Linux 9	A script injection vulnerability was identified in the Tuned package. The `instance_create()` D-Bus function can be called by locally logged-in users without authentication. This flaw allows a local non-privileged user to execute a D-Bus call with `script_pre` or `script_post` options that permit arbitrary scripts with their absolute paths to be passed. These user or attacker-controlled executable scripts or programs could then be executed by Tuned with root privileges that could allow attackers to local privilege escalation.	2024-11-26	7.8	CVE-2024-52336

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Rohit Harsh--Fence URL	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rohit Harsh Fence URL allows Stored XSS.This issue affects Fence URL: from n/a through 2.0.0.	2024-11-28	7.1	CVE-2024-53733
sandboxie-plus--Sandboxie	Sandboxie is a sandbox-based isolation software for 32-bit and 64-bit Windows NT-based operating systems. An authenticated user (**UserA**) with no privileges is authorized to read all files created in sandbox belonging to other users in the sandbox folders `C:\Sandbox\UserB\xxx`. An authenticated attacker who can use `explorer.exe` or `cmd.exe` outside any sandbox can read other users' files in `C:\Sandbox\xxx`. By default in Windows 7+, the `C:\Users\UserA` folder is not readable by **UserB**. All files edited or created during the sandbox processing are affected by the vulnerability. All files in C:\Users are safe. If `UserB` runs a cmd in a sandbox, he will be able to access `C:\Sandox\UserA`. In addition, if **UserB** create a folder `C:\Sandbox\UserA` with malicious ACLs, when **UserA** will user the sandbox, Sandboxie doesn't reset ACLs ! This issue has not yet been fixed. Users are advised to limit access to their systems using Sandboxie.	2024-11-29	9.2	CVE-2024-49360
scottopolis--AppPresser Mobile App Framework	The AppPresser - Mobile App Framework plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 4.4.6. This is due to the plugin not properly validating a user's password reset code prior to updating their password. This makes it possible for unauthenticated attackers, with knowledge of a user's email address, to reset the user's password and gain access to their account.	2024-11-26	9.8	CVE-2024-11024
Sensei--Sensei Mac Cleaner	The application Sensei Mac Cleaner contains a local privilege escalation vulnerability, allowing an attacker to perform multiple operations as the root user. These operations include arbitrary file deletion and writing, loading and unloading daemons, manipulating file permissions, and loading extensions, among other actions. The vulnerable module org.cindori.SenseiHelper can be contacted via XPC. While the module performs client validation, it relies on the client's PID obtained through the public processIdentifier property of the NSXPCConnection class. This approach makes the module susceptible to a PID Reuse Attack, enabling an attacker to impersonate a legitimate client and send crafted XPC messages to invoke arbitrary methods exposed by the HelperProtocol interface.	2024-11-25	7.8	CVE-2024-7915
Sharp Corporation--Multiple MFPs (multifunction printers)	The web interface of the affected devices processes a cookie value improperly, leading to a stack buffer overflow. More precisely, giving too long character string to MFPSESSIONID parameter results in a stack buffer overflow. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	2024-11-26	9	CVE-2024-28038
Sharp Corporation--Multiple MFPs (multifunction printers)	"sessionlist.html" and "sys_trayentryreboot.html" are accessible with no authentication. "sessionlist.html" provides logged-in users' session information including session cookies, and "sys_trayentryreboot.html" allows to reboot the device. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	2024-11-26	9.1	CVE-2024-33610
Sharp Corporation--Multiple MFPs (multifunction printers)	There are several hidden accounts. Some of them are intended for maintenance engineers, and with the knowledge of their passwords (e.g., by examining the coredump), these accounts can be used to re-configure the device. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	2024-11-26	9.1	CVE-2024-35244
Sharp Corporation--Multiple MFPs (multifunction printers)	API keys for some cloud services are hardcoded in the "main" binary. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	2024-11-26	9.1	CVE-2024-36248
Sharp Corporation--Multiple MFPs (multifunction printers)	Improper processing of some parameters of installed_emanual_list.html leads to a path traversal vulnerability. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	2024-11-26	7.5	CVE-2024-33605
Sharp Corporation--Multiple MFPs (multifunction printers)	Cross-site scripting vulnerability exists in Sharp Corporation and Toshiba Tech Corporation multiple MFPs (multifunction printers). If this vulnerability is exploited, an arbitrary script may be executed on the administrative page of the affected MFPs. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	2024-11-26	7.4	CVE-2024-36249
Sharp Corporation--Multiple MFPs	The web interface of the affected devices process some crafted HTTP requests improperly, leading to a device crash. More precisely, a crafted parameter to	2024-11-26	7.5	CVE-2024-36251

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
(multifunction printers)	billcodedef_sub_sel.html is not processed properly and device-crash happens. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].			
Sharp Corporation--Multiple MFPs (multifunction printers)	Out-of-bounds read vulnerability exists in Sharp Corporation and Toshiba Tec Corporation multiple MFPs (multifunction printers), which may lead to a denial-of-service (DoS) condition.	2024-11-26	7.5	CVE-2024-36254
Softpulse Infotech--SP Blog Designer	Path Traversal: '.../...//' vulnerability in Softpulse Infotech SP Blog Designer allows PHP Local File Inclusion.This issue affects SP Blog Designer: from n/a through 1.0.0.	2024-11-28	7.5	CVE-2024-52498
Spencer14420--SPEmailHandler-PHP	sp-php-email-handler is a PHP package for handling contact form submissions. Messages sent using this script are vulnerable to abuse, as the script allows anybody to specify arbitrary email recipients and include user-provided content in confirmation emails. This could enable malicious actors to use your server to send spam, phishing emails, or other malicious content, potentially damaging your domain's reputation and leading to blacklisting by email providers. Patched in version 1.0.0 by removing user-provided content from confirmation emails. All pre-release versions (alpha and beta) are vulnerable to this issue and should not be used. There are no workarounds for this issue. Users must upgrade to version 1.0.0 to mitigate the vulnerability.	2024-11-27	8.6	CVE-2024-53860
SUSE--openSUSE Factory	Various problems in obs-scm-bridge allows attackers that create specially crafted git repositories to leak information of cause denial of service.	2024-11-28	7.3	CVE-2024-22038
Tenda--AC8	A vulnerability was found in Tenda AC8 16.03.34.09 and classified as critical. Affected by this issue is the function route_static_check of the file /goform/SetStaticRouteCfg. The manipulation of the argument list leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-26	8.8	CVE-2024-11745
Trellix--Trellix Enterprise Security Manager (ESM)	A vulnerability in ESM 11.6.10 allows unauthenticated access to the internal Snowservice API and enables remote code execution through command injection, executed as the root user.	2024-11-29	9.8	CVE-2024-11482
Trellix--Trellix Enterprise Security Manager (ESM)	A vulnerability in ESM 11.6.10 allows unauthenticated access to the internal Snowservice API. This leads to improper handling of path traversal, insecure forwarding to an AJP backend without adequate validation, and lack of authentication for accessing internal API endpoints.	2024-11-29	8.2	CVE-2024-11481
tumultinc--Tumult Hype Animations	The Tumult Hype Animations plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the hypeanimations_panel() function in all versions up to, and including, 1.9.15. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-11-28	9.9	CVE-2024-11082
Tyche Softwares--Booking & Appointment Plugin for WooCommerce	The Booking & Appointment Plugin for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'save_google_calendar_data' function in versions up to, and including, 6.9.0. This makes it possible for authenticated attackers, with subscriber-level permissions or above to update the site options arbitrarily.	2024-11-26	8.8	CVE-2024-10729
Universal Audio--UAConnect	The com.uaudio.bsd.helper service, responsible for handling privileged operations, fails to implement critical client validation during XPC inter-process communication (IPC). Specifically, the service does not verify the code requirements, entitlements, or security flags of any client attempting to establish a connection. This lack of proper validation allows unauthorized clients to exploit the service's methods and escalate privileges to root.	2024-11-25	7.8	CVE-2024-8272
Valor Apps--Easy Folder Listing Pro	Valor Apps Easy Folder Listing Pro has a deserialization vulnerability that allows an unauthenticated, remote attacker to execute arbitrary code with the privileges of the Joomla! application. Fixed in versions 3.8 and 4.5.	2024-11-26	9.8	CVE-2024-11145
VMware--VMware Aria Operations	VMware Aria Operations contains a local privilege escalation vulnerability. A malicious actor with local administrative privileges may trigger this vulnerability to escalate privileges to root user on the appliance running VMware Aria Operations.	2024-11-26	7.8	CVE-2024-38830
VMware--VMware Aria Operations	VMware Aria Operations contains a local privilege escalation vulnerability. A malicious actor with local administrative privileges can insert malicious commands into the properties file to escalate privileges to a root user on the appliance running VMware Aria Operations.	2024-11-26	7.8	CVE-2024-38831

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
VMware--VMware Aria Operations	VMware Aria Operations contains a stored cross-site scripting vulnerability. A malicious actor with editing access to views may be able to inject malicious script leading to stored cross-site scripting in the product VMware Aria Operations.	2024-11-26	7.1	CVE-2024-38832
webbytemplate--Office Locator	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in webbytemplate Office Locator.This issue affects Office Locator: from n/a through 1.3.0.	2024-11-28	7.5	CVE-2024-52501
WP WOX--Footer Flyout Widget	Cross-Site Request Forgery (CSRF) vulnerability in WP WOX Footer Flyout Widget allows Stored XSS.This issue affects Footer Flyout Widget: from n/a through 1.1.	2024-11-28	7.1	CVE-2024-53732
WP-speedup--Block Editor Bootstrap Blocks	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP-speedup Block Editor Bootstrap Blocks allows Reflected XSS.This issue affects Block Editor Bootstrap Blocks: from n/a through 6.6.1.	2024-11-28	7.1	CVE-2024-11402
wpdevart--Booking calendar, Appointment Booking System	The Booking calendar, Appointment Booking System plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 3.2.15 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 the SVG file.	2024-11-26	7.2	CVE-2024-9504
Zabbix--Zabbix	A non-admin user account on the Zabbix frontend with the default User role, or with any other role that gives API access can exploit this vulnerability. An SQLi exists in the CUser class in the addRelatedObjects function, this function is being called from the CUser.get function which is available for every user who has API access.	2024-11-27	9.9	CVE-2024-42327
Zabbix--Zabbix	The HttpRequest object allows to get the HTTP headers from the server's response after sending the request. The problem is that the returned strings are created directly from the data returned by the server and are not correctly encoded for JavaScript. This allows to create internal strings that can be used to access hidden properties of objects.	2024-11-27	9.1	CVE-2024-42330
Zabbix--Zabbix	A bug in the code allows an attacker to sign a forged zbx_session cookie, which then allows them to sign in with admin permissions.	2024-11-28	8.8	CVE-2024-36466
Zabbix--Zabbix	An authenticated user with API access (e.g.: user with default User role), more specifically a user with access to the user.update API endpoint is enough to be able to add themselves to any group (e.g.: Zabbix Administrators), except to groups that are disabled or having restricted GUI access.	2024-11-27	7.5	CVE-2024-36467
zhmcclient--python-zhmcclient	zhmcclient is a pure Python client library for the IBM Z HMC Web Services API. In affected versions the Python package "zhmcclient" writes password-like properties in clear text into its HMC and API logs in the following cases: 1. The 'boot-ftp-password' and 'ssc-master-pw' properties when creating or updating a partition in DPM mode, in the zhmcclient API and HMC logs. 2. The 'ssc-master-pw' and 'zaware-master-pw' properties when updating an LPAR in classic mode, in the zhmcclient API and HMC logs. 3. The 'ssc-master-pw' and 'zaware-master-pw' properties when creating or updating an image activation profile in classic mode, in the zhmcclient API and HMC logs. 4. The 'password' property when creating or updating an HMC user, in the zhmcclient API log. 5. The 'bind-password' property when creating or updating an LDAP server definition, in the zhmcclient API and HMC logs. This issue affects only users of the zhmcclient package that have enabled the Python loggers named "zhmcclient.api" (for the API log) or "zhmcclient.hmc" (for the HMC log) and that use the functions listed above. This issue has been fixed in zhmcclient version 1.18.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-11-29	8.2	CVE-2024-53865
zhmcclient--zhmc-ansible-modules	ibm.ibm_zhmc is an Ansible collection for the IBM Z HMC. The Ansible collection "ibm.ibm_zhmc" writes password-like properties in clear text into its log file and into the output returned by some of its Ansible module in the following cases: 1. The 'boot_ftp_password' and 'ssc_master_pw' properties are passed as input to the zhmc_partition Ansible module. 2. The 'ssc_master_pw' and 'zaware_master_pw' properties are passed as input to the zhmc_lpar Ansible module. 3. The 'password' property is passed as input to the zhmc_user Ansible module (just in log file, not in module output). 4. The 'bind_password' property is passed as input to the zhmc_ldap_server_definition Ansible module. These properties appear in the module output only when they were specified in the module input and when creating or updating the corresponding resources. They do not appear in the output when retrieving facts for the corresponding resources. These properties appear in the log file only when the "log_file" module input parameter is used. By default, no log file is created. This issue has been fixed in	2024-11-29	8.2	CVE-2024-53979

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ibm.ibm_zhmc version 1.9.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.			
Zyxel--ATP series firmware	A directory traversal vulnerability in the web management interface of Zyxel ATP series firmware versions V5.00 through V5.38, USG FLEX series firmware versions V5.00 through V5.38, USG FLEX 50(W) series firmware versions V5.10 through V5.38, and USG20(W)-VPN series firmware versions V5.10 through V5.38 could allow an attacker to download or upload files via a crafted URL.	2024-11-27	7.5	CVE-2024-11667
1000projects -- bookstore_management_system	A vulnerability, which was classified as critical, has been found in 1000 Projects Bookstore Management System 1.0. Affected by this issue is some unknown functionality of the file /forget_password_process.php. The manipulation of the argument unm leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-21	9.8	CVE-2024-11590
angeljudesuarez -- tailoring_management_system	A vulnerability was found in itsourcecode Tailoring Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /expedit.php. The manipulation of the argument expcat leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-23	9.8	CVE-2024-11631
angeljudesuarez -- tailoring_management_system	A vulnerability classified as critical was found in itsourcecode Tailoring Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /expcatedit.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.	2024-11-21	8.8	CVE-2024-11589
antonhoelstad -- wp_quick_setup	Unrestricted Upload of File with Dangerous Type vulnerability in Anton Hoelstad WP Quick Setup allows Upload a Web Shell to a Web Server.This issue affects WP Quick Setup: from n/a through 2.0.	2024-11-18	8.8	CVE-2024-52429
arm -- mbed	An issue was discovered in MBed OS 6.16.0. During processing of HCI packets, the software dynamically determines the length of the packet header by looking up the identifying first byte and matching it against a table of possible lengths. The initial parsing function, hciTrSerialRxIncoming does not drop packets with invalid identifiers but also does not set a safe default for the length of unknown packets' headers, leading to a buffer overflow. This can be leveraged into an arbitrary write by an attacker. It is possible to overwrite the pointer to a not-yet-allocated buffer that is supposed to receive the contents of the packet body. One can then overwrite the state variable used by the function to determine which state of packet parsing is currently occurring. Because the buffer is allocated when the last byte of the header has been copied, the combination of having a bad header length variable that will never match the counter variable and being able to overwrite the state variable with the resulting buffer overflow can be used to advance the function to the next step while skipping the buffer allocation and resulting pointer write. The next 16 bytes from the packet body are then written wherever the corrupted data pointer is pointing.	2024-11-20	7.5	CVE-2024-48981
arm -- mbed	An issue was discovered in MBed OS 6.16.0. Its hci parsing software dynamically determines the length of certain hci packets by reading a byte from its header. This value is assumed to be greater than or equal to 3, but the software doesn't ensure that this is the case. Supplying a length less than 3 leads to a buffer overflow in a buffer that is allocated later. It is simultaneously possible to cause another integer overflow by supplying large length values because the provided length value is increased by a few bytes to account for additional information that is supposed to be stored there. This bug is trivial to exploit for a denial of service but is not certain to suffice to bring the system down and can generally not be exploited further because the exploitable buffer is dynamically allocated.	2024-11-20	7.5	CVE-2024-48982
arm -- mbed	An issue was discovered in MBed OS 6.16.0. During processing of HCI packets, the software dynamically determines the length of the packet data by reading 2 bytes from the packet header. A buffer is then allocated to contain the entire packet, the size of which is calculated as the length of the packet body determined earlier plus the header length. WsfMsgAlloc then increments this again by sizeof(wsfMsg_t). This may cause an integer overflow that results in the buffer being significantly too small to contain the entire packet. This may cause a buffer overflow of up to 65 KB . This bug is trivial to exploit for a denial of service but can generally not be exploited further because the exploitable buffer is dynamically allocated.	2024-11-20	7.5	CVE-2024-48983
arm -- mbed	An issue was discovered in MBed OS 6.16.0. During processing of HCI packets, the software dynamically determines the length of the packet data by reading 2 bytes from the packet data. A buffer is then allocated to contain the entire packet, the size of which is calculated as the length of the packet body determined earlier and the header length. If the allocate fails because the specified packet is too large, no	2024-11-20	7.5	CVE-2024-48985

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exception handling occurs and hciTrSerialRxIncoming continues to write bytes into the 4-byte large temporary header buffer, leading to a buffer overflow. This can be leveraged into an arbitrary write by an attacker. It is possible to overwrite the pointer to the buffer that is supposed to receive the contents of the packet body but which couldn't be allocated. One can then overwrite the state variable used by the function to determine which step of the parsing process is currently being executed. This advances the function to the next state, where it proceeds to copy data to that arbitrary location. The packet body is then written wherever the corrupted data pointer is pointing.			
arm -- mbed	An issue was discovered in MBed OS 6.16.0. Its hci parsing software dynamically determines the length of certain hci packets by reading a byte from its header. Certain events cause a callback, the logic for which allocates a buffer (the length of which is determined by looking up the event type in a table). The subsequent write operation, however, copies the amount of data specified in the packet header, which may lead to a buffer overflow. This bug is trivial to exploit for a denial of service but is not certain to suffice to bring the system down and can generally not be exploited further because the exploitable buffer is dynamically allocated.	2024-11-20	7.5	CVE-2024-48986
avlditest -- libdoip	A vulnerability was found in AVL-DiTEST-DiagDev libdoip 1.0.0. It has been rated as problematic. This issue affects the function DoIPConnection::reactOnReceivedTcpMessage of the file DoIPConnection.cpp. The manipulation leads to null pointer dereference.	2024-11-21	7.5	CVE-2024-11588
cesanta -- mongoose	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows to write a NULL byte value beyond the memory space dedicated for the hostname field.	2024-11-18	9.8	CVE-2024-42383
cesanta -- mongoose	Integer Overflow or Wraparound vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and produce a segmentation fault on the application.	2024-11-18	7.5	CVE-2024-42384
cesanta -- mongoose	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and produce a segmentation fault on the application.	2024-11-18	7.5	CVE-2024-42386
cesanta -- mongoose	Improper Neutralization of Delimiters vulnerability in Cesanta Mongoose Web Server v7.14 allows to trigger an infinite loop bug if the input string contains unexpected characters.	2024-11-18	7.5	CVE-2024-42392
cesanta -- mongoose	Improper Neutralization of Delimiters vulnerability in Cesanta Mongoose Web Server v7.14 allows to trigger an out-of-bound memory write if the PEM certificate contains unexpected characters.	2024-11-18	7	CVE-2024-42385
cisco--cisco	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to create or overwrite arbitrary files on an affected device, which could result in a denial of service (DoS) condition. The vulnerability is due to insufficient input validation for specific commands. An attacker could exploit this vulnerability by including crafted arguments to those specific commands. A successful exploit could allow the attacker to create or overwrite arbitrary files on the affected device, which could result in a DoS condition.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-18	8.4	CVE-2020-26071
code4berry -- decoration_management_system	A vulnerability classified as critical was found in Code4Berry Decoration Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /decoration/admin/update_image.php of the component User Image Handler. The manipulation of the argument productimage1 leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-20	8.8	CVE-2024-11484
code4berry -- decoration_management_system	A vulnerability has been found in Code4Berry Decoration Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /decoration/admin/btndates_report.php of the component Between Dates Reports. The manipulation of the argument fromdate/todate leads to sql 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.	2024-11-20	8.8	CVE-2024-11487
code4berry -- decoration_management_system	A vulnerability, which was classified as critical, has been found in Code4Berry Decoration Management System 1.0. Affected by this issue is some unknown functionality of the file /decoration/admin/userregister.php of the component User Handler. The manipulation leads to permission issues. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-20	8.1	CVE-2024-11485

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The vendor was contacted early about this disclosure but did not respond in any way.			
codesys--codesys	A low privileged remote attacker may modify the configuration of the CODESYS V3 service through a missing authentication vulnerability which could lead to full system access and/or DoS.	2024-11-18	8.8	CVE-2024-41969
dlink -- di-8003_firmware	D-LINK DI-8003 v16.07.26A1 was discovered to contain a buffer overflow via the ip parameter in the ip_position_asp function.	2024-11-19	9.8	CVE-2024-52759
dlink -- di-8200_firmware	D-Link DI-8200 16.07.26A1 is vulnerable to remote command execution in the msp_info_htm function via the flag parameter and cmd parameter.	2024-11-21	9.8	CVE-2024-51151
fabianros -- simple_car_rental_system	A vulnerability was found in code-projects Simple Car Rental System 1.0. It has been classified as critical. Affected is an unknown function of the file /book_car.php. The manipulation of the argument fname/id_no/gender/email/phone/location 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 "fname" to be affected. Further analysis indicates that other arguments might be affected as well.	2024-11-23	9.8	CVE-2024-11632
google -- android	In the getHost() function of UriTest.java, there is the possibility of incorrect web origin determination. This could lead to incorrect security decisions with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-20	9.8	CVE-2018-9467
google -- android	In decrypt of ClearKeyCasPlugin.cpp there is a possible out-of-bounds write due to a missing bounds check. This could lead to remote arbitrary code execution with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-19	8.8	CVE-2018-9411
google -- android	In ArrayConcatVisitor of builtins-array.cc, there is a possible type confusion due to improper input validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-19	8.8	CVE-2018-9433
google -- android	In the xmlSnprintfElementContent function of valid.c, there is a possible out of bounds write. This could lead to remote escalation of privilege in an unprivileged app with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-19	8.8	CVE-2018-9466
google -- android	In ResStringPool::setTo of ResourceTypes.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	7.8	CVE-2018-9338
google -- android	In writeTypedArrayList and readTypedArrayList of Parcel.java, there is a possible escalation of privilege due to type confusion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	7.8	CVE-2018-9339
google -- android	In impeg2d_mc_fullx_fully of impeg2d_mc.c there is a possible out of bound write due to missing bounds check. This could lead to remote arbitrary code execution with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-19	7.8	CVE-2018-9341
google -- android	In several functions of DescramblerImpl.cpp, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	7.8	CVE-2018-9344
google -- android	In IMSA_Recv_Thread and VT_IMCB_Thread of ImsaClient.cpp and VideoTelephony.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	7.8	CVE-2018-9366
google -- android	In FT_ACDK_CCT_V2_OP_ISP_SET_TUNING_PARAS of Meta_CCAP_Para.cpp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	7.8	CVE-2018-9367
google -- android	In mtkscoaudio debugfs there is a possible arbitrary kernel memory write due to missing bounds check and weakened SELinux policies. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	7.8	CVE-2018-9368
google -- android	In f_hidg_read and hidg_disable of f_hid.c, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	7.8	CVE-2018-9417

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In CryptoPlugin::decrypt of CryptoPlugin.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	7.8	CVE-2018-9424
google -- android	In startDevice of AAudioServiceStreamBase.cpp there is a possible out of bounds write due to a use after free. This could lead to local arbitrary code execution with no additional execution privileges needed. User interaction is needed for exploitation. https://source.android.com/security/bulletin/2018-07-01	2024-11-19	7.8	CVE-2018-9428
google -- android	In createPhonebookDialogView and createMapDialogView of BluetoothPermissionActivity.java, there is a possible permissions bypass. This could lead to local escalation of privilege due to hiding and bypassing the user's ability to disable access to contacts, with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-19	7.8	CVE-2018-9432
google -- android	In the LG LAF component, there is a special command that allowed modification of certain partitions. This could lead to bypass of secure boot. User interaction is not needed for exploitation.	2024-11-19	7.5	CVE-2018-9364
google -- android	In l2cble_process_sig_cmd of l2c_ble.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	7.5	CVE-2018-9419
google -- android	In sdpu_extract_attr_seq of sdp_utils.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	7.5	CVE-2018-9456
google -- android	In bootloader there is fastboot command allowing user specified kernel command line arguments. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-19	7.3	CVE-2018-9369
google -- android	In download.c there is a special mode allowing user to download data into memory and causing possible memory corruptions due to missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-19	7.3	CVE-2018-9370
h3c -- gr-1800ax_firmware	H3C GR-1800AX MiniGRW1B0V100R007 is vulnerable to remote code execution (RCE) via the aspForm parameter.	2024-11-20	9.8	CVE-2024-52765
hkcms -- hkcms	HkCms <= v2.3.2.240702 is vulnerable to file upload in the getFileName method in /app/common/library/Upload.php.	2024-11-20	9.8	CVE-2024-52677
IBM--Concert Software	IBM Concert Software 1.0.0, 1.0.1, 1.0.2, and 1.0.2.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify, or delete information in the back-end database.	2024-11-19	7.6	CVE-2024-52360
ibm--ibm	IBM Engineering Systems Design Rhapsody - Model Manager 7.0.2 and 7.0.3 could allow a remote attacker to bypass security restrictions, caused by a race condition. By sending a specially crafted request, an attacker could exploit this vulnerability to remotely execute code.	2024-11-22	9.8	CVE-2024-41779
irfanview -- irfanview	IrfanView ECW File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of ECW files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-23971.	2024-11-22	7.8	CVE-2024-11513
irfanview -- irfanview	IrfanView ECW File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of ECW files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-23975.	2024-11-22	7.8	CVE-2024-11514
irfanview -- irfanview	IrfanView JPM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPM files. The issue results from the	2024-11-22	7.8	CVE-2024-11515

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24010.			
irfanview -- irfanview	IrfanView JPM File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPM files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24011.	2024-11-22	7.8	CVE-2024-11516
irfanview -- irfanview	IrfanView JPM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPM files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24118.	2024-11-22	7.8	CVE-2024-11517
irfanview -- irfanview	IrfanView RLE File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of RLE files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24444.	2024-11-22	7.8	CVE-2024-11518
irfanview -- irfanview	IrfanView RLE File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of RLE files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24445.	2024-11-22	7.8	CVE-2024-11519
irfanview -- irfanview	IrfanView ARW File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of ARW files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24488.	2024-11-22	7.8	CVE-2024-11520
irfanview -- irfanview	IrfanView DJVU File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DJVU files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24578.	2024-11-22	7.8	CVE-2024-11521
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24595.	2024-11-22	7.8	CVE-2024-11522
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory	2024-11-22	7.8	CVE-2024-11523

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24597.			
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24598.	2024-11-22	7.8	CVE-2024-11524
irfanview -- irfanview	IrfanView DXF File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24599.	2024-11-22	7.8	CVE-2024-11525
irfanview -- irfanview	IrfanView CGM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24600.	2024-11-22	7.8	CVE-2024-11526
irfanview -- irfanview	IrfanView DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24601.	2024-11-22	7.8	CVE-2024-11527
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24602.	2024-11-22	7.8	CVE-2024-11528
irfanview -- irfanview	IrfanView DWG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24604.	2024-11-22	7.8	CVE-2024-11529
irfanview -- irfanview	IrfanView CGM File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24605.	2024-11-22	7.8	CVE-2024-11530
irfanview -- irfanview	IrfanView CGM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the	2024-11-22	7.8	CVE-2024-11531

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24606.			
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24615.	2024-11-22	7.8	CVE-2024-11532
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24616.	2024-11-22	7.8	CVE-2024-11533
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24617.	2024-11-22	7.8	CVE-2024-11534
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24618.	2024-11-22	7.8	CVE-2024-11535
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24619.	2024-11-22	7.8	CVE-2024-11536
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24620.	2024-11-22	7.8	CVE-2024-11537
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24629.	2024-11-22	7.8	CVE-2024-11538
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory	2024-11-22	7.8	CVE-2024-11539

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24699.			
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24700.	2024-11-22	7.8	CVE-2024-11540
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24702.	2024-11-22	7.8	CVE-2024-11541
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24703.	2024-11-22	7.8	CVE-2024-11542
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24704.	2024-11-22	7.8	CVE-2024-11543
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24707.	2024-11-22	7.8	CVE-2024-11544
irfanview -- irfanview	IrfanView DXF File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24709.	2024-11-22	7.8	CVE-2024-11545
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24714.	2024-11-22	7.8	CVE-2024-11546
irfanview -- irfanview	IrfanView DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory	2024-11-22	7.8	CVE-2024-11547

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24732.			
irfanview -- irfanview	IrfanView DWG File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24745.	2024-11-22	7.8	CVE-2024-11548
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24746.	2024-11-22	7.8	CVE-2024-11549
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24748.	2024-11-22	7.8	CVE-2024-11550
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24749.	2024-11-22	7.8	CVE-2024-11551
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24751.	2024-11-22	7.8	CVE-2024-11552
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24752.	2024-11-22	7.8	CVE-2024-11553
irfanview -- irfanview	IrfanView DWG File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24754.	2024-11-22	7.8	CVE-2024-11554
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the	2024-11-22	7.8	CVE-2024-11555

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24780.			
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24795.	2024-11-22	7.8	CVE-2024-11556
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24807.	2024-11-22	7.8	CVE-2024-11557
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24808.	2024-11-22	7.8	CVE-2024-11558
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24809.	2024-11-22	7.8	CVE-2024-11559
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24853.	2024-11-22	7.8	CVE-2024-11560
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24857.	2024-11-22	7.8	CVE-2024-11561
irfanview -- irfanview	IrfanView CGM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24858.	2024-11-22	7.8	CVE-2024-11562
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the	2024-11-22	7.8	CVE-2024-11563

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24860.			
irfanview -- irfanview	IrfanView DWG File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24864.	2024-11-22	7.8	CVE-2024-11564
irfanview -- irfanview	IrfanView CGM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24866.	2024-11-22	7.8	CVE-2024-11565
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24868.	2024-11-22	7.8	CVE-2024-11566
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24871.	2024-11-22	7.8	CVE-2024-11567
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24872.	2024-11-22	7.8	CVE-2024-11568
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24873.	2024-11-22	7.8	CVE-2024-11569
irfanview -- irfanview	IrfanView DXF File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24885.	2024-11-22	7.8	CVE-2024-11570
irfanview -- irfanview	IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the	2024-11-22	7.8	CVE-2024-11571

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24895.			
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24897.	2024-11-22	7.8	CVE-2024-11572
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24898.	2024-11-22	7.8	CVE-2024-11573
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24900.	2024-11-22	7.8	CVE-2024-11574
irfanview -- irfanview	IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24901.	2024-11-22	7.8	CVE-2024-11575
irfanview -- irfanview	IrfanView SID File Parsing Uninitialized Pointer Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of SID files. The issue results from the lack of proper initialization of a pointer prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-23276.	2024-11-22	7.8	CVE-2024-9258
irfanview -- irfanview	IrfanView SID File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of SID files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-23278.	2024-11-22	7.8	CVE-2024-9259
irfanview -- irfanview	IrfanView SID File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of SID files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-23280.	2024-11-22	7.8	CVE-2024-9260
irfanview -- irfanview	IrfanView SID File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of IrfanView. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of SID files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a	2024-11-22	7.8	CVE-2024-9261

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-23283.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix possible UAF in amdgpu_cs_pass1() Since the gang_size check is outside of chunk parsing loop, we need to reset i before we free the chunk data. Suggested by Ye Zhang (@VAR10CK) of Baidu Security.	2024-11-19	7.8	CVE-2023-52921
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: vsock/virtio: Initialization of the dangling pointer occurring in vsk->trans During loopback communication, a dangling pointer can be created in vsk->trans, potentially leading to a Use-After-Free condition. This issue is resolved by initializing vsk->trans to NULL.	2024-11-19	7.8	CVE-2024-50264
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: USB: serial: io_edgeport: fix use after free in debug printk The "dev_dbg(&urb->dev->dev, ..." which happens after usb_free_urb(urb) is a use after free of the "urb" pointer. Store the "dev" pointer at the start of the function to avoid this issue.	2024-11-19	7.8	CVE-2024-50267
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net: vertexcom: mse102x: Fix possible double free of TX skb The scope of the TX skb is wider than just mse102x_tx_frame_spi(), so in case the TX skb room needs to be expanded, we should free the the temporary skb instead of the original skb. Otherwise the original TX skb pointer would be freed again in mse102x_tx_work(), which leads to crashes: Internal error: Oops: 0000000096000004 [#2] PREEMPT SMP CPU: 0 PID: 712 Comm: kworker/0:1 Tainted: G D 6.6.23 Hardware name: chargebyte Charge SOM DC-ONE (DT) Workqueue: events mse102x_tx_work [mse102x] pstate: 20400009 (nzCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : skb_release_data+0xb8/0x1d8 lr : skb_release_data+0x1ac/0x1d8 sp : ffff8000819a3cc0 x29: ffff8000819a3cc0 x28: ffff0000046daa60 x27: ffff0000057f2dc0 x26: ffff000005386c00 x25: 0000000000000002 x24: 00000000ffffffff x23: 0000000000000000 x22: 0000000000000001 x21: ffff0000057f2e50 x20: 0000000000000006 x19: 0000000000000000 x18: ffff00003fdacfcc x17: e69ad452d0c49def x16: 84a005feff870102 x15: 0000000000000000 x14: 000000000000024a x13: 0000000000000002 x12: 0000000000000000 x11: 0000000000000400 x10: 0000000000000930 x9 : ffff00003fd913e8 x8 : fffffc00001bc008 x7 : 0000000000000000 x6 : 0000000000000008 x5 : ffff00003fd91340 x4 : 0000000000000000 x3 : 0000000000000009 x2 : 00000000fffffffe x1 : 0000000000000000 x0 : 0000000000000000 Call trace: skb_release_data+0xb8/0x1d8 kfree_skb_reason+0x48/0xb0 mse102x_tx_work+0x164/0x35c [mse102x] process_one_work+0x138/0x260 worker_thread+0x32c/0x438 kthread+0x118/0x11c ret_from_fork+0x10/0x20 Code: aa1303e0 97fffab6 72001c1f 54000141 (f9400660)	2024-11-19	7.8	CVE-2024-50276
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: add missing size check in amdgpu_debugfs_gprwave_read() Avoid a possible buffer overflow if size is larger than 4K. (cherry picked from commit f5d873f5825b40d886d03bd2aede91d4cf002434)	2024-11-19	7.8	CVE-2024-50282
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix slab-use-after-free in smb3_preauth_hash_rsp ksmbd_user_session_put should be called under smb3_preauth_hash_rsp(). It will avoid freeing session before calling smb3_preauth_hash_rsp().	2024-11-19	7.8	CVE-2024-50283
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net/sched: stop qdisc_tree_reduce_backlog on TC_H_ROOT In qdisc_tree_reduce_backlog, Qdiscs with major handle ffff: are assumed to be either root or ingress. This assumption is bogus since it's valid to create egress qdiscs with major handle ffff: Budimir Markovic found that for qdiscs like DRR that maintain an active class list, it will cause a UAF with a dangling class pointer. In 066a3b5b2346, the concern was to avoid iterating over the ingress qdisc since its parent is itself. The proper fix is to stop when parent TC_H_ROOT is reached because the only way to retrieve ingress is when a hierarchy which does not contain a ffff: major handle call into qdisc_lookup with TC_H_MAJ(TC_H_ROOT). In the scenario where major ffff: is an egress qdisc in any of the tree levels, the updates will also propagate to TC_H_ROOT, which then the iteration must stop. net/sched/sch_api.c | 2 +- 1 file changed, 1 insertion(+), 1 deletion(-)	2024-11-19	7.8	CVE-2024-53057
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: media: s5p-jpeg: prevent buffer overflows The current logic allows word to be less than 2. If this happens, there will be buffer overflows, as reported by smatch. Add extra checks to prevent it. While here, remove an unused word = 0 assignment.	2024-11-19	7.8	CVE-2024-53061

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: firmware: arm_scmi: Fix slab-use-after-free in scmi_bus_notifier() The scmi_dev->name is released prematurely in __scmi_device_destroy(), which causes slab-use-after-free when accessing scmi_dev->name in scmi_bus_notifier(). So move the release of scmi_dev->name to scmi_device_release() to avoid slab-use-after-free. | BUG: KASAN: slab-use-after-free in strncmp+0xe4/0xec | Read of size 1 at addr ffffff80a482bcc0 by task swapper/0/1 | | CPU: 1 PID: 1 Comm: swapper/0 Not tainted 6.6.38-debug #1 | Hardware name: Qualcomm Technologies, Inc. SA8775P Ride (DT) | Call trace: | dump_backtrace+0x94/0x114 | show_stack+0x18/0x24 | dump_stack_lvl+0x48/0x60 | print_report+0xf4/0x5b0 | kasan_report+0xa4/0xec | __asan_report_load1_noabort+0x20/0x2c | strncmp+0xe4/0xec | scmi_bus_notifier+0x5c/0x54c | notifier_call_chain+0xb4/0x31c | blocking_notifier_call_chain+0x68/0x9c | bus_notify+0x54/0x78 | device_del+0x1bc/0x840 | device_unregister+0x20/0xb4 | __scmi_device_destroy+0xac/0x280 | scmi_device_destroy+0x94/0xd0 | scmi_chan_setup+0x524/0x750 | scmi_probe+0x7fc/0x1508 | platform_probe+0xc4/0x19c | really_probe+0x32c/0x99c | __driver_probe_device+0x15c/0x3c4 | driver_probe_device+0x5c/0x170 | __driver_attach+0x1c8/0x440 | bus_for_each_dev+0xf4/0x178 | driver_attach+0x3c/0x58 | bus_add_driver+0x234/0x4d4 | driver_register+0xf4/0x3c0 | __platform_driver_register+0x60/0x88 | scmi_driver_init+0xb0/0x104 | do_one_initcall+0xb4/0x664 | kernel_init_freeable+0x3c8/0x894 | kernel_init+0x24/0x1e8 | ret_from_fork+0x10/0x20 | | Allocated by task 1: | kasan_save_stack+0x2c/0x54 | kasan_set_track+0x2c/0x40 | kasan_save_alloc_info+0x24/0x34 | __kasan_kmalloc+0xa0/0xb8 | __kmalloc_node_track_caller+0x6c/0x104 | kstrdup+0x48/0x84 | kstrdup_const+0x34/0x40 | __scmi_device_create.part.0+0x8c/0x408 | scmi_device_create+0x104/0x370 | scmi_chan_setup+0x2a0/0x750 | scmi_probe+0x7fc/0x1508 | platform_probe+0xc4/0x19c | really_probe+0x32c/0x99c | __driver_probe_device+0x15c/0x3c4 | driver_probe_device+0x5c/0x170 | __driver_attach+0x1c8/0x440 | bus_for_each_dev+0xf4/0x178 | driver_attach+0x3c/0x58 | bus_add_driver+0x234/0x4d4 | driver_register+0xf4/0x3c0 | __platform_driver_register+0x60/0x88 | scmi_driver_init+0xb0/0x104 | do_one_initcall+0xb4/0x664 | kernel_init_freeable+0x3c8/0x894 | kernel_init+0x24/0x1e8 | ret_from_fork+0x10/0x20 | | Freed by task 1: | kasan_save_stack+0x2c/0x54 | kasan_set_track+0x2c/0x40 | kasan_save_free_info+0x38/0x5c | __kasan_slab_free+0xe8/0x164 | __kmem_cache_free+0x11c/0x230 | kfree+0x70/0x130 | kfree_const+0x20/0x40 | __scmi_device_destroy+0x70/0x280 | scmi_device_destroy+0x94/0xd0 | scmi_chan_setup+0x524/0x750 | scmi_probe+0x7fc/0x1508 | platform_probe+0xc4/0x19c | really_probe+0x32c/0x99c | __driver_probe_device+0x15c/0x3c4 | driver_probe_device+0x5c/0x170 | __driver_attach+0x1c8/0x440 | bus_for_each_dev+0xf4/0x178 | driver_attach+0x3c/0x58 | bus_add_driver+0x234/0x4d4 | driver_register+0xf4/0x3c0 | __platform_driver_register+0x60/0x88 | scmi_driver_init+0xb0/0x104 | do_one_initcall+0xb4/0x664 | kernel_init_freeable+0x3c8/0x894 | kernel_init+0x24/0x1e8 | ret_from_fork+0x10/0x20	2024-11-19	7.8	CVE-2024-53068
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: usb: typec: fix potential out of bounds in ucsi_ccg_update_set_new_cam_cmd() The "*cmd" variable can be controlled by the user via debugfs. That means "new_cam" can be as high as 255 while the size of the uc->updated[] array is UCSI_MAX_ALTMODES (30). The call tree is: ucsi_cmd() // val comes from simple_attr_write_xsigned() -> ucsi_send_command() -> ucsi_send_command_common() -> ucsi_run_command() // calls ucsi->ops->sync_control() -> ucsi_ccg_sync_control()	2024-11-19	7.1	CVE-2024-50268
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: security/keys: fix slab-out-of-bounds in key_task_permission KASAN reports an out of bounds read: BUG: KASAN: slab-out-of-bounds in __kuid_val include/linux/uidgid.h:36 BUG: KASAN: slab-out-of-bounds in uid_eq include/linux/uidgid.h:63 [inline] BUG: KASAN: slab-out-of-bounds in key_task_permission+0x394/0x410 security/keys/permission.c:54 Read of size 4 at addr ffff88813c3ab618 by task stress-ng/4362 CPU: 2 PID: 4362 Comm: stress-ng Not tainted 5.10.0-14930-gafbffd6c3ede #15 Call Trace: __dump_stack lib/dump_stack.c:82 [inline] dump_stack+0x107/0x167 lib/dump_stack.c:123 print_address_description.constprop.0+0x19/0x170 mm/kasan/report.c:400	2024-11-19	7.1	CVE-2024-50301

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	__kasan_report.cold+0x6c/0x84 mm/kasan/report.c:560 kasan_report+0x3a/0x50 mm/kasan/report.c:585 __kuid_val include/linux/uidgid.h:36 [inline] uid_eq include/linux/uidgid.h:63 [inline] key_task_permission+0x394/0x410 security/keys/permission.c:54 search_nested_keyrings+0x90e/0xe90 security/keys/keyring.c:793 This issue was also reported by syzbot. It can be reproduced by following these steps(more details [1]): 1. Obtain more than 32 inputs that have similar hashes, which ends with the pattern '0xxxxxxe6'. 2. Reboot and add the keys obtained in step 1. The reproducer demonstrates how this issue happened: 1. In the search_nested_keyrings function, when it iterates through the slots in a node(below tag ascend_to_node), if the slot pointer is meta and node->back_pointer != NULL(it means a root), it will proceed to descend_to_node. However, there is an exception. If node is the root, and one of the slots points to a shortcut, it will be treated as a keyring. 2. Whether the ptr is keyring decided by keyring_ptr_is_keyring function. However, KEYRING_PTR_SUBTYPE is 0x2UL, the same as ASSOC_ARRAY_PTR_SUBTYPE_MASK. 3. When 32 keys with the similar hashes are added to the tree, the ROOT has keys with hashes that are not similar (e.g. slot 0) and it splits NODE A without using a shortcut. When NODE A is filled with keys that all hashes are xxe6, the keys are similar, NODE A will split with a shortcut. Finally, it forms the tree as shown below, where slot 6 points to a shortcut. NODE A +------>+---+ ROOT | | 0 | xxe6 +---+ | +---+ xxxx | 0 | shortcut : : xxe6 +---+ | +---+ xxe6 : : | | | xxe6 +---+ | +---+ | 6 |---+ : : xxe6 +---+ +---+ xxe6 : : | f | xxe6 +---+ +---+ xxe6 | f | +---+ 4. As mentioned above, If a slot(slot 6) of the root points to a shortcut, it may be mistakenly transferred to a key*, leading to a read out-of-bounds read. To fix this issue, one should jump to descend_to_node if the ptr is a shortcut, regardless of whether the node is root or not. [1] https://lore.kernel.org/linux-kernel/1cfa878e-8c7b-4570-8606-21daf5e13ce7@huaweicloud.com/ [jarkko: tweaked the commit message a bit to have an appropriate closes tag.]				
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: media: mgb4: protect driver against spectre Frequency range is set from sysfs via frequency_range_store(), being vulnerable to spectre, as reported by smatch: drivers/media/pci/mgb4/mgb4_cmt.c:231 mgb4_cmt_set_vin_freq_range() warn: potential spectre issue 'cmt_vals_in' [r] drivers/media/pci/mgb4/mgb4_cmt.c:238 mgb4_cmt_set_vin_freq_range() warn: possible spectre second half. 'reg_set' Fix it.	2024-11-19	7.1	CVE-2024-53062
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: virtio_net: Add hash_key_length check Add hash_key_length check in virtnet_probe() to avoid possible out of bound errors when setting/reading the hash key.	2024-11-19	7.1	CVE-2024-53082
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix slab-use-after-free in ksmbd_smb2_session_create There is a race condition between ksmbd_smb2_session_create and ksmbd_expire_session. This patch add missing sessions_table_lock while adding/deleting session from global session table.	2024-11-19	7	CVE-2024-50286
lis -- video_gallery	Deserialization of Untrusted Data vulnerability in Lis Lis Video Gallery allows Object Injection.This issue affects Lis Video Gallery: from n/a through 0.2.1.	2024-11-18	9.8	CVE-2024-52430
litestar -- litestar	Litestar is an Asynchronous Server Gateway Interface (ASGI) framework. Prior to version 2.13.0, the multipart form parser shipped with litestar expects the entire request body as a single byte string and there is no default limit for the total size of the request body. This allows an attacker to upload arbitrary large files wrapped in a `multipart/form-data` request and cause excessive memory consumption on the server. The multipart form parser in affected versions is vulnerable to this type of attack by design. The public method signature as well as its implementation both expect the entire request body to be available as a single byte string. It is not possible to accept large file uploads in a safe way using this parser. This may be a regression, as a variation of this issue was already reported in CVE-2023-25578. Limiting the part number is not sufficient to prevent out-of-memory errors on the server. A patch is available in version 2.13.0.	2024-11-20	7.5	CVE-2024-52581
mindstien -- my_geo_posts_free	Deserialization of Untrusted Data vulnerability in Mindstien Technologies My Geo Posts Free allows Object Injection.This issue affects My Geo Posts Free: from n/a through 1.2.	2024-11-18	9.8	CVE-2024-52433
n/a -- n/a	The MP3 Sticky Player plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 8.0 via the content/downloader.php file. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. Please note the vendor released the patched version as the same version as the affected version.	2024-11-23	7.5	CVE-2024-10803

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a -- n/a	Vulnerability in the Oracle Agile PLM Framework product of Oracle Supply Chain (component: Software Development Kit, Process Extension). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM Framework. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Agile PLM Framework accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2024-11-18	7.5	CVE-2024-21287
n/a -- n/a	The The Request a Quote for WooCommerce and Elementor - Get a Quote Button - Product Enquiry Form Popup - Product Quotation plugin for WordPress is vulnerable to arbitrary shortcode execution via fire_contact_form AJAX action in all versions up to, and including, 1.4. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	2024-11-23	7.3	CVE-2024-11034
n/a -- n/a	The Activity Log - Monitor & Record User Changes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the event parameters in all versions up to, and including, 2.11.1 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 an administrative user accesses an injected page.	2024-11-21	7.2	CVE-2024-10788
n/a -- n/a	A low privileged remote attacker may modify the BACNet service properties due to incorrect permission assignment for critical resources which may lead to a DoS limited to BACNet communication.	2024-11-18	7.1	CVE-2024-41974
nixsolutions -- nix_anti-spam_light	Deserialization of Untrusted Data vulnerability in NIX Solutions Ltd NIX Anti-Spam Light allows Object Injection.This issue affects NIX Anti-Spam Light: from n/a through 0.0.4.	2024-11-18	9.8	CVE-2024-52432
paloaltonetworks -- pan-os	An authentication bypass in Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to gain PAN-OS administrator privileges to perform administrative actions, tamper with the configuration, or exploit other authenticated privilege escalation vulnerabilities like CVE-2024-9474 https://security.paloaltonetworks.com/CVE-2024-9474 . The risk of this issue is greatly reduced if you secure access to the management web interface by restricting access to only trusted internal IP addresses according to our recommendedÂ best practice deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue is applicable only to PAN-OS 10.2, PAN-OS 11.0, PAN-OS 11.1, and PAN-OS 11.2 software. Cloud NGFW and Prisma Access are not impacted by this vulnerability.	2024-11-18	9.8	CVE-2024-0012
paloaltonetworks -- pan-os	A privilege escalation vulnerability in Palo Alto Networks PAN-OS software allows a PAN-OS administrator with access to the management web interface to perform actions on the firewall with root privileges. Cloud NGFW and Prisma Access are not impacted by this vulnerability.	2024-11-18	7.2	CVE-2024-9474
pandasecurity -- panda_dome	Panda Security Dome Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Panda Security Dome. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the PSANHost executable. By creating a junction, an attacker can abuse the service to delete arbitrary files. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-23402.	2024-11-22	7.8	CVE-2024-7242
pandasecurity -- panda_dome	Panda Security Dome Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Panda Security Dome. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the PSANHost executable. By creating a junction, an attacker can abuse the service to create arbitrary files. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-23413.	2024-11-22	7	CVE-2024-7243
pandasecurity -- panda_dome	Panda Security Dome VPN DLL Hijacking Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Panda Security Dome. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the VPN process. The process does not	2024-11-22	7	CVE-2024-7244

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	restrict DLL search to trusted paths, which can result in the loading of a malicious DLL. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-23428.			
pandasecurity -- panda_dome	Panda Security Dome VPN Incorrect Permission Assignment Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Panda Security Dome. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Hydra Sdk Windows Service. The issue lies in the lack of proper permissions set on a folder created by the service. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-23429.	2024-11-22	7	CVE-2024-7245
phpgurukul -- boat_booking_system	File Upload vulnerability in change-image.php in Anuj Kumar's Boat Booking System version 1.0 allows local attackers to upload a malicious PHP script via the Image Upload Mechanism parameter.	2024-11-20	7.2	CVE-2024-51208
pressaholic -- wordpress_video_robot	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pressaholic WordPress Video Robot - The Ultimate Video Importer allows SQL Injection.This issue affects WordPress Video Robot - The Ultimate Video Importer: from n/a through 1.20.0.	2024-11-18	9.8	CVE-2024-52431
qualcomm -- mdm9206_firmware	Certain unprivileged processes are able to perform IOCTL calls.	2024-11-22	7.8	CVE-2017-9711
scripteo -- ads_booster_by_ads_pro	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Scripteo Ads Booster by Ads Pro allows PHP Local File Inclusion.This issue affects Ads Booster by Ads Pro: from n/a through 1.12.	2024-11-18	9.8	CVE-2024-52428
siemens -- tecnomatix_plant_simulation	A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2302.0018), Tecnomatix Plant Simulation V2404 (All versions < V2404.0007). The affected applications contain a stack based overflow vulnerability while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24486)	2024-11-18	7.8	CVE-2024-52572
supsystic -- popup	Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Supsystic Popup by Supsystic allows Command Injection.This issue affects Popup by Supsystic: from n/a through 1.10.29.	2024-11-18	9.1	CVE-2024-52434
tenda -- ac6_firmware	Tenda AC6 v2.0 v15.03.06.50 was discovered to contain a buffer overflow in the function 'fromSetSysTime.	2024-11-19	9.8	CVE-2024-52714
tungstenautomation -- power_pdf	Tungsten Automation Power PDF XPS File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of XPS files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24385.	2024-11-22	7.8	CVE-2024-9732
tungstenautomation -- power_pdf	Tungsten Automation Power PDF PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24389.	2024-11-22	7.8	CVE-2024-9733
tungstenautomation -- power_pdf	Tungsten Automation Power PDF PDF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24400.	2024-11-22	7.8	CVE-2024-9734

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tungstenautomation -- power_pdf	Tungsten Automation Power PDF JPF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24451.	2024-11-22	7.8	CVE-2024-9735
tungstenautomation -- power_pdf	Tungsten Automation Power PDF PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24452.	2024-11-22	7.8	CVE-2024-9736
tungstenautomation -- power_pdf	Tungsten Automation Power PDF PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24453.	2024-11-22	7.8	CVE-2024-9737
tungstenautomation -- power_pdf	Tungsten Automation Power PDF PDF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24454.	2024-11-22	7.8	CVE-2024-9738
tungstenautomation -- power_pdf	Tungsten Automation Power PDF PDF File Parsing Memory Corruption Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24455.	2024-11-22	7.8	CVE-2024-9739
tungstenautomation -- power_pdf	Tungsten Automation Power PDF BMP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24456.	2024-11-22	7.8	CVE-2024-9740
tungstenautomation -- power_pdf	Tungsten Automation Power PDF PDF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24457.	2024-11-22	7.8	CVE-2024-9741

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tungstenautomation -- power_pdf	Tungsten Automation Power PDF PSD File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PSD files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24458.	2024-11-22	7.8	CVE-2024-9742
tungstenautomation -- power_pdf	Tungsten Automation Power PDF PDF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24459.	2024-11-22	7.8	CVE-2024-9743
tungstenautomation -- power_pdf	Tungsten Automation Power PDF JP2 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24460.	2024-11-22	7.8	CVE-2024-9744
tungstenautomation -- power_pdf	Tungsten Automation Power PDF TIF File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of TIF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24461.	2024-11-22	7.8	CVE-2024-9745
tungstenautomation -- power_pdf	Tungsten Automation Power PDF TGA File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of TGA files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24462.	2024-11-22	7.8	CVE-2024-9746
tungstenautomation -- power_pdf	Tungsten Automation Power PDF PSD File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PSD files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24463.	2024-11-22	7.8	CVE-2024-9747
tungstenautomation -- power_pdf	Tungsten Automation Power PDF XPS File Parsing Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of XPS files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24464.	2024-11-22	7.8	CVE-2024-9748

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tungstenautomation -- power_pdf	Tungsten Automation Power PDF PNG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Tungsten Automation Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PNG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-24466.	2024-11-22	7.8	CVE-2024-9750
vivwebsolutions -- dynamic_widgets	Cross-Site Request Forgery (CSRF) vulnerability in Vivwebs Dynamic Widgets.This issue affects Dynamic Widgets: from n/a through 1.6.4.	2024-11-19	8.8	CVE-2024-51669
vollstart -- event_tickets_with_ticket_scanner	Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Saso Nikolov Event Tickets with Ticket Scanner allows Server Side Include (SSI) Injection.This issue affects Event Tickets with Ticket Scanner: from n/a through 2.3.11.	2024-11-18	8.8	CVE-2024-52427
WAGO--TP600	A low privileged remote attacker may modify the boot mode configuration setup of the device, leading to modification of the firmware upgrade process or a denial-of-service attack.	2024-11-18	8.1	CVE-2024-41967
WAGO--TP600	A low privileged remote attacker can overwrite an arbitrary file on the filesystem leading to a DoS and data loss.	2024-11-18	8.1	CVE-2024-41971
WAGO--WAGO	A low privileged remote attacker can specify an arbitrary file on the filesystem whichÂ may lead to an arbitrary file writes with root privileges.	2024-11-18	8.1	CVE-2024-41973
wordpress--wordpress	The Social Login plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 5.9.0. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email and the user does not have an already-existing account for the service returning the token.	2024-11-23	9.8	CVE-2024-10961
wordpress--wordpress	The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.4.2 via the _load_template function. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.	2024-11-23	8.8	CVE-2024-10873
wordpress--wordpress	The WP-Orphanage Extended plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2. This is due to missing or incorrect nonce validation on the wporphanageex_menu_settings() function. This makes it possible for unauthenticated attackers to escalate the privileges of all orphan accounts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-11-23	8.8	CVE-2024-11415
wordpress--wordpress	The School Management System for Wordpress plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the mj_smgt_load_documets_new() and mj_smgt_load_documets() functions in all versions up to, and including, 91.5.0. This makes it possible for authenticated attackers, with Student-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-11-23	8.8	CVE-2024-9660
wordpress--wordpress	The Image Optimizer, Resizer and CDN - Sirv plugin for WordPress is vulnerable to unauthorized modification of data that can lead to a denial of service due to insufficient validation on the filename parameter of the sirv_upload_file_by_chunks() function and lack of in all versions up to, and including, 7.3.0. This makes it possible for authenticated attackers, with Contributor-level access and above, to delete arbitrary option values on the WordPress site. This can be leveraged to delete an option that would create an error on the site and deny service to legitimate users.	2024-11-20	8.1	CVE-2024-10855
wordpress--wordpress	The Sky Addons for Elementor (Free Templates Library, Live Copy, Animations, Post Grid, Post Carousel, Particles, Sliders, Chart, Blogs) plugin for WordPress is vulnerable to unauthorized modification of data that can lead to a denial of service due to a missing capability check on the save_options() function in all versions up to, and including, 2.6.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to update arbitrary options on the WordPress site. Please note this is limited to option values that can be saved as arrays.	2024-11-22	8.1	CVE-2024-11104

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress--wordpress	The Sky Addons for Elementor (Free Templates Library, Live Copy, Animations, Post Grid, Post Carousel, Particles, Sliders, Chart, Blog, Video Gallery) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.6.1. This is due to missing or incorrect nonce validation on the save_options() function. This makes it possible for unauthenticated attackers to update arbitrary options on the WordPress site via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Please note this is limited to option values that can be saved as arrays.	2024-11-22	8.1	CVE-2024-11601
wpdownloadmanager -- premium_packages_-_sell_digital_products_securely	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in W3 Eden, Inc. Premium Packages allows SQL Injection.This issue affects Premium Packages: from n/a through 5.9.3.	2024-11-18	7.2	CVE-2024-52435
wpexperts -- post_smtp	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Post SMTP allows Blind SQL Injection.This issue affects Post SMTP: from n/a through 2.9.9.	2024-11-18	7.2	CVE-2024-52436
zohocorp -- manageengine_adaudit_plus	Zohocorp ManageEngine ADAudit Plus versions below 8123 are vulnerable to SQL Injection inÂ the reports module.	2024-11-18	8.8	CVE-2024-49574
zte -- nh8091_firmware	ZTE NH8091 product has an improper permission control vulnerability. Due to improper permission control of the Web module interface, an authenticated attacker may exploit the vulnerability to execute arbitrary commands.	2024-11-18	8.8	CVE-2024-22067
1000 Projects--Beauty Parlour Management System	A vulnerability was found in 1000 Projects Beauty Parlour Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation of the argument name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-12	7.3	CVE-2024-11100
1000 Projects--Beauty Parlour Management System	A vulnerability classified as critical has been found in 1000 Projects Beauty Parlour Management System 1.0. This affects an unknown part of the file /admin/forgot-password.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.	2024-11-15	7.3	CVE-2024-11257
1000 Projects--Beauty Parlour Management System	A vulnerability classified as critical was found in 1000 Projects Beauty Parlour Management System 1.0. This vulnerability affects unknown code of the file /admin/index.php. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-15	7.3	CVE-2024-11258
1000 Projects--Portfolio Management System MCA	A vulnerability was found in 1000 Projects Portfolio Management System MCA 1.0 and classified as critical. This issue affects some unknown processing of the file /login.php. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-15	7.3	CVE-2024-11256
adobe -- after_effects	After Effects versions 23.6.9, 24.6.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47441
adobe -- after_effects	After Effects versions 23.6.9, 24.6.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47442
adobe -- after_effects	After Effects versions 23.6.9, 24.6.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47443
adobe -- illustrator	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-45114
adobe -- illustrator	Illustrator versions 28.7.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47450

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- illustrator	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47451
adobe -- illustrator	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47452
adobe -- indesign	InDesign Desktop versions ID18.5.2, ID19.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-49507
adobe -- indesign	InDesign Desktop versions ID18.5.2, ID19.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-49508
adobe -- indesign	InDesign Desktop versions ID18.5.3, ID19.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-49509
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by a Double Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47426
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47427
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47428
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47429
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47430
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47431
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47432
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47433
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-47434
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an Untrusted Search Path vulnerability that might allow attackers to execute arbitrary code. If the application uses a search path to locate critical resources such as programs, then an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. The problem extends to any type of critical resource that the application trusts. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-49515
adobe -- substance_3d_pai	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of	2024-11-12	7.8	CVE-2024-49516

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nter	the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-49517
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-49518
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-49519
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-49520
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-49525
Adobe--Adobe Commerce	Adobe Commerce versions 3.2.5 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to a security feature bypass. A low privileged attacker could exploit this vulnerability to send crafted requests from the vulnerable server to internal systems, which could result in the bypassing of security measures such as firewalls. Exploitation of this issue does not require user interaction.	2024-11-12	7.7	CVE-2024-49521
Adobe--Animate	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-49526
Adobe--Animate	Animate versions 23.0.7, 24.0.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-49528
Adobe--Photoshop Desktop	Photoshop Desktop versions 24.7.3, 25.11 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	7.8	CVE-2024-49514
adonesevangelista -- agri-trading_online_shopping_system	A business logic vulnerability exists in the Add to Cart function of itsourcecode Agri-Trading Online Shopping System 1.0, which allows remote attackers to manipulate the quant parameter when adding a product to the cart. By setting the quantity value to -0, an attacker can exploit a flaw in the application's total price calculation logic. This vulnerability causes the total price to be reduced to zero, allowing the attacker to add items to the cart and proceed to checkout.	2024-11-14	7.5	CVE-2024-50968
algolplus-- Advanced Order Export For WooCommerce	The Advanced Order Export For WooCommerce plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.5.5 via deserialization of untrusted input during Order export when the "Try to convert serialized values" option is enabled. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain allows attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	2024-11-13	8.1	CVE-2024-10828
amd -- ryzen_ai_software	Improper input validation in the NPU driver could allow an attacker to supply a specially crafted pointer potentially leading to arbitrary code execution.	2024-11-12	7.8	CVE-2024-21974
amd -- ryzen_ai_software	Improper input validation in the NPU driver could allow an attacker to supply a specially crafted pointer potentially leading to arbitrary code execution.	2024-11-12	7.8	CVE-2024-21975
AMD--AMD Cloud Manageability Service Software	Incorrect default permissions in the AMD Cloud Manageability Service (ACMS) Software installation directory could allow an attacker to achieve privilege escalation potentially resulting in arbitrary code execution.	2024-11-12	7.3	CVE-2024-21939

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
AMD--AMD Management Console	Incorrect default permissions in the AMD Management Console installation directory could allow an attacker to achieve privilege escalation potentially resulting in arbitrary code execution.	2024-11-12	7.3	CVE-2024-21957
AMD--AMD Management Plug-In for SCCM	Incorrect default permissions in the AMD Management Plugin for the MicrosoftÂ® System Center Configuration Manager (SCCM) installation directory could allow an attacker to achieve privilege escalation, potentially resulting in arbitrary code execution.	2024-11-12	7.3	CVE-2024-21938
AMD--AMD Provisioning Console (APC) Software	Incorrect default permissions in the AMD Provisioning Console installation directory could allow an attacker to achieve privilege escalation, potentially resulting in arbitrary code execution.	2024-11-12	7.3	CVE-2024-21958
AMD--AMD Ryzen AI Software	Improper input validation in the NPU driver could allow an attacker to supply a specially crafted pointer potentially leading to arbitrary code execution.	2024-11-12	8.8	CVE-2024-21976
AMD--AMD Ryzen Master Monitoring SDK	Incorrect default permissions in the AMD RyzenTM Master monitoring SDK installation directory could allow an attacker to achieve privilege escalation potentially resulting in arbitrary code execution.	2024-11-12	7.3	CVE-2024-21945
AMD--AMD Ryzen Master Utility for Overclocking Control	Incorrect default permissions in the AMD RyzenTM Master Utility installation directory could allow an attacker to achieve privilege escalation potentially resulting in arbitrary code execution.	2024-11-12	7.3	CVE-2024-21946
AMD--AMD Software: PRO Edition	Incorrect default permissions in the AMD HIP SDK installation directory could allow an attacker to achieve privilege escalation potentially resulting in arbitrary code execution.	2024-11-12	7.3	CVE-2024-21937
AMI--AptioV	APTIOV contains a vulnerability in the BIOS where a user or attacker may cause an improper restriction of operations within the bounds of a memory buffer over the network. A successful exploitation of this vulnerability may lead to code execution outside of the intended System Management Mode.	2024-11-12	7.2	CVE-2024-42442
ampache -- ampache	Ampache is a web based audio/video streaming application and file manager. This vulnerability exists in the interface section of the Ampache menu, where users can change "Custom URL - Logo". This section is not properly sanitized, allowing for the input of strings that can execute JavaScript. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-11-11	9	CVE-2024-51490
ampache -- ampache	Ampache is a web based audio/video streaming application and file manager. The current implementation of token parsing fails to properly validate CSRF tokens when activating or deactivating controllers. This vulnerability allows an attacker to exploit CSRF attacks, potentially enabling them to change website features that should only be managed by administrators through malicious requests. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-11-11	8.1	CVE-2024-51484
ampache -- ampache	Ampache is a web based audio/video streaming application and file manager. The current implementation of token parsing fails to properly validate CSRF tokens when activating or deactivating plugins. This vulnerability allows an attacker to exploit CSRF attacks, potentially enabling them to change website features that should only be managed by administrators through malicious requests. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-11-11	8.1	CVE-2024-51485
ampache -- ampache	Ampache is a web based audio/video streaming application and file manager. The vulnerability exists in the interface section of the Ampache menu, where users can change the "Custom URL?-?Favicon". This section is not properly sanitized, allowing for the input of strings that can execute JavaScript. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-11-11	8.4	CVE-2024-51486
ampache -- ampache	Ampache is a web based audio/video streaming application and file manager. The current implementation of token parsing fails to properly validate CSRF tokens when activating or deactivating catalog. This vulnerability allows an attacker to exploit CSRF attacks, potentially enabling them to change website features that should only be managed by administrators through malicious requests. This issue	2024-11-11	8.1	CVE-2024-51487

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.			
angeljudesuarez -- construction_management_system	A SQL injection vulnerability in print.php of Itsourcecode Construction Management System 1.0 allows remote attackers to execute arbitrary SQL commands via the map_id parameter.	2024-11-13	7.2	CVE-2024-50971
angeljudesuarez -- construction_management_system	A SQL injection vulnerability in printtool.php of Itsourcecode Construction Management System 1.0 allows remote attackers to execute arbitrary SQL commands via the borrow_id parameter.	2024-11-13	7.2	CVE-2024-50972
angeljudesuarez -- tailoring_management_system	A vulnerability classified as critical was found in itsourcecode Tailoring Management System 1.0. This vulnerability affects unknown code of the file /incadd.php. The manipulation of the argument inccat/desc/date/amount leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "inccat" to be affected. But it must be assumed "desc", "date", and "amount" are affected as well.	2024-11-11	9.8	CVE-2024-11074
anisha -- job_recruitment	A vulnerability, which was classified as critical, has been found in code-projects Job Recruitment 1.0. This issue affects some unknown processing of the file /activation.php. The manipulation of the argument e_hash leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-11	9.8	CVE-2024-11076
anisha -- job_recruitment	A vulnerability, which was classified as critical, was found in code-projects Job Recruitment 1.0. Affected is an unknown function of the file /index.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-11	9.8	CVE-2024-11077
anisha -- job_recruitment	A vulnerability was found in code-projects Job Recruitment 1.0 and classified as critical. This issue affects some unknown processing of the file /login.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-12	9.8	CVE-2024-11099
anisha -- job_recruitment	A vulnerability was found in code-projects Job Recruitment up to 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file admin.php. The manipulation of the argument userid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-12	8.8	CVE-2024-11127
Anthony Carbon-- WDES Responsive Mobile Menu	Deserialization of Untrusted Data vulnerability in Anthony Carbon WDES Responsive Mobile Menu allows Object Injection.This issue affects WDES Responsive Mobile Menu: from n/a through 5.3.18.	2024-11-16	9.8	CVE-2024-52414
Apache Software Foundation-- Apache Airflow	Apache Airflow versions before 2.10.3 contain a vulnerability that could expose sensitive configuration variables in task logs. This vulnerability allows DAG authors to unintentionally or intentionally log sensitive configuration variables. Unauthorized users could access these logs, potentially exposing critical data that could be exploited to compromise the security of the Airflow deployment. In version 2.10.3, secrets are now masked in task logs to prevent sensitive configuration variables from being exposed in the logging output. Users should upgrade to Airflow 2.10.3 or the latest version to eliminate this vulnerability.Â If you suspect that DAG authors could have logged the secret values to the logs and that your logs are not additionally protected, it is also recommended that you update those secrets.	2024-11-15	7.5	CVE-2024-45784
Apache Software Foundation-- Apache CloudStack	Account users in Apache CloudStack by default are allowed to register templates to be downloaded directly to the primary storage for deploying instances. Due to missing validation checks for KVM-compatible templates in CloudStack 4.0.0 through 4.18.2.4 and 4.19.0.0 through 4.19.1.2, an attacker that can register templates, can use them to deploy malicious instances on KVM-based environments and exploit this to gain access to the host filesystems that could result in the compromise of resource integrity and confidentiality, data loss, denial of service, and availability of KVM-based infrastructure managed by CloudStack. Users are recommended to upgrade to Apache CloudStack 4.18.2.5 or 4.19.1.3, or later, which addresses this issue. Additionally, all user-registered KVM-compatible templates can be scanned and checked that they are flat files that should not be using any additional or unnecessary features. For example, operators can run the following command on their file-based primary storage(s) and inspect the output. An empty output for the	2024-11-12	8.5	CVE-2024-50386

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disk being validated means it has no references to the host filesystems; on the other hand, if the output for the disk being validated is not empty, it might indicate a compromised disk. However, bear in mind that (i) volumes created from templates will have references for the templates at first and (ii) volumes can be consolidated while migrating, losing their references to the templates. Therefore, the command execution for the primary storages can show both false positives and false negatives. for file in $(find /path/to/storage/ -type f -regex [a-f0-9\-]*.*); do echo "Retrieving file [$file] info. If the output is not empty, that might indicate a compromised disk; check it carefully."; qemu-img info -U $file | grep file: ; printf "\n\n"; done For checking the whole template/volume features of each disk, operators can run the following command: for file in $(find /path/to/storage/ -type f -regex [a-f0-9\-]*.*); do echo "Retrieving file [$file] info."; qemu-img info -U $file; printf "\n\n"; done			
Apache Software Foundation--Apache Traffic Server	Unchecked return value can allow Apache Traffic Server to retain privileges on startup. This issue affects Apache Traffic Server: from 9.2.0 through 9.2.5, from 10.0.0 through 10.0.1. Users are recommended to upgrade to version 9.2.6 or 10.0.2, which fixes the issue.	2024-11-14	9.1	CVE-2024-50306
Apache Software Foundation--Apache Traffic Server	Improper Input Validation vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.11, from 9.0.0 through 9.2.5. Users are recommended to upgrade to version 9.2.6, which fixes the issue, or 10.0.2, which does not have the issue.	2024-11-14	7.5	CVE-2024-38479
Apache Software Foundation--Apache Traffic Server	Valid Host header field can cause Apache Traffic Server to crash on some platforms. This issue affects Apache Traffic Server: from 9.2.0 through 9.2.5. Users are recommended to upgrade to version 9.2.6, which fixes the issue, or 10.0.2, which does not have the issue.	2024-11-14	7.5	CVE-2024-50305
Arttia Creative--Datasets Manager by Arttia Creative	Unrestricted Upload of File with Dangerous Type vulnerability in Arttia Creative Datasets Manager by Arttia Creative.This issue affects Datasets Manager by Arttia Creative: from n/a through 1.5.	2024-11-14	10	CVE-2024-52375
Autodesk--Installer	A maliciously crafted DLL file when placed in temporary files and folders that are leveraged by the Autodesk Installer could lead to escalation of privileges to NT AUTHORITY/SYSTEM due to insecure privilege management.	2024-11-15	7.2	CVE-2024-9500
Avigilon--VideoIQ iCVR HD camera	Avigilon - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	2024-11-14	7.5	CVE-2024-45253
axelkeller--GPX Viewer	The GPX Viewer plugin for WordPress is vulnerable to arbitrary file creation due to a missing capability check and file type validation in the gpxv_file_upload() function in all versions up to, and including, 2.2.8. This makes it possible for authenticated attackers, with subscriber-level access and above, to create arbitrary files on the affected site's server which may make remote code execution possible.	2024-11-13	8.8	CVE-2024-10629
ays-pro--Chartify WordPress Chart Plugin	The Chartify - WordPress Chart Plugin plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.9.5 via the 'source' parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.	2024-11-14	9.8	CVE-2024-10571
Baxter--Life2000 Ventilation System	The software tools used by service personnel to test & calibrate the ventilator do not support user authentication. An attacker with access to the Service PC where the tools are installed could obtain diagnostic information through the test tool or manipulate the ventilator's settings and embedded software via the calibration tool, without having to authenticate to either tool. This could result in unauthorized disclosure of information and/or have unintended impacts on device settings and performance.	2024-11-14	10	CVE-2024-48966
Baxter--Life2000 Ventilation System	The ventilator and the Service PC lack sufficient audit logging capabilities to allow for detection of malicious activity and subsequent forensic examination. An attacker with access to the ventilator and/or the Service PC could, without detection, make unauthorized changes to ventilator settings that result in	2024-11-14	10	CVE-2024-48967

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthorized disclosure of information and/or have unintended impacts on device performance.			
Baxter--Life2000 Ventilation System	The ventilator's microcontroller lacks memory protection. An attacker could connect to the internal JTAG interface and read or write to flash memory using an off-the-shelf debugging tool, which could disrupt the function of the device and/or cause unauthorized information disclosure.	2024-11-14	9.3	CVE-2024-48970
Baxter--Life2000 Ventilation System	The Clinician Password and Serial Number Clinician Password are hard-coded into the ventilator in plaintext form. This could allow an attacker to obtain the password off the ventilator and use it to gain unauthorized access to the device, with clinician privileges.	2024-11-14	9.3	CVE-2024-48971
Baxter--Life2000 Ventilation System	The debug port on the ventilator's serial interface is enabled by default. This could allow an attacker to send and receive messages over the debug port (which are unencrypted; see 3.2.1) that result in unauthorized disclosure of information and/or have unintended impacts on device settings and performance.	2024-11-14	9.3	CVE-2024-48973
Baxter--Life2000 Ventilation System	The ventilator does not perform proper file integrity checks when adopting firmware updates. This makes it possible for an attacker to force unauthorized changes to the device's configuration settings and/or compromise device functionality by pushing a compromised/illegitimate firmware file. This could disrupt the function of the device and/or cause unauthorized information disclosure.	2024-11-14	9.3	CVE-2024-48974
Baxter--Life2000 Ventilation System	There is no limit on the number of failed login attempts permitted with the Clinician Password or the Serial Number Clinician Password. An attacker could execute a brute-force attack to gain unauthorized access to the ventilator, and then make changes to device settings that could disrupt the function of the device and/or result in unauthorized information disclosure.	2024-11-14	9.3	CVE-2024-9832
Baxter--Life2000 Ventilation System	Improper data protection on the ventilator's serial interface could allow an attacker to send and receive messages that result in unauthorized disclosure of information and/or have unintended impacts on device settings and performance.	2024-11-14	9.3	CVE-2024-9834
BdThemes--Instant Image Generator	Unrestricted Upload of File with Dangerous Type vulnerability in BdThemes Instant Image Generator allows Upload a Web Shell to a Web Server.This issue affects Instant Image Generator: from n/a through 1.5.4.	2024-11-14	10	CVE-2024-52377
Bigfive--CF7 Reply Manager	Unrestricted Upload of File with Dangerous Type vulnerability in Bigfive CF7 Reply Manager.This issue affects CF7 Reply Manager: from n/a through 1.2.3.	2024-11-16	9.9	CVE-2024-52404
Bikram Joshi--B-Banner Slider	Unrestricted Upload of File with Dangerous Type vulnerability in Bikram Joshi B-Banner Slider allows Upload a Web Shell to a Web Server.This issue affects B-Banner Slider: from n/a through 1.1.	2024-11-16	9.9	CVE-2024-52405
BlackBerry--SecuSUITE	A code injection vulnerability in the SecuSUITE Server Web Administration Portal of SecuSUITE versions 5.0.420 and earlier could allow an attacker to potentially inject script commands or other executable content into the server that would run with root privilege.	2024-11-12	7.3	CVE-2024-51721
Boa web server--Boa web server 0.94.14rc21	Boa web server - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	2024-11-14	7.5	CVE-2024-47916
Bosch Rexroth AG--IndraDrive FWA-INDRV*-MP*	A vulnerability in the PROFINET stack implementation of the IndraDrive (all versions) of Bosch Rexroth allows an attacker to cause a denial of service, rendering the device unresponsive by sending arbitrary UDP messages.	2024-11-13	7.5	CVE-2024-48989
Ciprian Popescu--W3P SEO	Cross-Site Request Forgery (CSRF) vulnerability in Ciprian Popescu W3P SEO allows Stored XSS.This issue affects W3P SEO: from n/a before 1.8.6.	2024-11-14	7.1	CVE-2024-51684
Cisco--Cisco BroadWorks	A vulnerability in the local interface of Cisco BroadWorks Network Server could allow an unauthenticated, remote attacker to exhaust system resources, causing a denial of service (DoS) condition. This vulnerability exists because rate limiting does not occur for certain incoming TCP connections. An attacker could exploit this vulnerability by sending a high rate of TCP connections to the server. A successful exploit could allow the attacker to cause TCP connection resources to grow rapidly until the Cisco BroadWorks Network Server becomes unusable. Note: To recover from this vulnerability, either Cisco BroadWorks Network Server software must be restarted or the Cisco BroadWorks Network Server node must be rebooted. For more information, see the section of this advisory.	2024-11-15	8.6	CVE-2023-20125

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.			
Cisco--Cisco Cyber Vision	A vulnerability in the Modbus preprocessor of the Snort detection engine could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to an integer overflow while processing Modbus traffic. An attacker could exploit this vulnerability by sending crafted Modbus traffic through an affected device. A successful exploit could allow the attacker to cause the Snort process to hang, causing traffic inspection to stop.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	7.5	CVE-2022-20685
Cisco--Cisco Industrial Network Director	A vulnerability in the web UI of Cisco IND could allow an authenticated, remote attacker to execute arbitrary commands with administrative privileges on the underlying operating system of an affected device. This vulnerability is due to improper input validation when uploading a Device Pack. An attacker could exploit this vulnerability by altering the request that is sent when uploading a Device Pack. A successful exploit could allow the attacker to execute arbitrary commands as NT AUTHORITY\SYSTEM on the underlying operating system of an affected device. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	9.9	CVE-2023-20036
Cisco--Cisco IOS XR Software	A vulnerability in the implementation of the CLI on a device that is running ConfD could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient validation of a process argument on an affected device. An attacker could exploit this vulnerability by injecting commands during the execution of this process. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privilege level of ConfD, which is commonly root.	2024-11-15	8.8	CVE-2022-20655
Cisco--Cisco Modeling Labs	A vulnerability in the external authentication mechanism of Cisco Modeling Labs could allow an unauthenticated, remote attacker to access the web interface with administrative privileges. This vulnerability is due to the improper handling of certain messages that are returned by the associated external authentication server. An attacker could exploit this vulnerability by logging in to the web interface of an affected server. Under certain conditions, the authentication mechanism would be bypassed and the attacker would be logged in as an administrator. A successful exploit could allow the attacker to obtain administrative privileges on the web interface of an affected server, including the ability to access and modify every simulation and all user-created data. To exploit this vulnerability, the attacker would need valid user credentials that are stored on the associated external authentication server. Cisco has released software updates that address this vulnerability. There are workarounds that address this vulnerability.	2024-11-15	9.1	CVE-2023-20154
Cisco--Cisco Redundancy Configuration Manager	A vulnerability in Cisco RCM for Cisco StarOS Software could allow an unauthenticated, remote attacker to perform remote code execution on the application with root-level privileges in the context of the configured container. This vulnerability exists because the debug mode is incorrectly enabled for specific services. An attacker could exploit this vulnerability by connecting to the device and navigating to the service with debug mode enabled. A successful exploit could allow the attacker to execute arbitrary commands as the root user. The attacker would need to perform detailed reconnaissance to allow for unauthenticated access. The vulnerability can also be exploited by an authenticated attacker. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	8.1	CVE-2022-20649
Cisco--Cisco TelePresence Video Communication Server (VCS) Expressway	A vulnerability in the certificate validation of Cisco Expressway-C and Cisco TelePresence VCS could allow an unauthenticated, remote attacker to gain unauthorized access to sensitive data. The vulnerability is due to a lack of validation of the SSL server certificate that an affected device receives when it establishes a connection to a Cisco Unified Communications Manager device. An attacker could exploit this vulnerability by using a man-in-the-middle technique to intercept the traffic between the devices, and then using a	2024-11-15	7.4	CVE-2022-20814

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	self-signed certificate to impersonate the endpoint. A successful exploit could allow the attacker to view the intercepted traffic in clear text or alter the contents of the traffic. Note: Cisco Expressway-E is not affected by this vulnerability.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.			
Cisco--Cisco TelePresence Video Communication Server (VCS) Expressway	A vulnerability in the REST API of Cisco Expressway Series and Cisco TelePresence VCS could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected system. An attacker could exploit this vulnerability by persuading a user of the REST API to follow a crafted link. A successful exploit could allow the attacker to cause the affected system to reload. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	7.4	CVE-2022-20853
Citrix Session Recording--Citrix Session Recording	Limited remote code execution with privilege of a NetworkService Account accessÂ inÂ Citrix Session Recording if the attacker is an authenticated user on the same intranet as the session recording server	2024-11-12	8.8	CVE-2024-8069
Clarisse K.--Writer Helper	Unrestricted Upload of File with Dangerous Type vulnerability in Clarisse K. Writer Helper allows Upload a Web Shell to a Web Server.This issue affects Writer Helper: from n/a through 3.1.6.	2024-11-16	9.9	CVE-2024-52399
cli--cli	The GitHub CLI version 2.6.1 and earlier are vulnerable to remote code execution through a malicious codespace SSH server when using `gh codespace ssh` or `gh codespace logs` commands. This has been patched in the cli v2.62.0. Developers connect to remote codespaces through an SSH server running within the devcontainer, which is generally provided through the [default devcontainer image](https://docs.github.com/en/codespaces/setting-up-your-project-for-codespaces/adding-a-dev-container-... https://docs.github.com/en/codespaces/setting-up-your-project-for-codespaces/adding-a-dev-container-configuration/introduction-to-dev-containers#using-the-default-dev-container-configuration) . GitHub CLI [retrieves SSH connection details](https://github.com/cli/cli/blob/30066b0042d0c5928d959e288144300cb28196c9/internal/codespaces/rpc/inv... https://github.com/cli/cli/blob/30066b0042d0c5928d959e288144300cb28196c9/internal/codespaces/rpc/invoker.go#L230-L244), such as remote username, which is used in [executing `ssh` commands](https://github.com/cli/cli/blob/e356c69a6f0125cfaac782c35acf77314f18908d/pkg/cmd/codespace/ssh.go#L2... https://github.com/cli/cli/blob/e356c69a6f0125cfaac782c35acf77314f18908d/pkg/cmd/codespace/ssh.go#L263) for `gh codespace ssh` or `gh codespace logs` commands. This exploit occurs when a malicious third-party devcontainer contains a modified SSH server that injects `ssh` arguments within the SSH connection details. `gh codespace ssh` and `gh codespace logs` commands could execute arbitrary code on the user's workstation if the remote username contains something like `-oProxyCommand="echo hacked" #`. The `-oProxyCommand` flag causes `ssh` to execute the provided command while `#` shell comment causes any other `ssh` arguments to be ignored. In `2.62.0`, the remote username information is being validated before being used.	2024-11-14	8	CVE-2024-52308
cmorillas1--External Database Based Actions	The External Database Based Actions plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 0.1. This is due to a missing capability check in the 'edba_admin_handle' function. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to update the plugin settings and log in as any existing user on the site, such as an administrator.	2024-11-15	7.5	CVE-2024-10311
cmsMinds--Boat Rental Plugin for WordPress	Unrestricted Upload of File with Dangerous Type vulnerability in cmsMinds Boat Rental Plugin for WordPress allows Upload a Web Shell to a Web Server.This issue affects Boat Rental Plugin for WordPress: from n/a through 1.0.1.	2024-11-14	10	CVE-2024-52376

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects--Job Recruitment	A vulnerability was found in code-projects Job Recruitment 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file reset.php. The manipulation of the argument e leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-15	7.3	CVE-2024-11241
codeSavory--BasePress Migration Tools	Unrestricted Upload of File with Dangerous Type vulnerability in codeSavory BasePress Migration Tools allows Upload a Web Shell to a Web Server.This issue affects BasePress Migration Tools: from n/a through 1.0.0.	2024-11-16	9.9	CVE-2024-52407
craftcms--cms	Craft is a content management system (CMS). A vulnerability in CraftCMS allows an attacker to bypass local file system validation by utilizing a double file:// scheme (e.g., file://file:////). This enables the attacker to specify sensitive folders as the file system, leading to potential file overwriting through malicious uploads, unauthorized access to sensitive files, and, under certain conditions, remote code execution (RCE) via Server-Side Template Injection (SSTI) payloads. Note that this will only work if you have an authenticated administrator account with allowAdminChanges enabled. This is fixed in 5.4.6 and 4.12.5.	2024-11-13	8.4	CVE-2024-52291
craftcms--cms	Craft is a content management system (CMS). The dataUrl function can be exploited if an attacker has write permissions on system notification templates. This function accepts an absolute file path, reads the file's content, and converts it into a Base64-encoded string. By embedding this function within a system notification template, the attacker can exfiltrate the Base64-encoded file content through a triggered system email notification. Once the email is received, the Base64 payload can be decoded, allowing the attacker to read arbitrary files on the server. This is fixed in 5.4.9 and 4.12.8.	2024-11-13	7.7	CVE-2024-52292
craftcms--cms	Craft is a content management system (CMS). Prior to 4.12.2 and 5.4.3, Craft is missing normalizePath in the function FileHelper::absolutePath could lead to Remote Code Execution on the server via twig SSTI. This is a sequel to CVE-2023-40035. This vulnerability is fixed in 4.12.2 and 5.4.3.	2024-11-13	7.2	CVE-2024-52293
creativeinteractivemedia--Real3D Flipbook Lite 3D FlipBook, PDF Viewer, PDF Embedder	The 3D FlipBook, PDF Viewer, PDF Embedder - Real 3D FlipBook WordPress Plugin plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'r3dfb_save_thumbnail_callback' function in all versions up to, and including, 4.6. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-11-16	8.8	CVE-2024-9849
cyberlord92--Login using WordPress Users (WP as SAML IDP)	The Login using WordPress Users (WP as SAML IDP) plugin for WordPress is vulnerable to time-based SQL Injection via the 'id' parameter in all versions up to, and including, 1.15.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-11-16	7.2	CVE-2024-9887
Dang Ngoc Binh--Audio Record	Unrestricted Upload of File with Dangerous Type vulnerability in Dang Ngoc Binh Audio Record allows Upload a Web Shell to a Web Server.This issue affects Audio Record: from n/a through 1.0.	2024-11-11	10	CVE-2024-51792
Davor Zeljkovic--Convert Docx2post	Unrestricted Upload of File with Dangerous Type vulnerability in Davor Zeljkovic Convert Docx2post allows Upload a Web Shell to a Web Server.This issue affects Convert Docx2post: from n/a through 1.4.	2024-11-16	9.1	CVE-2024-52397
decidim--decidim	Decidim is a participatory democracy framework. The meeting embeds feature used in the online or hybrid meetings is subject to potential XSS attack through a malformed URL. This vulnerability is fixed in 0.28.3 and 0.29.0.	2024-11-13	7.7	CVE-2024-45594
decidim-ice--decidim-module-decidim_awesome	An improper neutralization of special elements used in an SQL command in the papertrail/version- model of the decidim_awesome-module <= v0.11.1 (> 0.9.0) allows an authenticated admin user to manipulate sql queries to disclose information, read and write files or execute commands.	2024-11-12	9	CVE-2024-43415
dell --smartfabric_os10	Dell SmartFabric OS10 Software, version(s) 10.5.6.x, 10.5.5.x, 10.5.4.x, 10.5.3.x, contain(s) an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2024-11-12	7.8	CVE-2024-49557
dell --smartfabric_os10	Dell SmartFabric OS10 Software, version(s) 10.5.6.x, 10.5.5.x, 10.5.4.x, 10.5.3.x, contain(s) an Improper Privilege Management vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2024-11-12	7.8	CVE-2024-49558

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- smartfabric_os10	Dell SmartFabric OS10 Software, version(s) 10.5.6.x, 10.5.5.x, 10.5.4.x, 10.5.3.x, contain(s) a command injection vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution.	2024-11-12	7.8	CVE-2024-49560
Dell--SmartFabric OS10 Software	Dell SmartFabric OS10 Software, version(s) 10.5.6.x, 10.5.5.x, 10.5.4.x, 10.5.3.x, contain(s) an Execution with Unnecessary Privileges vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution	2024-11-12	7.8	CVE-2024-48837
Delta Electronics--DIAScreen	If an attacker tricks a valid user into running Delta Electronics DIAScreen with a file containing malicious code, a stack-based buffer overflow in CEtherIPTagItem can be exploited, allowing the attacker to remotely execute arbitrary code.	2024-11-11	7.8	CVE-2024-39354
Delta Electronics--DIAScreen	If an attacker tricks a valid user into running Delta Electronics DIAScreen with a file containing malicious code, a stack-based buffer overflow in BACnetParameter can be exploited, allowing the attacker to remotely execute arbitrary code.	2024-11-11	7.8	CVE-2024-39605
Delta Electronics--DIAScreen	If an attacker tricks a valid user into running Delta Electronics DIAScreen with a file containing malicious code, a stack-based buffer overflow in BACnetObjectInfo can be exploited, allowing the attacker to remotely execute arbitrary code.	2024-11-11	7.8	CVE-2024-47131
dlink -- dsl6740c_firmware	The D-Link DSL6740C modem has an Incorrect Use of Privileged APIs vulnerability, allowing unauthenticated remote attackers to modify any user's password by leveraging the API, thereby granting access to Web, SSH, and Telnet services using that user's account.	2024-11-11	9.8	CVE-2024-11068
dlink -- dsl6740c_firmware	The D-Link DSL6740C modem has an OS Command Injection vulnerability, allowing remote attackers with administrator privileges to inject and execute arbitrary system commands through a specific functionality provided by SSH and Telnet.	2024-11-11	7.2	CVE-2024-11062
dlink -- dsl6740c_firmware	The D-Link DSL6740C modem has an OS Command Injection vulnerability, allowing remote attackers with administrator privileges to inject and execute arbitrary system commands through a specific functionality provided by SSH and Telnet.	2024-11-11	7.2	CVE-2024-11063
dlink -- dsl6740c_firmware	The D-Link DSL6740C modem has an OS Command Injection vulnerability, allowing remote attackers with administrator privileges to inject and execute arbitrary system commands through a specific functionality provided by SSH and Telnet.	2024-11-11	7.2	CVE-2024-11064
dlink -- dsl6740c_firmware	The D-Link DSL6740C modem has an OS Command Injection vulnerability, allowing remote attackers with administrator privileges to inject and execute arbitrary system commands through a specific functionality provided by SSH and Telnet.	2024-11-11	7.2	CVE-2024-11065
dlink -- dsl6740c_firmware	The D-Link DSL6740C modem has an OS Command Injection vulnerability, allowing remote attackers with administrator privileges to inject and execute arbitrary system commands through the specific web page.	2024-11-11	7.2	CVE-2024-11066
dlink -- dsl6740c_firmware	The D-Link DSL6740C modem has a Path Traversal Vulnerability, allowing unauthenticated remote attackers to exploit this vulnerability to read arbitrary system files. Additionally, since the device's default password is a combination of the MAC address, attackers can obtain the MAC address through this vulnerability and attempt to log in to the device using the default password.	2024-11-11	7.5	CVE-2024-11067
DMC--Airin Blog	Deserialization of Untrusted Data vulnerability in DMC Airin Blog allows Object Injection.This issue affects Airin Blog: from n/a through 1.6.1.	2024-11-16	9.8	CVE-2024-52413
DonnellC--Global Gateway e4 | Payeezy Gateway	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in DonnellC Global Gateway e4 | Payeezy Gateway.This issue affects Global Gateway e4 | Payeezy Gateway: from n/a through 2.0.	2024-11-14	8.6	CVE-2024-52371
DoThatTask--Do That Task	Unrestricted Upload of File with Dangerous Type vulnerability in DoThatTask Do That Task allows Upload a Web Shell to a Web Server.This issue affects Do That Task: from n/a through 1.5.5.	2024-11-14	10	CVE-2024-52374
dotnetzip.semverd_project -- dotnetzip.semverd	Directory Traversal vulnerability in DotNetZip v.1.16.0 and before allows a remote attacker to execute arbitrary code via the src/Zip.Shared/ZipEntry.Extract.cs component NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2024-11-13	9.8	CVE-2024-48510
Elastic--Kibana	A deserialization issue in Kibana can lead to arbitrary code execution when Kibana attempts to parse a YAML document containing a crafted payload. A successful attack requires a malicious user to have a combination of both specific Elasticsearch indices privileges https://www.elastic.co/guide/en/elasticsearch/reference/current/defining-roles.html#roles-indices-priv Â and Kibana privileges https://www.elastic.co/guide/en/fleet/current/fleet-roles-and-privileges.html Â assigned to them. The following Elasticsearch indices permissions are required * writeÂ privilege on the system indices .kibana_ingest* * The allow_restricted_indicesÂ flag is set to true	2024-11-14	9.1	CVE-2024-37285

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Any of the following Kibana privileges are additionally required * Under FleetÂ the AllÂ privilege is granted * Under IntegrationÂ the ReadÂ or AllÂ privilege is granted * Access to the fleet-setupÂ privilege is gained through the Fleet Server's service account token			
Eugen Bobrowski--Debug Tool	Missing Authorization vulnerability in Eugen Bobrowski Debug Tool allows Upload a Web Shell to a Web Server.This issue affects Debug Tool: from n/a through 2.2.	2024-11-16	10	CVE-2024-52416
Flowcraft UX Design Studio--Advanced Personalization	Deserialization of Untrusted Data vulnerability in Flowcraft UX Design Studio Advanced Personalization allows Object Injection.This issue affects Advanced Personalization: from n/a through 1.1.2.	2024-11-16	9.8	CVE-2024-52411
fortinet --forticlient	A privilege context switching error vulnerability [CWE-270] in FortiClient Windows version 7.2.4 and below, version 7.0.12 and below, 6.4 all versions may allow an authenticated user to escalate their privileges via lua auto patch scripts.	2024-11-12	8.8	CVE-2024-36513
fortinet --forticlient	A untrusted search path in Fortinet FortiClientWindows versions 7.4.0, versions 7.2.4 through 7.2.0, versions 7.0.12 through 7.0.0 allows an attacker to run arbitrary code via DLL hijacking and social engineering.	2024-11-12	7.8	CVE-2024-36507
Fortinet--FortiClientWindows	A authentication bypass using an alternate path or channel in Fortinet FortiClientWindows version 7.4.0, versions 7.2.4 through 7.2.0, versions 7.0.12 through 7.0.0, and 6.4.10 through 6.4.0 allows low privilege attacker to execute arbitrary code with high privilege via spoofed named pipe messages.	2024-11-13	7.8	CVE-2024-47574
Fortinet--FortiManager	A client-side enforcement of server-side security in Fortinet FortiAnalyzer-BigData at least version 7.4.0 and 7.2.0 through 7.2.6 and 7.0.1 through 7.0.6 and 6.4.5 through 6.4.7 and 6.2.5, FortiManager version 7.4.0 through 7.4.1 and 7.2.0 through 7.2.4 and 7.0.0 through 7.0.11 and 6.4.0 through 6.4.14, FortiAnalyzer version 7.4.0 through 7.4.1 and 7.2.0 through 7.2.4 and 7.0.0 through 7.0.11 and 6.4.0 through 6.4.14 allows attacker to improper access control via crafted requests.	2024-11-12	7.5	CVE-2024-23666
Fortinet--FortiOS	A session fixation in Fortinet FortiOS version 7.4.0 through 7.4.3 and 7.2.0 through 7.2.7 and 7.0.0 through 7.0.13 allows attacker to execute unauthorized code or commands via phishing SAML authentication link.	2024-11-12	7.5	CVE-2023-50176
FraudLabs Pro--FraudLabs Pro SMS Verification	Cross-Site Request Forgery (CSRF) vulnerability in FraudLabs Pro FraudLabs Pro SMS Verification allows Stored XSS.This issue affects FraudLabs Pro SMS Verification: from n/a through 1.10.1.	2024-11-14	7.1	CVE-2024-51688
FreeBSD--FreeBSD	The fetch(3) library uses environment variables for passing certain information, including the revocation file pathname. The environment variable name used by fetch(1) to pass the filename to the library was incorrect, in effect ignoring the option. Fetch would still connect to a host presenting a certificate included in the revocation file passed to the --crl option.	2024-11-12	7.5	CVE-2024-45289
GeekRMX--Twitter @Anywhere Plus	Cross-Site Request Forgery (CSRF) vulnerability in GeekRMX Twitter @Anywhere Plus allows Stored XSS.This issue affects Twitter @Anywhere Plus: from n/a through 2.0.	2024-11-14	7.1	CVE-2024-51659
GentleSource--Appointmind	Cross-Site Request Forgery (CSRF) vulnerability in GentleSource Appointmind allows Stored XSS.This issue affects Appointmind: from n/a through 4.0.0.	2024-11-14	7.1	CVE-2024-51679
GeoVision--GV-VS12	Certain EOL GeoVision devices have an OS Command Injection vulnerability. Unauthenticated remote attackers can exploit this vulnerability to inject and execute arbitrary system commands on the device. Moreover, this vulnerability has already been exploited by attackers, and we have received related reports.	2024-11-15	9.8	CVE-2024-11120
GitLab--GitLab	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.0 prior to 17.3.7, starting from 17.4 prior to 17.4.4, and starting from 17.5 prior to 17.5.2, which could have allowed unauthorized access to the Kubernetes agent in a cluster under specific configurations.	2024-11-14	8.5	CVE-2024-9693
glpi-project--glpi	GLPI is a free asset and IT management software package. An authenticated user can exploit multiple SQL injection vulnerabilities. One of them can be used to alter another user account data and take control of it. Upgrade to 10.0.17.	2024-11-15	8.1	CVE-2024-40638
gogs--gogs/gogs	A remote command execution vulnerability exists in gogs/gogs versions <=0.12.7 when deployed on a Windows server. The vulnerability arises due to improper validation of the `tree_path` parameter during file uploads. An attacker can set `tree_path=.git.` to upload a file into the .git directory, allowing them to write or	2024-11-15	10	CVE-2022-1884

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	rewrite the `.git/config` file. If the `core.sshCommand` is set, this can lead to remote command execution.			
google -- android	In shouldHideDocument of ExternalStorageProvider.java, there is a possible bypass of a file path filter designed to prevent access to sensitive directories due to incorrect unicode normalization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-13	7.8	CVE-2024-43093
Google--Android	In PVRSRVRGXKickTA3DKM of rgxta3d.c, there is a possible arbitrary code execution due to improper input validation. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	8.4	CVE-2024-31337
Google--Android	In multiple locations, there is a possible permissions bypass due to a missing null check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	8.4	CVE-2024-34719
Google--Android	In multiple locations, there is a possible arbitrary code execution due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	8.4	CVE-2024-34729
Google--Android	In DevmemXIntMapPages of devicemem_server.c, there is a possible use-after-free due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	8.4	CVE-2024-34747
Google--Android	In getInstalledAccessibilityPreferences of AccessibilitySettings.java, there is a possible way to hide an enabled accessibility service in the accessibility service settings due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-13	8.4	CVE-2024-43087
Google--Android	In multiple functions in AppInfoBase.java, there is a possible way to manipulate app permission settings belonging to another user on the device due to a missing permission check. This could lead to local escalation of privilege across user boundaries with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	8.4	CVE-2024-43088
Google--Android	In filterMask of SkEmbossMaskFilter.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	8.8	CVE-2024-43091
Google--Android	In setTransactionState of SurfaceFlinger.cpp, there is a possible way to change protected display attributes due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	7.8	CVE-2024-40660
Google--Android	In mayAdminGrantPermission of AdminRestrictedPermissionsUtils.java, there is a possible way to access the microphone due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	7.8	CVE-2024-40661
Google--Android	In DevmemIntChangeSparse2 of devicemem_server.c, there is a possible way to achieve arbitrary code execution due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	7.8	CVE-2024-40671
Google--Android	In onReceive of AppRestrictionsFragment.java, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-13	7.8	CVE-2024-43080
Google--Android	In installExistingPackageAsUser of InstallPackageHelper.java, there is a possible carrier restriction bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	7.8	CVE-2024-43081
Google--Android	In handleMessage of UsbDeviceManager.java, there is a possible method to access device contents over USB without unlocking the device due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	7.8	CVE-2024-43085
Google--Android	In updateInternal of MediaProvider.java , there is a possible access of another app's files due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	7.8	CVE-2024-43089

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Google--Chrome	Use after free in Accessibility in Google Chrome prior to 131.0.6778.69 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2024-11-12	8.8	CVE-2024-11113
Google--Chrome	Inappropriate implementation in Views in Google Chrome on Windows prior to 131.0.6778.69 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2024-11-12	8.3	CVE-2024-11114
Google--Chrome	Insufficient policy enforcement in Navigation in Google Chrome on iOS prior to 131.0.6778.69 allowed a remote attacker to perform privilege escalation via a series of UI gestures. (Chromium security severity: Medium)	2024-11-12	8.8	CVE-2024-11115
Google--Chrome	Use after free in Media in Google Chrome on Windows prior to 131.0.6778.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2024-11-12	7.5	CVE-2024-11112
Grand Vice info--Webopac	Webopac from Grand Vice info does not properly validate uploaded file types, allowing unauthenticated remote attackers to upload and execute webshells, which could lead to arbitrary code execution on the server.	2024-11-11	9.8	CVE-2024-11018
Grand Vice info--Webopac	Webopac from Grand Vice info does not properly validate uploaded file types, allowing remote attackers with regular privileges to upload and execute webshells, which could lead to arbitrary code execution on the server.	2024-11-11	8.8	CVE-2024-11017
Grand Vice info--Webopac7	Webopac from Grand Vice info has a SQL Injection vulnerability, allowing unauthenticated remote attacks to inject arbitrary SQL commands to read, modify, and delete database contents.	2024-11-11	9.8	CVE-2024-11020
Halyra--CDI	Unrestricted Upload of File with Dangerous Type vulnerability in Halyra CDI.This issue affects CDI: from n/a through 5.5.3.	2024-11-16	9.1	CVE-2024-52398
Henrik Hoff--WP Course Manager	Cross-Site Request Forgery (CSRF) vulnerability in Henrik Hoff WP Course Manager allows Stored XSS.This issue affects WP Course Manager: from n/a through 1.3.	2024-11-14	7.1	CVE-2024-51658
Hive Support--Hive Support WordPress Help Desk	Unrestricted Upload of File with Dangerous Type vulnerability in Hive Support Hive Support - WordPress Help Desk allows Upload a Web Shell to a Web Server.This issue affects Hive Support - WordPress Help Desk: from n/a through 1.1.1.	2024-11-14	9.9	CVE-2024-52370
ibm -- soar	IBM Security SOAR 51.0.1.0 and earlier contains a mechanism for users to recover or change their passwords without knowing the original password, but the user account must be compromised prior to the weak recovery mechanism.	2024-11-14	8.1	CVE-2024-45670
IBM--Engineering Insights	IBM Engineering Lifecycle Optimization - Engineering Insights 7.0.2 and 7.0.3 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	2024-11-15	8.2	CVE-2024-39726
IBM--Sterling Secure Proxy	IBM Sterling Secure Proxy 6.0.0.0, 6.0.0.1, 6.0.0.2, 6.0.0.3, and 6.1.0.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot dot" sequences (/.../) to view arbitrary files on the system.	2024-11-15	7.5	CVE-2024-41784
icdsoft--MultiManager WP Manage All Your WordPress Sites Easily	The MultiManager WP - Manage All Your WordPress Sites Easily plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.0.5. This is due to the user impersonation feature inappropriately determining the current user via user-supplied input. This makes it possible for unauthenticated attackers to generate an impersonation link that will allow them to log in as any existing user, such as an administrator. NOTE: The user impersonation feature was disabled in version 1.1.0 and re-enabled with a patch in version 1.1.2.	2024-11-13	9.8	CVE-2024-11028
Icinga--icinga2	Icinga is a monitoring system which checks the availability of network resources, notifies users of outages, and generates performance data for reporting. The TLS certificate validation in all Icinga 2 versions starting from 2.4.0 was flawed, allowing an attacker to impersonate both trusted cluster nodes as well as any API users that use TLS client certificates for authentication (ApiUser objects with the client_cn attribute set). This vulnerability has been fixed in v2.14.3, v2.13.10, v2.12.11, and v2.11.12.	2024-11-12	9.8	CVE-2024-49369
ivanti -- avalanche	A null pointer dereference in Ivanti Avalanche before 6.4.6 allows a remote unauthenticated attacker to cause a denial of service.	2024-11-12	7.5	CVE-2024-50317
ivanti -- avalanche	A null pointer dereference in Ivanti Avalanche before 6.4.6 allows a remote unauthenticated attacker to cause a denial of service.	2024-11-12	7.5	CVE-2024-50318
ivanti -- avalanche	An infinite loop in Ivanti Avalanche before 6.4.6 allows a remote unauthenticated attacker to cause a denial of service.	2024-11-12	7.5	CVE-2024-50319

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ivanti -- avalanche	An infinite loop in Ivanti Avalanche before 6.4.6 allows a remote unauthenticated attacker to cause a denial of service.	2024-11-12	7.5	CVE-2024-50320
ivanti -- avalanche	An infinite loop in Ivanti Avalanche before 6.4.6 allows a remote unauthenticated attacker to cause a denial of service.	2024-11-12	7.5	CVE-2024-50321
ivanti -- connect_secure	Command injection in Ivanti Connect Secure before version 22.7R2.1 and Ivanti Policy Secure before version 22.7R1.1 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-11-12	7.2	CVE-2024-11007
ivanti -- connect_secure	A stack-based buffer overflow in IPsec of Ivanti Connect Secure before version 22.7R2.3 allows a remote unauthenticated attacker to cause a denial of service.	2024-11-12	7.5	CVE-2024-47907
Ivanti--Avalanche	An out-of-bounds read vulnerability in Ivanti Avalanche before 6.4.6 allows a remote unauthenticated attacker to leak sensitive information in memory.	2024-11-12	7.5	CVE-2024-50331
Ivanti--Connect Secure	Command injection in Ivanti Connect Secure before version 22.7R2.1 and Ivanti Policy Secure before version 22.7R1.1 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-11-12	9.1	CVE-2024-11005
Ivanti--Connect Secure	Command injection in Ivanti Connect Secure before version 22.7R2.1 and Ivanti Policy Secure before version 22.7R1.1 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-11-12	9.1	CVE-2024-11006
Ivanti--Connect Secure	Argument injection in Ivanti Connect Secure before version 22.7R2.2 and 9.1R18.9 and Ivanti Policy Secure before version 22.7R1.2 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-11-13	9.1	CVE-2024-38656
Ivanti--Connect Secure	Reflected XSS in Ivanti Connect Secure before version 22.7R2.1 and Ivanti Policy Secure before version 22.7R1.1 allows a remote unauthenticated attacker to obtain admin privileges. User interaction is required.	2024-11-12	8.4	CVE-2024-11004
Ivanti--Connect Secure	A use-after-free in Ivanti Connect Secure before version 22.7R2.3 and Ivanti Policy Secure before version 22.7R1.2 allows a remote authenticated attacker to achieve remote code execution.	2024-11-12	8.8	CVE-2024-9420
Ivanti--Connect Secure	Incorrect file permissions in Ivanti Connect Secure before version 22.6R2 and Ivanti Policy Secure before version 22.6R1 allow a local authenticated attacker to escalate their privileges.	2024-11-13	7.8	CVE-2024-39709
Ivanti--Connect Secure	Excessive binary privileges in Ivanti Connect Secure which affects versions 22.4R2 through 22.7R2.2 inclusive within the R2 release line and Ivanti Policy Secure before version 22.7R1.2 allow a local authenticated attacker to escalate privileges.	2024-11-12	7.8	CVE-2024-47906
Ivanti--Connect Secure	A null pointer dereference in Ivanti Connect Secure before version 22.7R2.1 and Ivanti Policy Secure before version 22.7R1.1 allows a remote unauthenticated attacker to cause a denial of service.	2024-11-12	7.5	CVE-2024-8495
Ivanti--Endpoint Manager	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security UpdateÂ allows a remote unauthenticated attacker to achieve remote code execution.	2024-11-12	9.8	CVE-2024-50330
Ivanti--Endpoint Manager	Path traversal in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security UpdateÂ allows a remote unauthenticated attacker to achieve remote code execution. User interaction is required.	2024-11-12	8.8	CVE-2024-50329
Ivanti--Endpoint Manager	Path traversal in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security UpdateÂ allows a local unauthenticated attacker to achieve code execution. User interaction is required.	2024-11-12	7.8	CVE-2024-50322
Ivanti--Endpoint Manager	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security UpdateÂ allows a local unauthenticated attacker to achieve code execution. User interaction is required.	2024-11-12	7.8	CVE-2024-50323
Ivanti--Endpoint Manager	Path traversal in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security UpdateÂ allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-11-12	7.2	CVE-2024-50324
Ivanti--Endpoint Manager	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security UpdateÂ allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-11-12	7.2	CVE-2024-50326
Ivanti--Endpoint Manager	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security UpdateÂ allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-11-12	7.2	CVE-2024-50327
Ivanti--Endpoint Manager	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security UpdateÂ allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-11-12	7.2	CVE-2024-50328
Ivanti--EPM	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2024-11-13	7.2	CVE-2024-32844

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Ivanti--Secure Access Client	Incorrect permissions in Ivanti Secure Access Client before 22.7R4 allows a local authenticated attacker to escalate their privileges.	2024-11-12	7.8	CVE-2024-7571
Ivanti--Secure Access Client	Improper authorization in Ivanti Secure Access Client before version 22.7R3 allows a local authenticated attacker to modify sensitive configuration files.	2024-11-12	7.1	CVE-2024-8539
Ivanti--Secure Access Client	Incorrect permissions in Ivanti Secure Access Client before version 22.7R4 allows a local authenticated attacker to create arbitrary folders.	2024-11-12	7.3	CVE-2024-9842
Jenkins Project--Jenkins Authorize Project Plugin	Jenkins Authorize Project Plugin 1.7.2 and earlier evaluates a string containing the job name with JavaScript on the Authorization view, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	2024-11-13	8	CVE-2024-52552
Jenkins Project--Jenkins OpenId Connect Authentication Plugin	Jenkins OpenId Connect Authentication Plugin 4.418.vccc7061f5b_6d and earlier does not invalidate the previous session on login.	2024-11-13	8.8	CVE-2024-52553
Jenkins Project--Jenkins Pipeline: Declarative Plugin	Jenkins Pipeline: Declarative Plugin 2.2214.vb_b_34b_2ea_9b_83 and earlier does not check whether the main (Jenkinsfile) script used to restart a build from a specific stage is approved, allowing attackers with Item/Build permission to restart a previous build whose (Jenkinsfile) script is no longer approved.	2024-11-13	8	CVE-2024-52551
Jenkins Project--Jenkins Shared Library Version Override Plugin	Jenkins Shared Library Version Override Plugin 17.v786074c9fce7 and earlier declares folder-scoped library overrides as trusted, so that they're not executed in the Script Security sandbox, allowing attackers with Item/Configure permission on a folder to configure a folder-scoped library override that runs without sandbox protection.	2024-11-13	8.8	CVE-2024-52554
Joshua Wolfe--The Novel Design Store Directory	Unrestricted Upload of File with Dangerous Type vulnerability in Joshua Wolfe The Novel Design Store Directory allows Upload a Web Shell to a Web Server.This issue affects The Novel Design Store Directory: from n/a through 4.3.0.	2024-11-11	10	CVE-2024-51788
kanboard--kanboard	Kanboard is project management software that focuses on the Kanban methodology. An authenticated Kanboard admin can read and delete arbitrary files from the server. File attachments, that are viewable or downloadable in Kanboard are resolved through its `path` entry in the `project_has_files` SQLite db. Thus, an attacker who can upload a modified sqlite.db through the dedicated feature, can set arbitrary file links, by abusing path traversals. Once the modified db is uploaded and the project page is accessed, a file download can be triggered and all files, readable in the context of the Kanboard application permissions, can be downloaded. This issue has been addressed in version 1.2.42 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-11-11	9.1	CVE-2024-51747
kanboard--kanboard	Kanboard is project management software that focuses on the Kanban methodology. An authenticated Kanboard admin can run arbitrary php code on the server in combination with a file write possibility. The user interface language is determined and loaded by the setting `application_language` in the `settings` table. Thus, an attacker who can upload a modified sqlite.db through the dedicated feature, has control over the filepath, which is loaded. Exploiting this vulnerability has one constraint: the attacker must be able to place a file (called translations.php) on the system. However, this is not impossible, think of anonymous FTP server or another application that allows uploading files. Once the attacker has placed its file with the actual php code as the payload, the attacker can craft a sqlite db settings, which uses path traversal to point to the directory, where the `translations.php` file is stored. Then gaining code execution after importing the crafted sqlite.db. This issue has been addressed in version 1.2.42 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-11-11	9.1	CVE-2024-51748
KCT--Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One	Missing Authorization vulnerability in KCT Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One: from n/a through 2.1.2.	2024-11-14	7.5	CVE-2024-52383
Kinetic Innovative Technologies Sdn	Unrestricted Upload of File with Dangerous Type vulnerability in Kinetic Innovative Technologies Sdn Bhd kineticPay for WooCommerce allows Upload a Web Shell to	2024-11-14	10	CVE-2024-52379

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Bhd--kineticPay for WooCommerce	a Web Server.This issue affects kineticPay for WooCommerce: from n/a through 2.0.8.			
Labs64--DigiPass	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Labs64 DigiPass allows Absolute Path Traversal.This issue affects DigiPass: from n/a through 0.3.0.	2024-11-14	7.5	CVE-2024-52378
Laravel-Backpack--FileManager	FileManager provides a Backpack admin interface for files and folder. Prior to 3.0.9, deserialization of untrusted data from the mimes parameter could lead to remote code execution. This vulnerability is fixed in 3.0.9.	2024-11-13	7.6	CVE-2024-52306
laurent22--joplin	Joplin is a free, open source note taking and to-do application. Joplin-desktop has a vulnerability that leads to remote code execution (RCE) when a user clicks on an <a> link within untrusted notes. The issue arises due to insufficient sanitization of <a> tag attributes introduced by the Mermaid. This vulnerability allows the execution of untrusted HTML content within the Electron window, which has full access to Node.js APIs, enabling arbitrary shell command execution.	2024-11-14	7.7	CVE-2024-49362
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the API-Access page allows authenticated users to inject arbitrary JavaScript through the "token" parameter when creating a new API token. This vulnerability can result in the execution of malicious code in the context of other users' sessions, compromising their accounts and enabling unauthorized actions. This vulnerability is fixed in 24.10.0.	2024-11-15	7.5	CVE-2024-49754
Made I.T.--Forms	Unrestricted Upload of File with Dangerous Type vulnerability in Made I.T. Forms allows Upload a Web Shell to a Web Server.This issue affects Forms: from n/a through 2.8.0.	2024-11-11	10	CVE-2024-51791
Medma Technologies--Matix Popup Builder	Missing Authorization vulnerability in Medma Technologies Matix Popup Builder allows Privilege Escalation.This issue affects Matix Popup Builder: from n/a through 1.0.0.	2024-11-14	9.8	CVE-2024-52382
melapress--WP Activity Log	The WP Activity Log plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the user_id parameter in all versions up to, and including, 5.2.1 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 an administrative user accesses an injected page.	2024-11-15	7.2	CVE-2024-10793
microsoft -- 365_apps	Microsoft Excel Remote Code Execution Vulnerability	2024-11-12	7.8	CVE-2024-49026
microsoft -- 365_apps	Microsoft Excel Remote Code Execution Vulnerability	2024-11-12	7.8	CVE-2024-49027
microsoft -- 365_apps	Microsoft Excel Remote Code Execution Vulnerability	2024-11-12	7.8	CVE-2024-49029
microsoft -- 365_apps	Microsoft Excel Remote Code Execution Vulnerability	2024-11-12	7.8	CVE-2024-49030
microsoft -- 365_apps	Microsoft Word Security Feature Bypass Vulnerability	2024-11-12	7.5	CVE-2024-49033
microsoft -- exchange_server	Microsoft Exchange Server Spoofing Vulnerability	2024-11-12	7.5	CVE-2024-49040
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-48994
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-48995
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-48996
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-48997

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-48998
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-48999
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49000
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49001
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49002
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49003
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49004
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49005
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49006
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49007
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49008
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49009
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49010
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49011
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49012
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49013
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49014
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49015
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49016
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49017
microsoft -- sql_server_2016	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49018

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- sql_server_2016	Microsoft SQL Server Remote Code Execution Vulnerability	2024-11-12	7.8	CVE-2024-49021
microsoft -- sql_server_2016	Microsoft.SqlServer.XEvent.Configuration.dll Remote Code Execution Vulnerability	2024-11-12	7.8	CVE-2024-49043
microsoft -- windows_10_1507	Windows Telephony Service Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-43620
microsoft -- windows_10_1507	Windows Telephony Service Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-43621
microsoft -- windows_10_1507	Windows Telephony Service Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-43622
microsoft -- windows_10_1507	Windows Task Scheduler Elevation of Privilege Vulnerability	2024-11-12	8.8	CVE-2024-49039
microsoft -- windows_10_1507	Windows NT OS Kernel Elevation of Privilege Vulnerability	2024-11-12	7.8	CVE-2024-43623
microsoft -- windows_11_22h2	Microsoft Windows VMSwitch Elevation of Privilege Vulnerability	2024-11-12	8.1	CVE-2024-43625
Microsoft-- airlift.microsoft.com	Authentication bypass by assumed-immutable data on airlift.microsoft.com allows an authorized attacker to elevate privileges over a network.	2024-11-12	7.3	CVE-2024-49056
Microsoft--Azure CycleCloud	Azure CycleCloud Remote Code Execution Vulnerability	2024-11-12	9.9	CVE-2024-43602
Microsoft--Azure Database for PostgreSQL Flexible Server	Azure Database for PostgreSQL Flexible Server Extension Elevation of Privilege Vulnerability	2024-11-12	7.2	CVE-2024-43613
Microsoft--Azure Database for PostgreSQL Flexible Server	Azure Database for PostgreSQL Flexible Server Extension Elevation of Privilege Vulnerability	2024-11-12	7.2	CVE-2024-49042
Microsoft--Azure Stack HCI	Azure Stack HCI Elevation of Privilege Vulnerability	2024-11-15	8.8	CVE-2024-49060
Microsoft-- LightGBM	LightGBM Remote Code Execution Vulnerability	2024-11-12	8.1	CVE-2024-43598
Microsoft-- Microsoft Office LTSC for Mac 2024	Microsoft Excel Remote Code Execution Vulnerability	2024-11-12	7.8	CVE-2024-49028
Microsoft-- Microsoft Office LTSC for Mac 2024	Microsoft Office Graphics Remote Code Execution Vulnerability	2024-11-12	7.8	CVE-2024-49031
Microsoft-- Microsoft Office LTSC for Mac 2024	Microsoft Office Graphics Remote Code Execution Vulnerability	2024-11-12	7.8	CVE-2024-49032
Microsoft-- Microsoft PC Manager	Microsoft PC Manager Elevation of Privilege Vulnerability	2024-11-12	7.8	CVE-2024-49051
Microsoft-- Microsoft SQL	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-38255

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Server 2017 (GDR)				
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-43459
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-48993
Microsoft--Microsoft SQL Server 2019 (CU 29)	SQL Server Native Client Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-43462
Microsoft--Microsoft TorchGeo	TorchGeo Remote Code Execution Vulnerability	2024-11-12	8.1	CVE-2024-49048
Microsoft--Microsoft Visual Studio 2022 version 17.6	.NET and Visual Studio Denial of Service Vulnerability	2024-11-12	7.5	CVE-2024-43499
Microsoft--Microsoft Visual Studio 2022 version 17.8	.NET and Visual Studio Remote Code Execution Vulnerability	2024-11-12	9.8	CVE-2024-43498
Microsoft--Python extension for Visual Studio Code	Visual Studio Code Python Extension Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-49050
Microsoft--Visual Studio Code Remote - SSH Extension	Visual Studio Code Remote Extension Elevation of Privilege Vulnerability	2024-11-12	7.1	CVE-2024-49049
Microsoft--Windows 10 Version 1809	Windows Hyper-V Shared Virtual Disk Elevation of Privilege Vulnerability	2024-11-12	8.8	CVE-2024-43624
Microsoft--Windows 10 Version 1809	Windows Telephony Service Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-43627
Microsoft--Windows 10 Version 1809	Windows Telephony Service Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-43628
Microsoft--Windows 10 Version 1809	Windows Telephony Service Remote Code Execution Vulnerability	2024-11-12	8.8	CVE-2024-43635
Microsoft--Windows 10 Version 1809	Windows Registry Elevation of Privilege Vulnerability	2024-11-12	7.5	CVE-2024-43452
Microsoft--Windows 10 Version 1809	Windows Telephony Service Elevation of Privilege Vulnerability	2024-11-12	7.8	CVE-2024-43626
Microsoft--Windows 10	Win32k Elevation of Privilege Vulnerability	2024-11-12	7.8	CVE-2024-43636

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Version 1809				
Microsoft--Windows 10 Version 1809	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	2024-11-12	7.8	CVE-2024-49046
Microsoft--Windows Server 2019	Windows DNS Spoofing Vulnerability	2024-11-12	7.5	CVE-2024-43450
Microsoft--Windows Server 2019	Active Directory Certificate Services Elevation of Privilege Vulnerability	2024-11-12	7.8	CVE-2024-49019
Microsoft--Windows Server 2022	Windows SMBv3 Server Remote Code Execution Vulnerability	2024-11-12	8.1	CVE-2024-43447
Microsoft--Windows Server 2022	Windows Update Stack Elevation of Privilege Vulnerability	2024-11-12	7.8	CVE-2024-43530
Microsoft--Windows Server 2022	Windows Kernel Elevation of Privilege Vulnerability	2024-11-12	7.8	CVE-2024-43630
Microsoft--Windows Server 2022	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-11-12	7.8	CVE-2024-43640
Microsoft--Windows Server 2025	Windows KDC Proxy Remote Code Execution Vulnerability	2024-11-12	9.8	CVE-2024-43639
Microsoft--Windows Server 2025	Windows DWM Core Library Elevation of Privilege Vulnerability	2024-11-12	7.8	CVE-2024-43629
Microsoft--Windows Server 2025	Windows Registry Elevation of Privilege Vulnerability	2024-11-12	7.8	CVE-2024-43641
Microsoft--Windows Server 2025	Windows SMB Denial of Service Vulnerability	2024-11-12	7.5	CVE-2024-43642
Microsoft--Windows Server 2025	Windows Client-Side Caching Elevation of Privilege Vulnerability	2024-11-12	7.8	CVE-2024-43644
mobisoft974--Relais 2FA	The Relais 2FA plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.0. This is due to incorrect authentication and capability checking in the 'rl_do_ajax' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email.	2024-11-12	9.8	CVE-2024-10245
n/a--dom-iterator	All versions of the package dom-iterator are vulnerable to Arbitrary Code Execution due to use of the Function constructor without complete input sanitization. Function generates a new function body and thus care must be given to ensure that the inputs to Function are not attacker-controlled. The risks involved are similar to that of allowing attacker-controlled input to reach eval.	2024-11-13	7.3	CVE-2024-21541
n/a--Harbor	Harbor fails to validate user permissions while deleting Webhook policies, allowing malicious users to view, update and delete Webhook policies of other users.Â Â The attacker could modify Webhook policies configured in other projects.	2024-11-14	7.7	CVE-2022-31666
n/a--Harbor	Harbor fails to validate the user permissions when updating p2p preheat policies.Â By sending a request to update a p2p preheat policy with an id that	2024-11-14	7.4	CVE-2022-31668

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	belongs to a project that the currently authenticated user doesn't have access to, the attacker could modify p2p preheat policies configured in other projects.			
n/a--Harbor	Harbor fails to validate the user permissions when updating tag retention policies.Â By sending a request to update a tag retention policy with an id that belongs to a projectÂ that the currently authenticated user doesn't have access to, the attacker could modify tag retention policies configured in other projects.	2024-11-14	7.7	CVE-2022-31670
n/a--Harbor	Harbor fails to validate user permissions when reading and updating job execution logs through the P2P preheat execution logs. By sending a request that attempts to read/update P2P preheat execution logs and specifying different job IDs, malicious authenticated usersÂ could read all the job logs stored in the Harbor database.	2024-11-14	7.4	CVE-2022-31671
n/a--Intel(R) CIP software	Improper input validation in some Intel(R) CIP software before version 2.4.10852 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-11-13	8.2	CVE-2024-36482
n/a--Intel(R) DSA	Improper Access Control in some Intel(R) DSA before version 24.3.26.8 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	7.3	CVE-2024-36488
n/a--Intel(R) EMA software	Improper access control for some Intel(R) EMA software before version 1.13.1.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	8.2	CVE-2024-32483
n/a--Intel(R) Extension for Transformers software	Path traversal for some Intel(R) Extension for Transformers software before version 1.5 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	7.1	CVE-2024-21799
n/a--Intel(R) Graphics Drivers	Untrusted pointer dereference in some Intel(R) Graphics Drivers may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	8.4	CVE-2024-34023
n/a--Intel(R) Graphics Drivers	Out-of-bounds write in some Intel(R) Graphics Drivers may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	8.4	CVE-2024-38665
n/a--Intel(R) Neural Compressor software	Improper neutralization of special elements used in an SQL command ('SQL Injection') in some Intel(R) Neural Compressor software before version v3.0 may allow an authenticated user to potentially enable escalation of privilege via adjacent access.	2024-11-13	8	CVE-2024-39368
n/a--Intel(R) Neural Compressor software	Improper input validation in some Intel(R) Neural Compressor software before version v3.0 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	2024-11-13	7.5	CVE-2024-28028
n/a--Intel(R) Neural Compressor software	Improper neutralization of special elements used in SQL command in some Intel(R) Neural Compressor software before version v3.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	7	CVE-2024-39766
n/a--Intel(R) processors with Intel(R) ACTM	Time-of-check Time-of-use Race Condition in some Intel(R) processors with Intel(R) ACTM may allow a privileged user to potentially enable escalation of privilege via local access.	2024-11-13	7.2	CVE-2024-22185
n/a--Intel(R) processors with Intel(R) ACTM	Exposure of resource to wrong sphere in some Intel(R) processors with Intel(R) ACTM may allow a privileged user to potentially enable escalation of privilege via local access.	2024-11-13	7.2	CVE-2024-24985
n/a--Intel(R) Processors	Protection mechanism failure in the SPP for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	8.8	CVE-2024-36242
n/a--Intel(R) Server Board M10JNP2SB Family	Improper input validation in UEFI firmware in some Intel(R) Server Board M10JNP2SB Family may allow a privileged user to potentially enable escalation of privilege via local access.	2024-11-13	7.5	CVE-2024-41167
n/a--Intel(R) Server Board M70KLP	Improper Access Control in UEFI firmware for some Intel(R) Server Board M70KLP may allow a privileged user to potentially enable escalation of privilege via local access.	2024-11-13	7.5	CVE-2024-39609
n/a--Intel(R) Server Board S2600BP	Improper input validation in UEFI firmware in some Intel(R) Server Board S2600BP Family may allow a privileged user to potentially enable escalation of privilege via local access.	2024-11-13	7.5	CVE-2024-31158

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Family				
n/a--Intel(R) Server Board S2600ST Family BIOS and Firmware Update software	Improper input validation in the Intel(R) Server Board S2600ST Family BIOS and Firmware Update software all versions may allow a privileged user to potentially enable escalation of privilege via local access.	2024-11-13	8.2	CVE-2024-36282
n/a--Intel(R) Server S2600BPBR	Improper input validation in UEFI firmware for some Intel(R) Server S2600BPBR may allow a privileged user to potentially enable escalation of privilege via local access.	2024-11-13	7.5	CVE-2024-31154
n/a--Intel(R) Xeon(R) processor memory controller configurations when using Intel(R) SGX	Improper conditions check in some Intel(R) Xeon(R) processor memory controller configurations when using Intel(R) SGX may allow a privileged user to potentially enable escalation of privilege via local access.	2024-11-13	8.8	CVE-2024-23918
n/a--Intel(R) Xeon(R) processor memory controller configurations when using Intel(R) SGX	Incorrect default permissions in some Intel(R) Xeon(R) processor memory controller configurations when using Intel(R) SGX may allow a privileged user to potentially enable escalation of privilege via local access.	2024-11-13	7.2	CVE-2024-21820
n/a--n/a	A flaw was found in GNOME Maps, which is vulnerable to a code injection attack via its service.json configuration file. If the configuration file is malicious, it may execute arbitrary code.	2024-11-17	9.8	CVE-2023-43091
n/a--n/a	EnGenius EWS356-FIT devices through 1.1.30 allow blind OS command injection. This allows an attacker to execute arbitrary OS commands via shell metacharacters to the Ping and Speed Test utilities.	2024-11-11	9.8	CVE-2024-36061
n/a--n/a	Multiple Buffer overflows in the MMS Client in MZ Automation LibIEC61850 before commit ac925fae8e281ac6defcd630e9dd756264e9c5bc allow a malicious server to cause a stack-based buffer overflow via the MMS FileDirResponse message.	2024-11-15	9.8	CVE-2024-45970
n/a--n/a	Multiple Buffer overflows in the MMS Client in MZ Automation LibIEC61850 before commit 1f52be9ddeae00e69cd43e4cac3cb4f0c880c4f0 allow a malicious server to cause a stack-based buffer overflow via the MMS IdentifyResponse message.	2024-11-15	9.8	CVE-2024-45971
n/a--n/a	The SYQ com.downloader.video.fast (aka Master Video Downloader) application through 2.0 for Android allows an attacker to execute arbitrary JavaScript code via the com.downloader.video.fast.SpeedMainAct component.	2024-11-11	9.1	CVE-2024-46962
n/a--n/a	The boa httpd of Trendnet TEW-820AP 1.01.B01 has a stack overflow vulnerability in /boafrm/formIPv6Addr, /boafrm/formIpv6Setup, /boafrm/formDnsv6. The reason is that the check of ipv6 address is not sufficient, which allows attackers to construct payloads for attacks.	2024-11-11	9.8	CVE-2024-50667
n/a--n/a	A SQL injection vulnerability in /omrs/admin/search.php in PHPGurukul Online Marriage Registration System v1.0 allows an attacker to execute arbitrary SQL commands via the "searchdata " parameter.	2024-11-11	9.8	CVE-2024-50989
n/a--n/a	An XML External Entity (XXE) vulnerability in the component DocumentBuilderFactory of powertac-server v1.9.0 allows attackers to access sensitive information or execute arbitrary code via supplying a crafted request containing malicious XML entities.	2024-11-11	9.8	CVE-2024-51135
n/a--n/a	gio/gsocks4aproxy.c in GNOME GLib before 2.82.1 has an off-by-one error and resultant buffer overflow because SOCKS4_CONN_MSG_LEN is not sufficient for a trailing '\0' character.	2024-11-11	9.8	CVE-2024-52533
n/a--n/a	An issue in DLink DWR 2000M 5G CPE With Wifi 6 Ax1800 and Dlink DWR 5G CPE DWR-2000M_1.34ME allows a local attacker to execute arbitrary code via a crafted payload to the Diagnostics function.	2024-11-12	8	CVE-2024-28726
n/a--n/a	A heap-based buffer overflow in tsMuxer version nightly-2024-03-14-01-51-12 allows attackers to cause Denial of Service (DoS) and Code Execution via a crafted MOV video file.	2024-11-14	8.8	CVE-2024-41209
n/a--n/a	Wi-Fi Alliance wfa_dut (in Wi-Fi Test Suite) through 9.0.0 allows OS command injection via 802.11x frames because the system() library function is used. For example, on Arcadyan FMIMG51AX000J devices, this leads to wfaTGSendPing remote code execution as root via traffic to TCP port 8000 or 8080 on a LAN interface. On other devices, this may be exploitable over a WAN interface.	2024-11-11	8.8	CVE-2024-41992

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	The com.superfast.video.downloader (aka Super Unlimited Video Downloader - All in One) application through 5.1.9 for Android allows an attacker to execute arbitrary JavaScript code via the com.bluesky.browser.ui.BrowserMainActivity component.	2024-11-11	8.1	CVE-2024-46963
n/a--n/a	The com.video.downloader.all (aka All Video Downloader) application through 11.28 for Android allows an attacker to execute arbitrary JavaScript code via the com.video.downloader.all.StartActivity component.	2024-11-11	8.1	CVE-2024-46964
n/a--n/a	The Ikhgur mn.ikhgur.khotoch (aka Video Downloader Pro & Browser) application through 1.0.42 for Android allows an attacker to execute arbitrary JavaScript code via the mn.ikhgur.khotoch.MainActivity component.	2024-11-11	8.1	CVE-2024-46966
n/a--n/a	UsersController.php in Run.codes 1.5.2 and older has a reset password race condition vulnerability.	2024-11-11	8.1	CVE-2024-48322
n/a--n/a	A heap-based buffer overflow in tsMuxer version nightly-2024-03-14-01-51-12 allows attackers to cause Denial of Service (DoS), Information Disclosure and Code Execution via a crafted MKV video file.	2024-11-14	8.8	CVE-2024-49777
n/a--n/a	A heap-based buffer overflow in tsMuxer version nightly-2024-05-12-02-01-18 allows attackers to cause Denial of Service (DoS) and Code Execution via a crafted MOV video file.	2024-11-14	8.8	CVE-2024-49778
n/a--n/a	D-Link DIR-820L 1.05b03 was discovered to contain a remote code execution (RCE) vulnerability via the ping_addr parameter in the ping_v4 and ping_v6 functions.	2024-11-11	8	CVE-2024-51186
n/a--n/a	GNOME libsoup before 3.6.1 allows a buffer overflow in applications that perform conversion to UTF-8 in soup_header_parse_param_list_strict. Input received over the network cannot trigger this.	2024-11-11	8.4	CVE-2024-52531
n/a--n/a	guix-daemon in GNU Guix before 5ab3c4c allows privilege escalation because build outputs are accessible by local users before file metadata concerns (e.g., for setuid and setgid programs) are properly addressed. The vulnerability can be remediated within the product via certain pull, reconfigure, and restart actions. Both 5ab3c4c and 5582241 are needed to resolve the vulnerability.	2024-11-17	8.1	CVE-2024-52867
n/a--n/a	Sercomm Router Etisalat Model S3- AC2100 is affected by Incorrect Access Control via the diagnostic utility in the router dashboard.	2024-11-12	7.3	CVE-2021-27702
n/a--n/a	A flaw was found in kube-controller-manager. This issue occurs when the initial application of a HPA config YAML lacking a .spec.behavior.scaleUp block causes a denial of service due to KCM pods going into restart churn.	2024-11-17	7.7	CVE-2024-0793
n/a--n/a	An invalid memory access when handling the ProtocolIE_ID field of E-RAB Release Indication messages in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	2024-11-15	7.5	CVE-2024-24452
n/a--n/a	An invalid memory access when handling the ProtocolIE_ID field of E-RAB NotToBeModifiedBearerModInd information element in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	2024-11-15	7.5	CVE-2024-24453
n/a--n/a	An invalid memory access when handling the ProtocolIE_ID field of E-RAB Modify Request messages in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	2024-11-15	7.5	CVE-2024-24454
n/a--n/a	An invalid memory access when handling a UE Context Release message containing an invalid UE identifier in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	2024-11-15	7.5	CVE-2024-24455
n/a--n/a	An invalid memory access when handling the ProtocolIE_ID field of E-RAB Setup List Context SURes messages in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	2024-11-15	7.5	CVE-2024-24457
n/a--n/a	An invalid memory access when handling the ENB Configuration Transfer messages containing invalid PLMN Identities in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	2024-11-15	7.5	CVE-2024-24458
n/a--n/a	An invalid memory access when handling the ProtocolIE_ID field of S1Setup Request messages in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	2024-11-15	7.5	CVE-2024-24459
n/a--n/a	NULL pointer dereference in the MMS Client in MZ Automation LibIEC1850 before commit 7afa40390b26ad1f4cf93deaa0052fe7e357ef33 allows a malicious server to Cause a Denial-of-Service via the MMS InitiationResponse message.	2024-11-15	7.5	CVE-2024-45969

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	An issue in TOTOLINK Bluetooth Wireless Adapter A600UB allows a local attacker to execute arbitrary code via the WifiAutoInstallDriver.exe and MSASN1.dll components.	2024-11-15	7.8	CVE-2024-51141
n/a--n/a	An issue in Open 5GS v.2.7.1 allows a remote attacker to cause a denial of service via the Network Function Virtualizations (NFVs) such as the User Plane Function (UPF) and the Session Management Function (SMF), The Packet Data Unit (PDU) session establishment process.	2024-11-12	7.5	CVE-2024-51179
n/a--n/a	GNOME libsoup before 3.6.0 allows HTTP request smuggling in some configurations because '\0' characters at the end of header names are ignored, i.e., a "Transfer-Encoding\0: chunked" header is treated the same as a "Transfer-Encoding: chunked" header.	2024-11-11	7.5	CVE-2024-52530
n/a--n/a	GNOME libsoup before 3.6.1 has an infinite loop, and memory consumption. during the reading of certain patterns of WebSocket data from clients.	2024-11-11	7.5	CVE-2024-52532
n/a--n/a	A heap buffer overflow was found in the virtio-snd device in QEMU. When reading input audio in the virtio-snd input callback, virtio_snd_pcm_in_cb, the function did not check whether the iov can fit the data buffer. This issue can trigger an out-of-bounds write if the size of the virtio queue element is equal to virtio_snd_pcm_status, which makes the available space for audio data zero.	2024-11-14	7.4	CVE-2024-7730
n/a--PostgreSQL	Incorrect control of environment variables in PostgreSQL PL/Perl allows an unprivileged database user to change sensitive process environment variables (e.g. PATH). That often suffices to enable arbitrary code execution, even if the attacker lacks a database server operating system user. Versions before PostgreSQL 17.1, 16.5, 15.9, 14.14, 13.17, and 12.21 are affected.	2024-11-14	8.8	CVE-2024-10979
NetScaler--NetScaler ADC	Authenticated user can access unintended user capabilitiesÂ inÂ NetScaler ADC and NetScaler Gateway if the appliance must be configured as a Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) with KCDAccount configuration for Kerberos SSO to access backend resourcesÂ ORÂ the appliance must be configured as anÂ Auth Server (AAA Vserver) with KCDAccount configuration for Kerberos SSO to access backend resources	2024-11-12	8.8	CVE-2024-8535
nextcloud--security-advisories	Nextcloud Mail is the mail app for Nextcloud, a self-hosted productivity platform. When a user is trying to set up a mail account with an email address like user@example.tld that does not support auto configuration, and an attacker managed to register autoconfig.tld, the used email details would be send to the server of the attacker. It is recommended that the Nextcloud Mail app is upgraded to 1.14.6, 1.15.4, 2.2.11, 3.6.3, 3.7.7 or 4.0.0.	2024-11-15	8.2	CVE-2024-52508
nikoarroyocuraza--online_furniture_shopping_project	A SQL injection vulnerability in orderview1.php of Itsourcecode Online Furniture Shopping Project 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2024-11-13	8.8	CVE-2024-50970
Nomysoft Informatics--Nomysem	Improper Privilege Management vulnerability in Nomysoft Informatics Nomysem allows Collect Data as Provided by Users.This issue affects Nomysem: before 13.10.2024.	2024-11-12	7.1	CVE-2024-8074
OpenBSD--OpenBSD	In OpenBSD 7.5 before errata 008 and OpenBSD 7.4 before errata 021, avoid possible mbuf double free in NFS client and server implementation, do not use uninitialized variable in error handling of NFS server.	2024-11-15	9.8	CVE-2024-10934
OpenSSL--OpenSSL	Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications. The SSL_free_buffers function is used to free the internal OpenSSL buffer used when processing an incoming record from the network. The call is only expected to succeed if the buffer is not currently in use. However, two scenarios have been identified where the buffer is freed even when still in use. The first scenario occurs where a record header has been received from the network and processed by OpenSSL, but the full record body has not yet arrived. In this case calling SSL_free_buffers will succeed even though a record has only been partially processed and the buffer is still in use.	2024-11-13	7.5	CVE-2024-4741

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The second scenario occurs where a full record containing application data has been received and processed by OpenSSL but the application has only read part of this data. Again a call to SSL_free_buffers will succeed even though the buffer is still in use. While these scenarios could occur accidentally during normal operation a malicious attacker could attempt to engineer a stituation where this occurs. We are not aware of this issue being actively exploited. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.			
Optimal Access Inc.--KBucket	Unrestricted Upload of File with Dangerous Type vulnerability in Optimal Access Inc. KBucket allows Upload a Web Shell to a Web Server.This issue affects KBucket: from n/a through 4.1.6.	2024-11-14	9.9	CVE-2024-52369
parisneo--parisneo/lollms-webui	parisneo/lollms-webui version 9.6 is vulnerable to Cross-Site Scripting (XSS) and Open Redirect due to inadequate input validation and processing of SVG files during the upload process. The XSS vulnerability allows attackers to embed malicious JavaScript code within SVG files, which is executed upon rendering, leading to potential credential theft and unauthorized data access. The Open Redirect vulnerability arises from insufficient URL validation within SVG files, enabling attackers to redirect users to malicious websites, thereby exposing them to phishing attacks, malware distribution, and reputation damage. These vulnerabilities are present in the application's functionality to send files to the AI module.	2024-11-14	7.3	CVE-2024-5125
Phan An--AJAX Random Posts	Deserialization of Untrusted Data vulnerability in Phan An AJAX Random Posts allows Object Injection.This issue affects AJAX Random Posts: from n/a through 0.3.3.	2024-11-16	9.8	CVE-2024-52409
Phoenixheart--Referrer Detector	Deserialization of Untrusted Data vulnerability in Phoenixheart Referrer Detector allows Object Injection.This issue affects Referrer Detector: from n/a through 4.2.1.0.	2024-11-16	9.8	CVE-2024-52410
Platform.ly--Platform.ly Official	Cross-Site Request Forgery (CSRF) vulnerability in Platform.Ly Platform.Ly Official allows Stored XSS.This issue affects Platform.Ly Official: from n/a through 1.1.3.	2024-11-14	7.1	CVE-2024-51687
Podlove--Podlove Podcast Publisher	Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Podlove Podlove Podcast Publisher.This issue affects Podlove Podcast Publisher: from n/a through 4.1.15.	2024-11-14	9.1	CVE-2024-52393
pressaholic--WordPress Video Robot - The Ultimate Video Importer	The WordPress Video Robot - The Ultimate Video Importer plugin for WordPress is vulnerable to privilege escalation due to insufficient validation on user meta that can be updated in the wpvr_rate_request_result() function in all versions up to, and including, 1.20.0. This makes it possible for authenticated attackers, with subscriber-level access and above, to update their user meta on a WordPress site. This can be leveraged to update their capabilities to that of an administrator.	2024-11-16	8.8	CVE-2024-9192
Progress Software Corporation--Telerik Report Server	In ProgressÂ® TelerikÂ® Report Server versions prior to 2024 Q4 (10.3.24.1112), the encryption of local asset data used an older algorithm which may allow a sophisticated actor to decrypt this information.	2024-11-13	7.1	CVE-2024-7295
Progress Software--Telerik UI for WinForms	In Progress Telerik UI for WinForms versions prior to 2024 Q4 (2024.4.1113), a code execution attack is possible through an insecure deserialization vulnerability.	2024-11-13	7.8	CVE-2024-10013
Progress Software--Telerik UI for WPF	In Progress Telerik UI for WPF versions prior to 2024 Q4 (2024.4.1111), a code execution attack is possible through an insecure deserialization vulnerability.	2024-11-13	7.8	CVE-2024-10012
Really Simple Plugins--Really Simple Security Pro multisite	The Really Simple Security (Free, Pro, and Pro Multisite) plugins for WordPress are vulnerable to authentication bypass in versions 9.0.0 to 9.1.1.1. This is due to improper user check error handling in the two-factor REST API actions with the 'check_login_and_get_user' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, when the "Two-Factor Authentication" setting is enabled (disabled by default).	2024-11-15	9.8	CVE-2024-10924
Red Hat--Migration Toolkit for Runtimes 1 on RHEL 8	A flaw was found in Undertow, which incorrectly parses cookies with certain value-delimiting characters in incoming requests. This issue could allow an attacker to construct a cookie value to exfiltrate HttpOnly cookie values or spoof arbitrary additional cookie values, leading to unauthorized data access or modification. The main threat from this flaw impacts data confidentiality and integrity.	2024-11-17	7.4	CVE-2023-4639

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Enterprise Linux	A vulnerability was found in Samba where a delegated administrator with permission to create objects in Active Directory can write to all attributes of the newly created object, including security-sensitive attributes, even after the object's creation. This issue occurs because the administrator owns the object due to the lack of an Access Control List (ACL) at the time of creation and later being recognized as the 'creator owner.' The retained significant rights of the delegated administrator may not be well understood, potentially leading to unintended privilege escalation or security risks.	2024-11-17	7.5	CVE-2020-25720
Red Hat--Red Hat Single Sign-On 7	A flaw was found in the Keycloak package. This flaw allows an attacker to utilize an LDAP injection to bypass the username lookup or potentially perform other malicious actions.	2024-11-14	7.5	CVE-2022-2232
redefiningtheweb--PDF Generator Addon for Elementor Page Builder	The PDF Generator Addon for Elementor Page Builder plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.7.5 via the rtw_pgaepb_dwnld_pdf() function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	2024-11-16	7.5	CVE-2024-9935
revmakx--Backup and Staging by WP Time Capsule	The Backup and Staging by WP Time Capsule plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the the UploadHandler.php file and no direct file access prevention in all versions up to, and including, 1.22.21. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-11-16	9.8	CVE-2024-8856
Richteam--Share Buttons Social Media	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Richteam Share Buttons - Social Media allows Blind SQL Injection.This issue affects Share Buttons - Social Media: from n/a through 1.0.2.	2024-11-11	8.5	CVE-2024-51845
Rockwell Automation--Arena Input Analyzer	A memory corruption vulnerability exists in the affected products when parsing DFT files. Local threat actors can exploit this issue to disclose information and to execute arbitrary code. To exploit this vulnerability a legitimate user must open a malicious DFT file.	2024-11-14	7.3	CVE-2024-6068
Rockwell Automation--FactoryTalk Updater	An authentication bypass vulnerability exists in the affected product. The vulnerability exists due to shared secrets across accounts and could allow a threat actor to impersonate a user if the threat actor is able to enumerate additional information required during authentication.	2024-11-12	9.1	CVE-2024-10943
Rockwell Automation--FactoryTalk Updater	A Remote Code Execution vulnerability exists in the affected product. The vulnerability requires a high level of permissions and exists due to improper input validation resulting in the possibility of a malicious Updated Agent being deployed.	2024-11-12	8.4	CVE-2024-10944
Rockwell Automation--FactoryTalk Updater	A Local Privilege Escalation vulnerability exists in the affected product. The vulnerability requires a local, low privileged threat actor to replace certain files during update and exists due to a failure to perform proper security checks before installation.	2024-11-12	7.3	CVE-2024-10945
Rockwell Automation--FactoryTalk View Machine Edition	A remote code execution vulnerability exists in the affected product. The vulnerability allows users to save projects within the public directory allowing anyone with local access to modify and/or delete files. Additionally, a malicious user could potentially leverage this vulnerability to escalate their privileges by changing the macro to execute arbitrary code.	2024-11-12	7.3	CVE-2024-37365
Sage AI--Sage AI: Chatbots, OpenAI GPT-4 Bulk Articles, Dalle-3 Image Generation	Unrestricted Upload of File with Dangerous Type vulnerability in Sage AI Sage AI: Chatbots, OpenAI GPT-4 Bulk Articles, Dalle-3 Image Generation allows Upload a Web Shell to a Web Server.This issue affects Sage AI: Chatbots, OpenAI GPT-4 Bulk Articles, Dalle-3 Image Generation: from n/a through 2.4.9.	2024-11-14	9.9	CVE-2024-52384
sap -- host_agent	An attacker who gains local membership to sapsys group could replace local files usually protected by privileged access. On successful exploitation the attacker could cause high impact on confidentiality and integrity of the application.	2024-11-12	7.1	CVE-2024-47595
SAP_SE--SAP Web Dispatcher	An unauthenticated attacker can create a malicious link which they can make publicly available. When an authenticated victim clicks on this malicious link, input data will be used by the web site page generation to create content which when	2024-11-12	8.8	CVE-2024-47590

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	executed in the victim's browser (XXS) or transmitted to another server (SSRF) gives the attacker the ability to execute arbitrary code on the server fully compromising confidentiality, integrity and availability.			
Schneider Electric--EcoStruxure IT Gateway	CWE-862: Missing Authorization vulnerability exists that could cause unauthorized access when enabled on the network and potentially impacting connected devices.	2024-11-13	9.8	CVE-2024-10575
Schneider Electric--Modicon M340 CPU (part numbers BMXP34*)	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause a potential arbitrary code execution after a successful Man-In-The-Middle attack followed by sending a crafted Modbus function call to tamper with memory area involved in memory size computation.	2024-11-13	8.1	CVE-2024-8938
Schneider Electric--Modicon M340 CPU (part numbers BMXP34*)	CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel vulnerability exists that could cause retrieval of password hash that could lead to denial of service and loss of confidentiality and integrity of controllers. To be successful, the attacker needs to inject themself inside the logical network while a valid user uploads or downloads a project file into the controller.	2024-11-13	7.5	CVE-2024-8933
Schneider Electric--Modicon M340 CPU (part numbers BMXP34*)	CWE-290: Authentication Bypass by Spoofing vulnerability exists that could cause a denial of service and loss of confidentiality and integrity of controllers when conducting a Man-In-The-Middle attack between the controller and the engineering workstation while a valid user is establishing a communication session. This vulnerability is inherent to Diffie Hellman algorithm which does not protect against Man-In-The-Middle attacks.	2024-11-13	7.5	CVE-2024-8935
Schneider Electric--PowerLogic PM5320	CWE-400: An Uncontrolled Resource Consumption vulnerability exists that could cause the device to become unresponsive resulting in communication loss when a large amount of IGMP packets is present in the network.	2024-11-13	7.5	CVE-2024-9409
Shoaib Rehmat--ZIJ KART	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Shoaib Rehmat ZIJ KART allows PHP Local File Inclusion.This issue affects ZIJ KART: from n/a through 1.1.	2024-11-14	8.1	CVE-2024-52381
siemens -- ruggedcom_rm1224_lte\(4g\)_eu_firmware	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.2), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.2), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V8.2), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.2), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.2), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.2), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.2), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.2), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.2), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.2), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.2), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.2), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.2), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.2), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.2), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.2), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.2), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.2), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.2), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.2). Affected devices do not properly validate input in configuration fields of the iperf functionality. This could allow an unauthenticated remote attacker to execute arbitrary code on the device.	2024-11-12	9.8	CVE-2024-50557
siemens -- ruggedcom_rm122	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.2), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-	2024-11-12	7.2	CVE-2024-50572

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
4_lte\(4g\)_eu_firmware	4AM00-2DA2) (All versions < V8.2), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V8.2), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.2), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.2), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.2), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.2), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.2), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.2), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.2), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.2), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.2), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.2), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.2), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.2), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.2), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.2), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.2), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.2), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.2). Affected devices do not properly sanitize an input field. This could allow an authenticated remote attacker with administrative privileges to inject code or spawn a system root shell.			
siemens -- simatic_cp_1543-1_firmware	A vulnerability has been identified in SIMATIC CP 1543-1 V4.0 (6GK7543-1AX10-0XE0) (All versions >= V4.0.44 < V4.0.50). Affected devices do not properly handle authorization. This could allow an unauthenticated remote attacker to gain access to the filesystem.	2024-11-12	7.5	CVE-2024-50310
siemens -- sinec_ins	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 3). The affected application does not properly sanitize user provided paths for SFTP-based file up- and downloads. This could allow an authenticated remote attacker to manipulate arbitrary files on the filesystem and achieve arbitrary code execution on the device.	2024-11-12	9.9	CVE-2024-46888
siemens -- sinec_ins	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 3). The affected application does not properly validate input sent to specific endpoints of its web API. This could allow an authenticated remote attacker with high privileges on the application to execute arbitrary code on the underlying OS.	2024-11-12	9.1	CVE-2024-46890
siemens -- sinec_ins	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 3). The affected application does not properly invalidate sessions when the associated user is deleted or disabled or their permissions are modified. This could allow an authenticated attacker to continue performing malicious actions even after their user account has been disabled.	2024-11-12	8.1	CVE-2024-46892
siemens -- siport	A vulnerability has been identified in SIPORT (All versions < V3.4.0). The affected application improperly assigns file permissions to installation folders. This could allow a local attacker with an unprivileged account to override or modify the service executables and subsequently gain elevated privileges.	2024-11-12	7.8	CVE-2024-47783
siemens -- solid_edge_se2024	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 9). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PSM files. This could allow an attacker to execute code in the context of the current process.	2024-11-12	7.8	CVE-2024-47940
siemens -- solid_edge_se2024	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 9). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-11-12	7.8	CVE-2024-47941
siemens -- solid_edge_se2024	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 9). The affected applications suffer from a DLL hijacking vulnerability. This could allow an attacker to execute arbitrary code via placing a crafted DLL file on the system.	2024-11-12	7.3	CVE-2024-47942
siemens -- spectrum_power_7	A vulnerability has been identified in Spectrum Power 7 (All versions < V24Q3). The affected product contains several root-owned SUID binaries that could allow an authenticated local attacker to escalate privileges.	2024-11-12	7.8	CVE-2024-29119

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- telecontrol_server_basic	A vulnerability has been identified in PP TeleControl Server Basic 1000 to 5000 V3.1 (6NH9910-0AA31-0AE1) (All versions < V3.1.2.1 with redundancy configured), PP TeleControl Server Basic 256 to 1000 V3.1 (6NH9910-0AA31-0AD1) (All versions < V3.1.2.1 with redundancy configured), PP TeleControl Server Basic 32 to 64 V3.1 (6NH9910-0AA31-0AF1) (All versions < V3.1.2.1 with redundancy configured), PP TeleControl Server Basic 64 to 256 V3.1 (6NH9910-0AA31-0AC1) (All versions < V3.1.2.1 with redundancy configured), PP TeleControl Server Basic 8 to 32 V3.1 (6NH9910-0AA31-0AB1) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic 1000 V3.1 (6NH9910-0AA31-0AD0) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic 256 V3.1 (6NH9910-0AA31-0AC0) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic 32 V3.1 (6NH9910-0AA31-0AF0) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic 5000 V3.1 (6NH9910-0AA31-0AE0) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic 64 V3.1 (6NH9910-0AA31-0AB0) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic 8 V3.1 (6NH9910-0AA31-0AA0) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic Serv Upgr (6NH9910-0AA31-0GA1) (All versions < V3.1.2.1 with redundancy configured), TeleControl Server Basic Upgr V3.1 (6NH9910-0AA31-0GA0) (All versions < V3.1.2.1 with redundancy configured). The affected system allows remote users to send maliciously crafted objects. Due to insecure deserialization of user-supplied content by the affected software, an unauthenticated attacker could exploit this vulnerability by sending a maliciously crafted serialized object. This could allow the attacker to execute arbitrary code on the device with SYSTEM privileges.	2024-11-12	10	CVE-2024-44102
Siemens--SIMATIC S7-PLCSIM V16	A vulnerability has been identified in SIMATIC S7-PLCSIM V16 (All versions), SIMATIC S7-PLCSIM V17 (All versions), SIMATIC STEP 7 Safety V16 (All versions), SIMATIC STEP 7 Safety V17 (All versions < V17 Update 8), SIMATIC STEP 7 Safety V18 (All versions < V18 Update 5), SIMATIC STEP 7 V16 (All versions), SIMATIC STEP 7 V17 (All versions < V17 Update 8), SIMATIC STEP 7 V18 (All versions < V18 Update 5), SIMATIC WinCC Unified V16 (All versions), SIMATIC WinCC Unified V17 (All versions < V17 Update 8), SIMATIC WinCC Unified V18 (All versions < V18 Update 5), SIMATIC WinCC V16 (All versions), SIMATIC WinCC V17 (All versions < V17 Update 8), SIMATIC WinCC V18 (All versions < V18 Update 5), SIMOCODE ES V16 (All versions), SIMOCODE ES V17 (All versions < V17 Update 8), SIMOCODE ES V18 (All versions), SIMOTION SCOUT TIA V5.4 SP1 (All versions), SIMOTION SCOUT TIA V5.4 SP3 (All versions), SIMOTION SCOUT TIA V5.5 SP1 (All versions), SINAMICS Startdrive V16 (All versions), SINAMICS Startdrive V17 (All versions), SINAMICS Startdrive V18 (All versions), SIRIUS Safety ES V17 (All versions < V17 Update 8), SIRIUS Safety ES V18 (All versions), SIRIUS Soft Starter ES V17 (All versions < V17 Update 8), SIRIUS Soft Starter ES V18 (All versions), TIA Portal Cloud V16 (All versions), TIA Portal Cloud V17 (All versions < V4.6.0.1), TIA Portal Cloud V18 (All versions < V4.6.1.0). Affected products do not properly sanitize user-controllable input when parsing user settings. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application.	2024-11-12	7.3	CVE-2023-32736
Skpstorm--SK WP Settings Backup	Cross-Site Request Forgery (CSRF) vulnerability in Skpstorm SK WP Settings Backup allows Object Injection.This issue affects SK WP Settings Backup: from n/a through 1.0.	2024-11-16	8.8	CVE-2024-52415
sodah--LUNA RADIO PLAYER	The LUNA RADIO PLAYER plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 6.24.01.24 via the js/fallback.php file. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	2024-11-13	7.5	CVE-2024-10816
SoftBank Corp.--Mesh Wi-Fi router RP562B	Improper neutralization of special elements used in an OS command ('OS Command Injection') issue exists in Mesh Wi-Fi router RP562B firmware version v1.0.2 and earlier. If this vulnerability is exploited, a network-adjacent authenticated attacker may execute an arbitrary OS command.	2024-11-12	8	CVE-2024-45827
Softpulse Infotech--Picsmize	Unrestricted Upload of File with Dangerous Type vulnerability in Softpulse Infotech Picsmize allows Upload a Web Shell to a Web Server.This issue affects Picsmize: from n/a through 1.0.0.	2024-11-14	10	CVE-2024-52380
Sound Research--SECOMN64 Driver	Potential vulnerabilities have been identified in the audio package for certain HP PC products using the Sound Research SECOMN64 driver, which might allow escalation of privilege. Sound Research has released driver updates to mitigate the potential vulnerabilities.	2024-11-12	8.8	CVE-2024-2208
Stephen Cui--Xin	Deserialization of Untrusted Data vulnerability in Stephen Cui Xin allows Object Injection.This issue affects Xin: from n/a through 1.0.8.1.	2024-11-16	9.8	CVE-2024-52412

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Subhasis Laha--Gallerio	Unrestricted Upload of File with Dangerous Type vulnerability in Subhasis Laha Gallerio allows Upload a Web Shell to a Web Server.This issue affects Gallerio: from n/a through 1.01.	2024-11-16	9.9	CVE-2024-52400
sudiptomahato--Blogger 301 Redirect	The Blogger 301 Redirect plugin for WordPress is vulnerable to blind time-based SQL Injection via the 'br' parameter in all versions up to, and including, 2.5.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-11-16	7.5	CVE-2024-10645
SUSE--rancher	A vulnerability has been identified in the way that Rancher stores vSphere's CPI (Cloud Provider Interface) and CSI (Container Storage Interface) credentials used to deploy clusters through the vSphere cloud provider. This issue leads to the vSphere CPI and CSI passwords being stored in a plaintext object inside Rancher. This vulnerability is only applicable to users that deploy clusters in vSphere environments.	2024-11-13	9.1	CVE-2022-45157
symfony--symfony	Symphony process is a module for the Symphony PHP framework which executes commands in sub-processes. When consuming a persisted remember-me cookie, Symfony does not check if the username persisted in the database matches the username attached with the cookie, leading to authentication bypass. This vulnerability is fixed in 5.4.47, 6.4.15, and 7.1.8.	2024-11-13	7.5	CVE-2024-51996
Synology--BeePhotos	Improper neutralization of special elements used in a command ('Command Injection') vulnerability in Task Manager component in Synology BeePhotos before 1.0.2-10026 and 1.1.0-10053 and Synology Photos before 1.6.2-0720 and 1.7.0-0795 allows remote attackers to execute arbitrary code via unspecified vectors.	2024-11-15	9.8	CVE-2024-10443
Team Devexhub--Devexhub Gallery	Unrestricted Upload of File with Dangerous Type vulnerability in Team Devexhub Devexhub Gallery allows Upload a Web Shell to a Web Server.This issue affects Devexhub Gallery: from n/a through 2.0.1.	2024-11-14	10	CVE-2024-52373
Team HB WEBSOL--HB AUDIO GALLERY	Unrestricted Upload of File with Dangerous Type vulnerability in Team HB WEBSOL HB AUDIO GALLERY allows Upload a Web Shell to a Web Server.This issue affects HB AUDIO GALLERY: from n/a through 3.0.	2024-11-11	10	CVE-2024-51790
Team PushAssist--Push Notifications for WordPress by PushAssist	Unrestricted Upload of File with Dangerous Type vulnerability in Team PushAssist Push Notifications for WordPress by PushAssist allows Upload a Web Shell to a Web Server.This issue affects Push Notifications for WordPress by PushAssist: from n/a through 3.0.8.	2024-11-16	9.9	CVE-2024-52408
TECNO--com.transsion.phoenix	Unauthorized access vulnerability in the mobile application (com.transsion.phoenix) can lead to the leakage of user information.	2024-11-14	7.5	CVE-2024-11206
tenda --ac10_firmware	A vulnerability classified as critical was found in Tenda AC10 16.03.10.13. Affected by this vulnerability is the function FUN_0044db3c of the file /goform/fast_setting_wifi_set. The manipulation of the argument timeZone leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-11	8.8	CVE-2024-11061
Tenda--AC10	A vulnerability was found in Tenda AC10 16.03.10.13 and classified as critical. Affected by this issue is the function formSetRebootTimer of the file /goform/SetSysAutoRebbotCfg. The manipulation of the argument rebootTime leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-15	8.8	CVE-2024-11248
tendacn --g3_firmware	Tenda G3 v3.0 v15.11.0.20 was discovered to contain a command injection vulnerability via the formSetUSBPartitionUmount function.	2024-11-13	8.8	CVE-2024-50852
tendacn --g3_firmware	Tenda G3 v3.0 v15.11.0.20 was discovered to contain a command injection vulnerability via the formSetDebugCfg function.	2024-11-13	8.8	CVE-2024-50853
tendacn --g3_firmware	Tenda G3 v3.0 v15.11.0.20 was discovered to contain a stack overflow via the formSetPortMapping function.	2024-11-13	8.8	CVE-2024-50854
timgeyssens -- ui-o-matic	A vulnerability has been found in TimGeyssens UIOMatic 5 and classified as critical. This vulnerability affects unknown code of the file /src/UIOMatic/wwwroot/backoffice/resources/uioMaticObject.r. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-12	7.2	CVE-2024-11124

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tolgee--tolgee-platform	Tolgee is an open-source localization platform. Tolgee 3.81.1 included the all configuration properties in the PublicConfiguratioDTO publicly exposed to users. This vulnerability is fixed in v3.81.2.	2024-11-12	9.8	CVE-2024-52297
TP-Link--VN020 F3v(T)	A vulnerability, which was classified as critical, has been found in TP-Link VN020 F3v(T) TT_V6.2.1021. Affected by this issue is some unknown functionality of the component DHCP DISCOVER Packet Parser. The manipulation of the argument hostname leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-15	7.5	CVE-2024-11237
tripetto--WordPress form builder plugin for contact forms, surveys and quizzes Tripetto	The Tripetto plugin for WordPress is vulnerable to Stored Cross-Site Scripting via File uploads in all versions up to, and including, 8.0.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses the file.	2024-11-15	7.2	CVE-2024-10260
uiuxlab--Uix Slideshow	The The Uix Slideshow plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.6.5. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	2024-11-16	7.3	CVE-2024-9839
UjW0L--Image Classify	Unrestricted Upload of File with Dangerous Type vulnerability in UjW0L Image Classify allows Upload a Web Shell to a Web Server.This issue affects Image Classify: from n/a through 1.0.0.	2024-11-11	10	CVE-2024-51789
Unknown--Recover WooCommerce Cart Abandonment, Newsletter, Email Marketing, Marketing Automation By FunnelKit	The Recover WooCommerce Cart Abandonment, Newsletter, Email Marketing, Marketing Automation By FunnelKit WordPress plugin before 3.3.0 does not sanitize and escape the bwfan-track-id parameter before using it in a SQL statement, allowing unauthenticated users to perform SQL injection attacks	2024-11-14	8.6	CVE-2024-9186
Unknown--WooCommerce Upload Files	The WooCommerce Upload Files plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the upload_files() function in all versions up to, and including, 84.3. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-11-13	9.8	CVE-2024-10820
VaeMendis--VaeMendis Ubooquity version 2.1.2	VaeMendis - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2024-11-14	7.5	CVE-2024-45254
VaeMendis--VaeMendis Ubooquity version 2.1.2	VaeMendis - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	2024-11-14	7.5	CVE-2024-47915
vanquish--WordPress User Extra Fields	The WordPress User Extra Fields plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_tmp_uploaded_file() function in all versions up to, and including, 16.6. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	2024-11-13	9.8	CVE-2024-11150
vanquish--WordPress User Extra Fields	The WordPress User Extra Fields plugin for WordPress is vulnerable to privilege escalation due to a missing capability check on the ajax_save_fields() function in all versions up to, and including, 16.6. This makes it possible for authenticated attackers, with subscriber-level access and above, to add custom fields that can be updated and then use the check_and_overwrite_wp_or_woocommerce_fields function to update the wp_capabilities field to have administrator privileges.	2024-11-13	8.8	CVE-2024-10800
vice -- webopac	Webopac from Grand Vice info has a SQL Injection vulnerability, allowing unauthenticated remote attacks to inject arbitrary SQL commands to read, modify, and delete database contents.	2024-11-11	9.8	CVE-2024-11016

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
webfulcreations -- computer_repair_shop	Unrestricted Upload of File with Dangerous Type vulnerability in Webful Creations Computer Repair Shop allows Upload a Web Shell to a Web Server.This issue affects Computer Repair Shop: from n/a through 3.8115.	2024-11-11	9.8	CVE-2024-51793
WebTechGlobal--Easy CSV Importer BETA	Unrestricted Upload of File with Dangerous Type vulnerability in WebTechGlobal Easy CSV Importer BETA allows Upload a Web Shell to a Web Server.This issue affects Easy CSV Importer BETA: from n/a through 7.0.0.	2024-11-14	10	CVE-2024-52372
wedevs--WP Project Manager Task, team, and project management plugin featuring kanban board and gantt charts	The WP Project Manager - Task, team, and project management plugin featuring kanban board and gantt charts plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.6.13 via the 'Abstract_Permission' class due to missing validation on the 'user_id' user controlled key. This makes it possible for unauthenticated attackers to spoof their identity to that of an administrator and access all of the plugins REST routes.	2024-11-13	7.3	CVE-2024-10174
Wibergs Web--CSV to html	Unrestricted Upload of File with Dangerous Type vulnerability in Wibergs Web CSV to html allows Upload a Web Shell to a Web Server.This issue affects CSV to html: from n/a through 3.04.	2024-11-16	9.9	CVE-2024-52406
wpdevteam--Essential Addons for Elementor Best Elementor Addon, Templates, Widgets, Kits & WooCommerce Builders	The Essential Addons for Elementor - Best Elementor Addon, Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 6.0.9 via the 'init_content_lostpassword_user_email_controls' function. This makes it possible for authenticated attackers, with Author-level access and above, to extract sensitive data including usernames and passwords of any user, including Administrators, as long as that user opens the email notification for a password change request and images are not blocked by the email client.	2024-11-15	8	CVE-2024-8979
WPExperts--User Management	Unrestricted Upload of File with Dangerous Type vulnerability in WPExperts User Management allows Upload a Web Shell to a Web Server.This issue affects User Management: from n/a through 1.1.	2024-11-16	9.9	CVE-2024-52403
wpvividplugins--Migration, Backup, Staging WPvivid Backup & Migration	The Migration, Backup, Staging - WPvivid plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 0.9.107 via deserialization of untrusted input in the 'replace_row_data' and 'replace_serialize_data' functions. This makes it possible for unauthenticated attackers 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. An administrator must create a staging site to trigger the exploit.	2024-11-14	8.8	CVE-2024-10962
wpxpo--Post Grid Gutenberg Blocks and WordPress Blog Plugin PostX	The Post Grid Gutenberg Blocks and WordPress Blog Plugin - PostX plugin for WordPress is vulnerable to unauthorized plugin installation/activation due to a missing capability check on the 'install_required_plugin_callback' function in all versions up to, and including, 4.1.16. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install and activate arbitrary plugins which can be leveraged to achieve remote code execution if another vulnerable plugin is installed and activated.	2024-11-16	8.8	CVE-2024-10728
xwikisas--macro-pdfviewer	macro-pdfviewer is a PDF Viewer Macro for XWiki using Mozilla pdf.js. The width parameter of the PDF viewer macro isn't properly escaped, allowing XSS for any user who can edit a page. XSS can impact the confidentiality, integrity and availability of the whole XWiki installation when an admin visits the page with the malicious code. This is fixed in 2.5.6.	2024-11-13	9	CVE-2024-52300
xwikisas--macro-pdfviewer	macro-pdfviewer is a PDF Viewer Macro for XWiki using Mozilla pdf.js. The PDF Viewer macro allows an attacker to view any attachment using the "Delegate my view right" feature as long as the attacker can view a page whose last author has access to the attachment. For this, the attacker only needs to provide the reference to a PDF file to the macro. To obtain the reference of the desired attachment, the attacker can access the Page Index, Attachments tab. Even if the UI shows N/A, the user can inspect the page and check the HTTP request that fetches the live data entries. The attachment URL is available in the returned JSON for all attachments, including protected ones and allows getting the necessary values. This vulnerability is fixed in version 2.5.6.	2024-11-13	7.5	CVE-2024-52298
xwikisas--macro-pdfviewer	macro-pdfviewer is a PDF Viewer Macro for XWiki using Mozilla pdf.js. Any user with view right on XWiki.PDFViewerService can access any attachment stored in	2024-11-13	7.5	CVE-2024-52299

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the wiki as the "key" that is passed to prevent this is computed incorrectly, calling skip on the digest stream doesn't update the digest. This is fixed in 2.5.6.			
zephyrproject-rtos--Zephyr	When the Global Pointer (GP) relative addressing is enabled (CONFIG_RISCV_GP=y), the gp reg points at 0x800 bytes past the start of the .sdata section which is then used by the linker to relax accesses to global symbols.	2024-11-15	9.3	CVE-2024-11263

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1000 Projects--Bookstore Management System	A vulnerability, which was classified as problematic, has been found in 1000 Projects Bookstore Management System 1.0. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-25	4.3	CVE-2024-11673
Advantech--EKI-6333AC-2G	A CWE-798 "Use of Hard-coded Credentials" was discovered affecting the following devices manufactured by Advantech: EKI-6333AC-2G (<= 1.6.3), EKI-6333AC-2GD (<= v1.6.3) and EKI-6333AC-1GPO (<= v1.2.1). The vulnerability is associated to the backup configuration functionality that by default encrypts the archives using a static password.	2024-11-26	6.5	CVE-2024-50377
Aftab Husain--Vertical Carousel	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aftab Husain Vertical Carousel allows Stored XSS.This issue affects Vertical Carousel: from n/a through 1.0.2.	2024-11-30	6.5	CVE-2024-53756
antonbond--Additional Order Filters for WooCommerce	The Additional Order Filters for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'shipping_method_filter' parameter in all versions up to, and including, 1.21 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.	2024-11-26	6.1	CVE-2024-11418
Apache Software Foundation--Apache NimBLE	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in Apache NimBLE. Specially crafted MESH message could result in memory corruption when non-default build configuration is used. This issue affects Apache NimBLE: through 1.7.0. Users are recommended to upgrade to version 1.8.0, which fixes the issue.	2024-11-26	6.3	CVE-2024-47248
Apache Software Foundation--Apache NimBLE	Improper Validation of Array Index vulnerability in Apache NimBLE. Lack of input validation for HCI events from controller could result in out-of-bound memory corruption and crash. This issue requires broken or bogus Bluetooth controller and thus severity is considered low. This issue affects Apache NimBLE: through 1.7.0. Users are recommended to upgrade to version 1.8.0, which fixes the issue.	2024-11-26	5	CVE-2024-47249
Apache Software Foundation--Apache NimBLE	Out-of-bounds Read vulnerability in Apache NimBLE. Missing proper validation of HCI advertising report could lead to out-of-bound access when parsing HCI event and thus bogus GAP 'device found' events being sent. This issue requires broken or bogus Bluetooth controller and thus severity is considered low. This issue affects Apache NimBLE: through 1.7.0. Users are recommended to upgrade to version 1.8.0, which fixes the issue.	2024-11-26	5	CVE-2024-47250
Atlassian--Confluence Data Center	This Medium severity Security Misconfiguration vulnerability was introduced in version 8.8.1 of Confluence Data Center and Server for Windows installations. This Security Misconfiguration vulnerability, with a CVSS Score of 6.4 allows an authenticated attacker of the Windows host to read sensitive information about the Confluence Data Center configuration which has high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to the latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release greater than or equal to 7.19.18 * Confluence Data Center and Server 8.5: Upgrade to a release greater than or equal to 8.5.5 * Confluence Data Center and Server 8.7: Upgrade to a release greater than or equal to 8.7.2 * Confluence Data Center and Server 8.8: Upgrade to a release greater than or equal to 8.8.0 See the release notes (https://confluence.atlassian.com/conf88/confluence-release-notes-1354501008.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). This vulnerability was reported via our Atlassian Bug Bounty Program by Chris Elliot.	2024-11-27	6.4	CVE-2024-21703

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autolab--Autolab	Autolab is a course management service that enables auto-graded programming assignments. A user can modify their first and or last name to include a valid excel / spreadsheet formula. When an instructor downloads their course's roster and opens, this name will then be evaluated as a formula. This could lead to leakage of information of students in the course roster by sending the data to a remote endpoint. This issue has been patched in the source code repository and the fix is expected to be released in the next version. Users are advised to manually patch their systems or to wait for the next release. There are no known workarounds for this vulnerability.	2024-11-27	6.8	CVE-2024-53260
Axis Communications AB--AXIS Camera Station Pro	Seth Fogie, member of the AXIS Camera Station Pro Bug Bounty Program, has found that the Incident report feature may expose sensitive credentials on the AXIS Camera Station windows client. If Incident report is not being used with credentials configured this flaw does not apply. Axis has released patched versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	2024-11-26	6.3	CVE-2024-6749
Axis Communications AB--AXIS Camera Station Pro	Gee-netics, member of the AXIS Camera Station Pro Bug Bounty Program has found that it is possible for a non-admin user to gain system privileges by redirecting a file deletion upon service restart. Axis has released patched versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	2024-11-26	4.2	CVE-2024-6476
Axis Communications AB--AXIS Camera Station Pro	Seth Fogie, member of AXIS Camera Station Pro Bug Bounty Program has found that it is possible to edit and/or remove views without the necessary permission due to a client-side-only check. Axis has released patched versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	2024-11-26	4.4	CVE-2024-6831
Axis Communications AB--AXIS OS	51l3nc3, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API managedoverlayimages.cgi was vulnerable to a race condition attack allowing for an attacker to block access to the overlay configuration page in the web interface of the Axis device. This flaw can only be exploited after authenticating with an operator- or administrator-privileged service account. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	2024-11-26	4.3	CVE-2024-8772
ays-pro--FAQ Builder AYS	The FAQ Builder AYS plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'ays_faq_tab' parameter in all versions up to, and including, 1.7.1 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.	2024-11-28	6.1	CVE-2024-11458
backstage--backstage	The Backstage Scaffolder plugin Houses types and utilities for building scaffolder-related modules. A vulnerability is identified in Backstage Scaffolder template functionality where Server-Side Template Injection (SSTI) can be exploited to perform Git config injection. The vulnerability allows an attacker to capture privileged git tokens used by the Backstage Scaffolder plugin. With these tokens, unauthorized access to sensitive resources in git can be achieved. The impact is considered medium severity as the Backstage Threat Model recommends restricting access to adding and editing templates in the Backstage Catalog plugin. The issue has been resolved in versions `v0.4.12`, `v0.5.1` and `v0.6.1` of the `@backstage/plugin-scaffolder-node` package. Users are encouraged to upgrade to this version to mitigate the vulnerability. Users are advised to upgrade. Users unable to upgrade may ensure that templates do not change git config.	2024-11-29	5.4	CVE-2024-53983
Berg Informatik--Stripe Donation	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Berg Informatik Stripe Donation allows Stored XSS.This issue affects Stripe Donation: from n/a through 1.2.5.	2024-12-01	6.5	CVE-2024-53752

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
BlackBerry--AtHoc	A Stored Cross-Site Scripting (XSS) vulnerability in the Management Console of BlackBerry AtHoc version 7.15 could allow an attacker to potentially execute actions in the context of the victim's session.	2024-11-25	4.6	CVE-2024-51723
bluenotes--BNE Gallery Extended	The BNE Gallery Extended plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'gallery' shortcode in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-26	6.4	CVE-2024-11119
Capitalize My Title--Capitalize My Title	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Capitalize My Title allows Stored XSS.This issue affects Capitalize My Title: from n/a through 0.5.3.	2024-11-30	6.5	CVE-2024-53760
cilium--cilium	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. For users with the following configuration: 1. An allow policy that selects a Layer 3 destination and a port range `AND` 2. A Layer 7 allow policy that selects a specific port within the first policy's range the Layer 7 enforcement would not occur for the traffic selected by the Layer 7 policy. This issue only affects users who use Cilium's port range functionality, which was introduced in Cilium v1.16. This issue is patched in PR #35150. This issue affects Cilium v1.16 between v1.16.0 and v1.16.3 inclusive. This issue is patched in Cilium v1.16.4. Users are advised to upgrade. Users with network policies that match the pattern described above can work around the issue by rewriting any policies that use port ranges to individually specify the ports permitted for traffic.	2024-11-25	5.8	CVE-2024-52529
cimatti--WordPress Contact Forms by Cimatti	The WordPress Contact Forms by Cimatti plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.9.2. This is due to missing or incorrect nonce validation on the process_bulk_action function. This makes it possible for unauthenticated attackers to delete forms via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-11-27	4.3	CVE-2024-10521
cli--cli	The gh cli is GitHub's official command line tool. A security vulnerability has been identified in the GitHub CLI that could leak authentication tokens when cloning repositories containing `git` submodules hosted outside of GitHub.com and ghe.com. This vulnerability stems from several `gh` commands used to clone a repository with submodules from a non-GitHub host including `gh repo clone`, `gh repo fork`, and `gh pr checkout`. These GitHub CLI commands invoke git with instructions to retrieve authentication tokens using the `credential.helper` configuration variable for any host encountered. Prior to version `2.63.0`, hosts other than GitHub.com and ghe.com are treated as GitHub Enterprise Server hosts and have tokens sourced from the following environment variables before falling back to host-specific tokens stored within system-specific secured storage: 1. `GITHUB_ENTERPRISE_TOKEN`, 2. `GH_ENTERPRISE_TOKEN` and 3. `GITHUB_TOKEN` when the `CODESPACES` environment variable is set. The result being `git` sending authentication tokens when cloning submodules. In version `2.63.0`, these GitHub CLI commands will limit the hosts for which `gh` acts as a credential helper to source authentication tokens. Additionally, `GITHUB_TOKEN` will only be used for GitHub.com and ghe.com. Users are advised to upgrade. Additionally users are advised to revoke authentication tokens used with the GitHub CLI and to review their personal security log and any relevant audit logs for actions associated with their account or enterprise	2024-11-27	6.5	CVE-2024-53858
cli--go-gh	go-gh is a Go module for interacting with the `gh` utility and the GitHub API from the command line. A security vulnerability has been identified in `go-gh` that could leak authentication tokens intended for GitHub hosts to non-GitHub hosts when within a codespace. `go-gh` sources authentication tokens from different environment variables depending on the host involved: 1. `GITHUB_TOKEN`, `GH_TOKEN` for GitHub.com and ghe.com and 2. `GITHUB_ENTERPRISE_TOKEN`,	2024-11-27	6.5	CVE-2024-53859

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`GH_ENTERPRISE_TOKEN` for GitHub Enterprise Server. Prior to version `2.11.1`, `auth.TokenForHost` could source a token from the `GITHUB_TOKEN` environment variable for a host other than GitHub.com or ghe.com when within a codespace. In version `2.11.1`, `auth.TokenForHost` will only source a token from the `GITHUB_TOKEN` environment variable for GitHub.com or ghe.com hosts. Successful exploitation could send authentication token to an unintended host. This issue has been addressed in version 2.11.1 and all users are advised to upgrade. Users are also advised to regenerate authentication tokens and to review their personal security log and any relevant audit logs for actions associated with their account or enterprise.			
code-projects--Farmacia	A vulnerability was found in code-projects Farmacia up to 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file pagamento.php. The manipulation of the argument notaFiscal leads to sql injection. The attack can be launched remotely.	2024-11-28	6.3	CVE-2024-11968
code-projects--Farmacia	A vulnerability was found in code-projects Farmacia 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /visualizer-forneccedor.chp. 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.	2024-11-30	6.3	CVE-2024-11998
code-projects--Farmacia	A vulnerability, which was classified as critical, was found in code-projects Farmacia 1.0. This affects an unknown part of the file /visualizar-produto.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-12-01	6.3	CVE-2024-12007
code-projects--Responsive Hotel Site	A vulnerability, which was classified as critical, has been found in code-projects Responsive Hotel Site 1.0. Affected by this issue is some unknown functionality of the file /admin/room.php. The manipulation of the argument troom leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-28	6.3	CVE-2024-11963
CodeAstro--Hospital Management System	A vulnerability, which was classified as critical, was found in CodeAstro Hospital Management System 1.0. Affected is an unknown function of the file /backend/doc/his_doc_update-account.php. The manipulation of the argument doc_dpic leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-26	6.3	CVE-2024-11674
Codeless--Cowidgets Elementor Addons	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Codeless Cowidgets - Elementor Addons allows Stored XSS.This issue affects Cowidgets - Elementor Addons: from n/a through 1.2.0.	2024-11-30	6.5	CVE-2024-53786
Codezips--Free Exam Hall Seating Management System	A vulnerability was found in Codezips Free Exam Hall Seating Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file profile.php of the component Profile Image Handler. The manipulation of the argument image leads to unrestricted upload. The attack can be initiated remotely. The researcher submit confuses the vulnerability class of this issue.	2024-11-25	4.3	CVE-2024-11661
collizo4sky--Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content ProfilePress	The ProfilePress plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.15.18 via the WordPress core search feature. This makes it possible for unauthenticated attackers to extract sensitive data from posts that have been restricted to higher-level roles such as administrator.	2024-11-27	5.3	CVE-2024-11083

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cosmosfarm-- By	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ì½”ìŠ¤ëª¨ìŠ¤íŒœ - Cosmosfarm ì†Œì…œ ê³µìœ ë²„íŠ¼ By ì½”ìŠ¤ëª¨ìŠ¤íŒœ allows Stored XSS.This issue affects ì†Œì…œ ê³µìœ ë²„íŠ¼ By ì½”ìŠ¤ëª¨ìŠ¤íŒœ: from n/a through 1.9.	2024-12-01	6.5	CVE-2024-53745
creativemindssolutions--CM WordPress Search And Replace Plugin	Multiple plugins for WordPress are vulnerable to Reflected Cross-Site Scripting via the cminds_free_guide shortcode in various versions 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.	2024-11-26	6.1	CVE-2024-11202
Dell--Wyse Management Suite	Dell Wyse Management Suite, version WMS 4.4 and prior, contain a Missing Authorization vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Denial of service and arbitrary file deletion	2024-11-26	5.9	CVE-2024-49596
denoland--deno	Deno is a runtime for JavaScript and TypeScript written in rust. Several cross-site scripting vulnerabilities existed in the `deno_doc` crate which lead to Self-XSS with deno doc --html. 1.) XSS in generated `search_index.js`, `deno_doc` outputs a JavaScript file for searching. However, the generated file used `innerHTML` on unsanitzed HTML input. 2.) XSS via property, method and enum names, `deno_doc` did not sanitize property names, method names and enum names. The first XSS most likely didn't have an impact since `deno doc --html` is expected to be used locally with own packages.	2024-11-25	5.4	CVE-2024-32468
Devnex--Devnex Addons For Elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Devnex Devnex Addons For Elementor allows DOM-Based XSS.This issue affects Devnex Addons For Elementor: from n/a through 1.0.8.	2024-11-30	6.5	CVE-2024-53766
Devolutions--Remote Desktop Manager	Incorrect authorization in the permission validation component of Devolutions Remote Desktop Manager 2024.2.21 and earlier on Windows allows a malicious authenticated user to bypass the "View Password" permission via specific actions.	2024-11-25	5.4	CVE-2024-11670
Devolutions--Remote Desktop Manager	Improper authentication in SQL data source MFA validation in Devolutions Remote Desktop Manager 2024.3.17 and earlier on Windows allows an authenticated user to bypass the MFA validation via data source switching.	2024-11-25	5.4	CVE-2024-11671
Devolutions--Remote Desktop Manager	Incorrect authorization in the add permission component in Devolutions Remote Desktop Manager 2024.2.21 and earlier on Windows allows an authenticated malicious user to bypass the "Add" permission via the import in vault feature.	2024-11-25	4.3	CVE-2024-11672
Eaton--Intelligent Power Manager (IPM)	Eaton Intelligent Power Manager (IPM) prior to 1.70 is vulnerable to stored Cross site scripting. The vulnerability exists due to insufficient validation of input from certain resources by the IPM software. The attacker would need access to the local Subnet and an administrator interaction to compromise the system	2024-11-25	5.2	CVE-2021-23282
Eaton--Intelligent Power Protector (IPP)	IPP software prior to v1.71 is vulnerable to default credential vulnerability. This could lead attackers to identify and access vulnerable systems.	2024-11-25	6.7	CVE-2022-33862
Eaton--Intelligent Power Protector	IPP software versions prior to v1.71 do not sufficiently verify the authenticity of data, in a way that causes it to accept invalid data.	2024-11-25	5.1	CVE-2022-33861
elemntor--Elementor Website Builder More than	The Elementor Website Builder - More than Just a Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter of the Icon widget in all versions up to, and including, 3.25.7 due to insufficient input	2024-11-26	6.4	CVE-2024-8236

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Just a Page Builder	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.			
EnGenius--ENH1350EXT	A vulnerability was found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118. It has been classified as critical. Affected is an unknown function of the file /admin/network/wifi_schedule. The manipulation of the argument wifi_schedule_day_em_5 leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-25	4.7	CVE-2024-11651
EnGenius--ENH1350EXT	A vulnerability was found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/sn_package/sn_https. The manipulation of the argument https_enable leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-25	4.7	CVE-2024-11652
EnGenius--ENH1350EXT	A vulnerability was found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/network/diag_traceroute. The manipulation of the argument diag_traceroute leads to command 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.	2024-11-25	4.7	CVE-2024-11653
EnGenius--ENH1350EXT	A vulnerability classified as critical has been found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118. This affects an unknown part of the file /admin/network/diag_traceroute6. The manipulation of the argument diag_traceroute6 leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-25	4.7	CVE-2024-11654
EnGenius--ENH1350EXT	A vulnerability classified as critical was found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118. This vulnerability affects unknown code of the file /admin/network/diag_pinginterface. The manipulation of the argument diag_ping leads to 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.	2024-11-25	4.7	CVE-2024-11655
EnGenius--ENH1350EXT	A vulnerability, which was classified as critical, has been found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118. This issue affects some unknown processing of the file /admin/network/diag_ping6. The manipulation of the argument diag_ping6 leads to 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.	2024-11-25	4.7	CVE-2024-11656
EnGenius--ENH1350EXT	A vulnerability, which was classified as critical, was found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118. Affected is an unknown function of the file /admin/network/diag_nslookup. The manipulation of the argument diag_nslookup leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-25	4.7	CVE-2024-11657
EnGenius--ENH1350EXT	A vulnerability has been found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/network/ajax_getChannelList. The manipulation of the argument countryCode leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and	2024-11-25	4.7	CVE-2024-11658

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	may be used. The vendor was contacted early about this disclosure but did not respond in any way.			
EnGenius--ENH1350EXT	A vulnerability was found in EnGenius ENH1350EXT, ENS500-AC and ENS620EXT up to 20241118 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/network/diag_iperf. The manipulation of the argument iperf leads to command 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.	2024-11-25	4.7	CVE-2024-11659
Fintelligence--Fintelligence Calculator	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fintelligence Fintelligence Calculator allows Stored XSS.This issue affects Fintelligence Calculator: from n/a through 1.0.3.	2024-11-28	6.5	CVE-2024-53731
FlickDevs--Countdown Timer for Elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FlickDevs Countdown Timer for Elementor allows Stored XSS.This issue affects Countdown Timer for Elementor: from n/a through 1.3.6.	2024-12-01	6.5	CVE-2024-53743
FlickDevs--Elementor Button Plus	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FlickDevs Elementor Button Plus allows Stored XSS.This issue affects Elementor Button Plus: from n/a through 1.3.3.	2024-12-01	6.5	CVE-2024-53746
Gabe Livan--Asset CleanUp: Page Speed Booster	Server-Side Request Forgery (SSRF) vulnerability in Gabe Livan Asset CleanUp: Page Speed Booster allows Server Side Request Forgery.This issue affects Asset CleanUp: Page Speed Booster: from n/a through 1.3.9.8.	2024-11-30	4.4	CVE-2024-53738
GitLab--GitLab	An issue was discovered in GitLab CE/EE affecting all versions from 16.9.8 before 17.4.5, 17.5 before 17.5.3, and 17.6 before 17.6.1. Certain API endpoints could potentially allow unauthorized access to sensitive data due to overly broad application of token scopes.	2024-11-26	6.5	CVE-2024-11669
GitLab--GitLab	A Denial of Service (DoS) issue has been discovered in GitLab CE/EE affecting all versions prior to 12.6 prior to 17.4.5, 17.5 prior to 17.5.3, and 17.6 prior to 17.6.1. An attacker could cause a denial of service with a crafted cargo.toml file.	2024-11-26	6.5	CVE-2024-8237
GitLab--GitLab	An issue has been discovered in GitLab EE affecting all versions starting from 17.3 before 17.3.7, all versions starting from 17.4 before 17.4.4, all versions starting from 17.5 before 17.5.2 in which an unauthenticated user may be able to read some information about an MR in a private project, under certain circumstances.	2024-11-26	5.3	CVE-2024-10240
GitLab--GitLab	An issue was discovered in GitLab CE/EE affecting all versions starting from 15.6 prior to 17.4.5, starting from 17.5 prior to 17.5.3, starting from 17.6 prior to 17.6.1 which could cause Denial of Service via integrating a malicious harbor registry.	2024-11-26	5.3	CVE-2024-8177
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 16.11 before 17.4.5, 17.5 before 17.5.3, and 17.6 before 17.6.1. Long-lived connections could potentially bypass authentication controls, allowing unauthorized access to streaming results.	2024-11-26	4.2	CVE-2024-11668
GitLab--GitLab	A denial of service (DoS) condition was discovered in GitLab CE/EE affecting all versions from 13.2.4 before 17.4.5, 17.5 before 17.5.3, and 17.6 before 17.6.1. By leveraging this vulnerability an attacker could create a DoS condition by sending crafted API calls. This was a regression of an earlier patch.	2024-11-26	4.3	CVE-2024-11828
Google--Android	In impeg2d_bit_stream_flush() of libmpeg2dec there is a possible OOB read due to a missing bounds check. This could lead to Remote DoS with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5	CVE-2017-13320

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Google--Android	In SensorService::isDataInjectionEnabled of frameworks/native/services/sensorservice/SensorService.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-27	6.2	CVE-2017-13321
Google--Android	In mv_err_cost of mcomp.c there is a possible out of bounds read due to missing bounds check. This could lead to denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5	CVE-2018-9349
Google--Android	In ih264d_assign_pic_num of ih264d_utils.c there is a possible out of bound read due to missing bounds check. This could lead to a denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5	CVE-2018-9350
Google--Android	In ih264e_fmt_conv_420p_to_420sp of ih264e_fmt_conv.c there is a possible out of bound read due to missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5	CVE-2018-9351
Google--Android	In ihevcd_allocate_dynamic_bufs of ihevcd_api.c there is a possible resource exhaustion due to integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5	CVE-2018-9352
Google--Android	In ihevcd_parse_slice_data of ihevcd_parse_slice.c there is a possible heap buffer out of bound read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5	CVE-2018-9353
Google--Android	In VideoFrameScheduler.cpp of VideoFrameScheduler::PLL::fit, there is a possible remote denial of service due to divide by 0. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-27	6.5	CVE-2018-9354
Google--Android	In BnAudioPolicyService::onTransact of IAudioPolicyService.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-28	6.2	CVE-2018-9377
Google--Chrome	Insufficient data validation in Mojo in Google Chrome prior to 129.0.6668.89 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	2024-11-27	5.5	CVE-2024-9369
Guangzhou Huayi Intelligent Technology--Jeewms	A vulnerability was found in Guangzhou Huayi Intelligent Technology Jeewms 3.7. It has been rated as problematic. This issue affects the function preHandle of the file src/main/java/com/zzjee/wm/controller/WmOmNoticeHController.java. The manipulation of the argument request leads to information disclosure. 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.	2024-11-28	5.3	CVE-2024-11961
heateor--Social Sharing Plugin Sassy Social Share	The Social Sharing Plugin - Sassy Social Share plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the heateor_mastodon_share parameter in all versions up to, and including, 3.3.69 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.	2024-11-30	6.1	CVE-2024-11252
Hitachi Energy--NSD570 Teleprotection	A vulnerability exists in NSD570 login panel that does not restrict excessive authentication attempts. If exploited, this could cause account takeover and unauthorized access to the system when an attacker conducts brute-force attacks	2024-11-26	5.3	CVE-2024-9928

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Equipment	against the equipment login. Note that the system supports only one concurrent session and implements a delay of more than a second between failed login attempts making it difficult to automate the attacks.			
Hitachi Energy--NSD570 Teleprotection Equipment	A vulnerability exists in NSD570 that allows any authenticated user to access all device logs disclosing login information with timestamps.	2024-11-26	4.3	CVE-2024-9929
IBM--Jazz Foundation	IBM Jazz Foundation 7.0.2 and below are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2024-11-25	6.1	CVE-2023-45181
IBM--Jazz Foundation	IBM Jazz Foundation 7.0.2 and 7.0.3 could allow a user to change their dashboard using a specially crafted HTTP request due to improper access control.	2024-11-25	5.3	CVE-2023-26280
IBM--Workload Scheduler	IBM Workload Scheduler 9.5, 10.1, and 10.2 stores user credentials in plain text which can be read by a local user.	2024-11-26	5.5	CVE-2024-49351
IDE Interactive--Content Audit Exporter	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in IDE Interactive Content Audit Exporter allows Retrieve Embedded Sensitive Data.This issue affects Content Audit Exporter: from n/a through 1.1.	2024-11-30	5.3	CVE-2024-53768
intellasoftsolutions--SEO Landing Page Generator	The SEO Landing Page 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, 1.66.2. 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.	2024-11-28	6.1	CVE-2024-11366
iseardmedia--Kudos Donations Easy donations and payments with Mollie	The Kudos Donations - Easy donations and payments with Mollie plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 's' parameter in all versions up to, and including, 3.2.9 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-11-28	6.1	CVE-2024-11684
iseardmedia--Kudos Donations Easy donations and payments with Mollie	The `Kudos Donations - Easy donations and payments with Mollie` 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, 3.2.9. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute if they can successfully trick a user into performing an action, such as clicking on a specially crafted link.	2024-11-28	6.1	CVE-2024-11685
jegtheme--Jeg Elementor Kit	The Jeg Elementor Kit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's JKit - Countdown widget in all versions up to, and including, 2.6.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-26	6.4	CVE-2024-10308
jegtheme--Jeg Elementor Kit	The Jeg Elementor Kit plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.6.9 via the render_content function in class/elements/views/class-tabs-view.php. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft template data.	2024-11-26	4.3	CVE-2024-8899

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Jenkins Project--Jenkins Filesystem List Parameter Plugin	Jenkins Filesystem List Parameter Plugin 0.0.14 and earlier does not restrict the path used for the File system objects list Parameter, allowing attackers with Item/Configure permission to enumerate file names on the Jenkins controller file system.	2024-11-27	4.3	CVE-2024-54004
jonkastonka--Sp*tify Play Button for WordPress	The Spotify Play Button for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's spotifyplaybutton shortcode in all versions up to, and including, 2.11 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-26	6.4	CVE-2024-11192
labibahmed42--Pricing Tables For WPBakery Page Builder (formerly Visual Composer)	The Pricing Tables For WPBakery Page Builder (formerly Visual Composer) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wdo_pricing_tables shortcode in all versions up to, and including, 1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-27	6.4	CVE-2024-10175
labsai--EDDI	E.D.D.I (Enhanced Dialog Driven Interface) is a middleware to connect and manage LLM API bots. A path traversal vulnerability exists in the backup export functionality of EDDI, as implemented in `RestExportService.java`. This vulnerability allows an attacker to access sensitive files on the server by manipulating the `botFilename` parameter in requests. The application fails to sanitize user input, enabling malicious inputs such as `..%2f..%2fetc%2fpasswd` to access arbitrary files. However, the **severity of this vulnerability is significantly limited** because EDDI typically runs within a **Docker container**, which provides additional layers of isolation and restricted permissions. As a result, while this vulnerability exposes files within the container, it does not inherently threaten the underlying host system or other containers. A patch is required to sanitize and validate the botFilename input parameter. Users should ensure they are using version 5.4 which contains this patdch. For temporary mitigation, access to the vulnerable endpoint should be restricted through firewall rules or authentication mechanisms.	2024-11-26	6.3	CVE-2024-53844
legalweb--LegalWeb Cloud	The LegalWeb Cloud plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'legalweb-popup' shortcode in all versions up to, and including, 1.1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-28	6.4	CVE-2024-11761
logichunt--Counter Up Animated Number Counter & Milestone Showcase	The Counter Up - Animated Number Counter & Milestone Showcase plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'lgx-counter' shortcode in all versions up to, and including, 2.4.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-27	6.4	CVE-2024-10895
man4toman--Parsi Date	The Parsi Date 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, 5.1.1. 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.	2024-11-26	6.1	CVE-2024-11032
Mozilla--Firefox for iOS	Accessing a non-secure HTTP site that uses a non-existent port may cause the SSL padlock icon in the location URL bar to, misleadingly, appear secure. This vulnerability affects Firefox for iOS < 133.	2024-11-26	5.4	CVE-2024-53975

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Mozilla--Firefox for iOS	Under certain circumstances, navigating to a webpage would result in the address missing from the location URL bar, making it unclear what the URL was for the loaded webpage. This vulnerability affects Firefox for iOS < 133.	2024-11-26	5.4	CVE-2024-53976
Mozilla--Firefox	Enhanced Tracking Protection's Strict mode may have inadvertently allowed a CSP `frame-src` bypass and DOM-based XSS through the Google SafeFrame shim in the Web Compatibility extension. This issue could have exposed users to malicious frames masquerading as legitimate content. This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Firefox ESR < 115.18, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	6.1	CVE-2024-11694
Mozilla--Firefox	A null pointer dereference may have inadvertently occurred in `pk12util`, and specifically in the `SEC_ASN1DecodeItem_Util` function, when handling malformed or improperly formatted input files. This vulnerability affects Firefox < 133 and Thunderbird < 133.	2024-11-26	6.5	CVE-2024-11706
Mozilla--Firefox	Missing thread synchronization primitives could have led to a data race on members of the PlaybackParams structure. This vulnerability affects Firefox < 133 and Thunderbird < 133.	2024-11-26	6.5	CVE-2024-11708
Mozilla--Firefox	A crafted URL containing Arabic script and whitespace characters could have hidden the true origin of the page, resulting in a potential spoofing attack. This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	5.4	CVE-2024-11695
Mozilla--Firefox	An attacker could cause a select dropdown to be shown over another tab; this could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 133, Firefox ESR < 128.5, Thunderbird < 133, and Thunderbird < 128.5.	2024-11-26	4.3	CVE-2024-11692
Mozilla--Firefox	The incorrect domain may have been displayed in the address bar during an interrupted navigation attempt. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 133 and Thunderbird < 133.	2024-11-26	4.3	CVE-2024-11701
Mozilla--Nunjucks	In Nunjucks versions prior to version 3.2.4, it was possible to bypass the restrictions which are provided by the autoescape functionality. If there are two user-controlled parameters on the same line used in the views, it was possible to inject cross site scripting payloads using the backslash \ character.	2024-11-26	6.1	CVE-2023-2142
n/a--n/a	pyspider through 0.3.10 allows /update XSS. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	2024-11-29	6.1	CVE-2024-39162
n/a--n/a	Local File Inclusion (LFI) vulnerability has been discovered in TCPDF 6.7.5. This vulnerability enables a user to read arbitrary files from the server's file system through <img> src tag, potentially exposing sensitive information.	2024-11-26	6.2	CVE-2024-51058
n/a--n/a	An issue in TOTOLINK-CX-A3002RU V1.0.4-B20171106.1512 and TOTOLINK-CX-N150RT V2.1.6-B20171121.1002 and TOTOLINK-CX-N300RT V2.1.6-B20170724.1420 and TOTOLINK-CX-N300RT V2.1.8-B20171113.1408 and TOTOLINK-CX-N300RT V2.1.8-B20191010.1107 and TOTOLINK-CX-N302RE V2.0.2-B20170511.1523 allows a remote attacker to execute arbitrary code via the /boafrm/formSysCmd component.	2024-11-27	6.8	CVE-2024-51228
n/a--n/a	An Open Redirect vulnerability in Taiga v6.8.1 allows attackers to redirect users to arbitrary websites via appending a crafted link to /login?next= in the login page URL.	2024-11-25	6.1	CVE-2024-53556
n/a--n/a	masterstack_imgcap v0.0.1 was discovered to contain a SQL injection vulnerability via the endpoint /submit.	2024-11-25	6.3	CVE-2024-53597

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	An authenticated arbitrary file upload vulnerability in the Documents module of SPIP v4.3.3 allows attackers to execute arbitrary code via uploading a crafted PDF file.	2024-11-26	6.3	CVE-2024-53619
n/a--n/a	Backdrop CMS before 1.28.4 and 1.29.x before 1.29.2 allows XSS via an SVG document, if the SVG tag is allowed for a text format.	2024-11-29	6.1	CVE-2024-54123
n/a--n/a	In FFmpeg version n6.1.1, specifically within the avcodec/speexdec.c module, a potential security vulnerability exists due to insufficient validation of certain parameters when parsing Speex codec extradata. This vulnerability could lead to integer overflow conditions, potentially resulting in undefined behavior or crashes during the decoding process.	2024-11-29	5.5	CVE-2024-35369
n/a--n/a	FFmpeg n6.1.1 has a vulnerability in the WAVARC decoder of the libavcodec library which allows for an integer overflow when handling certain block types, leading to a denial-of-service (DoS) condition.	2024-11-29	5.3	CVE-2024-36619
n/a--n/a	Zulip 8.3 is vulnerable to Cross Site Scripting (XSS) via the construct_copy_div function in copy_and_paste.js.	2024-11-29	5.4	CVE-2024-36624
n/a--n/a	Zulip 8.3 is vulnerable to Cross Site Scripting (XSS) via the replace_emoji_with_text function in ui_util.ts.	2024-11-29	5.4	CVE-2024-36625
n/a--n/a	In prestashop 8.1.4, a NULL pointer dereference was identified in the math_round function within Tools.php.	2024-11-29	5.3	CVE-2024-36626
n/a--n/a	WithSecure Elements Agent for Mac before 24.3, MDR before 24.3, and Elements Client Security for Mac before 16.10 allow a remote Denial of Service.	2024-11-29	5.5	CVE-2024-47193
n/a--n/a	A stored cross-site scripting (XSS) vulnerability was identified in PHPGURUKUL Vehicle Parking Management System v1.13 in /users/profile.php. This vulnerability allows authenticated users to inject malicious XSS scripts into the profile name field.	2024-11-26	5.4	CVE-2024-53365
n/a--n/a	A cross-site scripting (XSS) vulnerability in the /scroll.php endpoint of LafeLabs Chaos v0.0.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	2024-11-25	5.4	CVE-2024-53599
n/a--n/a	WikiDocs before 1.0.65 allows stored XSS by authenticated users via data that comes after $$\\, which is mishandled by a KaTeX parser.	2024-11-25	5.4	CVE-2024-53930
n/a--n/a	Quectel EC25-EUX EC25EUXGAR08A05M1G was discovered to contain a stack overflow.	2024-11-27	4.2	CVE-2024-37816
n/a--n/a	OpenVidReview 1.0 is vulnerable to Cross Site Scripting (XSS) in review names.	2024-11-27	4.8	CVE-2024-46055
n/a--n/a	A cross-site scripting (XSS) vulnerability in the Article module of SPIP v4.3.3 allows authenticated attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Title parameter.	2024-11-26	4.8	CVE-2024-53620
n/a--n/a	A Reflected Cross Site Scripting (XSS) vulnerability was found in /covid-tms/patient-search-report.php in PHPGurukul COVID 19 Testing Management System v1.0, which allows remote attackers to execute arbitrary code via the searchdata POST request parameter.	2024-11-27	4.8	CVE-2024-53635
n/a--n/a	stalld through 1.19.7 allows local users to cause a denial of service (file overwrite) via a /tmp/rtthrottle symlink attack.	2024-11-29	4.1	CVE-2024-54159
NEC Corporation--UNIVERGE IX	Cross-site request forgery (CSRF) vulnerability in NEC Corporation UNIVERGE IX from Ver9.2 to Ver10.10.21, for Ver10.8 up to Ver10.8.27 and for Ver10.9 up to Ver10.9.14 allows a attacker to hijack the authentication of screens on the device via the management interface.	2024-11-29	4.3	CVE-2024-11014

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
NetWin--SurgeMail	A Cross-Site Scripting (XSS) vulnerability in SurgeMail v78c2 could allow an attacker to execute arbitrary JavaScript code via an elaborate payload injected into vulnerable parameters.	2024-11-29	4.6	CVE-2024-11990
nicheaddons--Primary Addon for Elementor	The Primary Addon for Elementor plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.6.2 via the [prim_elementor_template] shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created with Elementor that they should not have access to.	2024-11-28	4.3	CVE-2024-10670
nicheaddons--Restaurant & Cafe Addon for Elementor	The Restaurant & Cafe Addon for Elementor plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.5.9 via the 'narestaurant_elementor_template' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created by Elementor that they should not have access to.	2024-11-28	4.3	CVE-2024-10780
NuttTaro--Video Player for WPBakery	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NuttTaro Video Player for WPBakery allows Stored XSS.This issue affects Video Player for WPBakery: from n/a through 1.0.1.	2024-12-01	6.5	CVE-2024-53747
pagup--Internal Linking for SEO traffic & Ranking Auto internal links (100% automatic)	The Internal Linking for SEO traffic & Ranking - Auto internal links (100% automatic) plugin for WordPress is vulnerable to time-based SQL Injection via the 'post_id' parameter in all versions up to, and including, 1.2.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-11-27	4.9	CVE-2024-11009
PickPlugins--Mail Picker	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PickPlugins Mail Picker allows DOM-Based XSS.This issue affects Mail Picker: from n/a through 1.0.14.	2024-11-30	6.5	CVE-2024-53772
Pixobe--Pixobe Cartography	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pixobe Pixobe Cartography allows DOM-Based XSS.This issue affects Pixobe Cartography: from n/a through 1.0.1.	2024-11-30	6.5	CVE-2024-53767
pluggabl--Booster for WooCommerce	The Booster for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wcj_product_meta shortcode in all versions up to, and including, 7.2.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with ShopManager-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-26	5.5	CVE-2024-9170
Plugin Devs--Post Carousel Slider for Elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Plugin Devs Post Carousel Slider for Elementor allows Stored XSS.This issue affects Post Carousel Slider for Elementor: from n/a through 1.4.0.	2024-12-01	6.5	CVE-2024-53749
Portfoliohub--WordPress Portfolio Builder Portfolio Gallery	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Portfoliohub WordPress Portfolio Builder - Portfolio Gallery allows Stored XSS.This issue affects WordPress Portfolio Builder - Portfolio Gallery: from n/a through 1.1.7.	2024-11-30	5.9	CVE-2024-53788
Praca.pl sp. z o.o.--Znajd Prac z Praca.pl	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Praca.Pl sp. Z o.O. ZnajdÅº PracÄ™ z Praca.Pl allows DOM-Based XSS.This issue affects ZnajdÅº PracÄ™ z Praca.Pl: from n/a through 2.2.3.	2024-11-30	6.5	CVE-2024-53773

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
r00tsector--HLS Player	The HLS Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'hls_player' shortcode in all versions up to, and including, 1.0.10 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-28	6.4	CVE-2024-11333
ragicsupport--Ragic Shortcode	The Ragic Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ragic' shortcode in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-28	6.4	CVE-2024-11431
realmag777--InPost Gallery	The The InPost Gallery plugin for WordPress is vulnerable to arbitrary shortcode execution via the inpost_gallery_get_shortcode_template AJAX action in all versions up to, and including, 2.1.4.2. 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.	2024-11-26	6.3	CVE-2024-11002
Red Hat--Red Hat Ansible Automation Platform 2	A vulnerability was found in the Ansible Automation Platform (AAP). This flaw allows attackers to escalate privileges by improperly leveraging read-scoped OAuth2 tokens to gain write access. This issue affects API endpoints that rely on ansible_base.oauth2_provider for OAuth2 authentication. While the impact is limited to actions within the user's assigned permissions, it undermines scoped access controls, potentially allowing unintended modifications in the application and consuming services.	2024-11-25	5	CVE-2024-11483
Red Hat--Red Hat build of Keycloak 24	A vulnerability was found in the Keycloak-services package. If untrusted data is passed to the SearchQueryUtils method, it could lead to a denial of service (DoS) scenario by exhausting system resources due to a Regex complexity.	2024-11-25	6.5	CVE-2024-10270
Red Hat--Red Hat build of Keycloak 24	A flaw was found in Keycloak. This issue occurs because sensitive runtime values, such as passwords, may be captured during the Keycloak build process and embedded as default values in bytecode, leading to unintended information disclosure. In Keycloak 26, sensitive data specified directly in environment variables during the build process is also stored as a default values, making it accessible during runtime. Indirect usage of environment variables for SPI options and Quarkus properties is also vulnerable due to unconditional expansion by PropertyMapper logic, capturing sensitive data as default values in all Keycloak versions up to 26.0.2.	2024-11-25	5.9	CVE-2024-10451
Red Hat--Red Hat build of Keycloak 24	A vulnerability was found in the Keycloak Server. The Keycloak Server is vulnerable to a denial of service (DoS) attack due to improper handling of proxy headers. When Keycloak is configured to accept incoming proxy headers, it may accept non-IP values, such as obfuscated identifiers, without proper validation. This issue can lead to costly DNS resolution operations, which an attacker could exploit to tie up IO threads and potentially cause a denial of service. The attacker must have access to send requests to a Keycloak instance that is configured to accept proxy headers, specifically when reverse proxies do not overwrite incoming headers, and Keycloak is configured to trust these headers.	2024-11-25	4.7	CVE-2024-9666
Red Hat--Red Hat Enterprise Linux 7 Extended Lifecycle Support	A log spoofing flaw was found in the Tuned package due to improper sanitization of some API arguments. This flaw allows an attacker to pass a controlled sequence of characters; newlines can be inserted into the log. Instead of the 'evil' the attacker could mimic a valid TuneD log line and trick the administrator. The quotes '' are usually used in TuneD logs citing raw user input, so there will always be the ' character ending the spoofed input, and the administrator can easily overlook this. This logged string is later used in logging and in the output of utilities, for example,	2024-11-26	5.5	CVE-2024-52337

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`tuned-adm get_instances` or other third-party programs that use Tuned's D-Bus interface for such operations.			
Red Hat--Red Hat OpenShift Container Platform 4	A flaw was found in OpenShift Console. A Server Side Request Forgery (SSRF) attack can happen if an attacker supplies all or part of a URL to the server to query. The server is considered to be in a privileged network position and can often reach exposed services that aren't readily available to clients due to network filtering. Leveraging such an attack vector, the attacker can have an impact on other services and potentially disclose information or have other nefarious effects on the system. The /api/dev-console/proxy/internet endpoint on the OpenShit Console allows authenticated users to have the console's pod perform arbitrary and fully controlled HTTP(s) requests. The full response to these requests is returned by the endpoint. While the name of this endpoint suggests the requests are only bound to the internet, no such checks are in place. An authenticated user can therefore ask the console to perform arbitrary HTTP requests from outside the cluster to a service inside the cluster.	2024-11-25	5.3	CVE-2024-6538
Rejuan Ahamed--Best Addons for Elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rejuan Ahamed Best Addons for Elementor allows Stored XSS.This issue affects Best Addons for Elementor: from n/a through 1.0.5.	2024-11-30	6.5	CVE-2024-53763
rswebstudios--Image Alt Text	The Image Alt Text plugin for WordPress is vulnerable to unauthorized modification of data| due to a missing capability check on the iat_add_alt_txt_action and iat_update_alt_txt_action AJAX actions in all versions up to, and including, 2.0.0. This makes it possible for authenticated attackers, with subscriber-level access and above, to update the alt text on arbitrary images.	2024-11-28	4.3	CVE-2024-11918
sanskritforum--Skt NURCaptcha	The Skt NURCaptcha plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.5.0. This is due to missing or incorrect nonce validation in the skt-nurc-admin.php file. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-11-26	6.1	CVE-2024-11342
sayedulsayem--Support SVG Upload svg files in wordpress without hassle	The Support SVG - Upload svg files in wordpress without hassle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REST API SVG File uploads 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 Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-11-26	6.4	CVE-2024-11091
Sergio Mic--SimpleSchema	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sergio MicÃ³ SimpleSchema allows DOM-Based XSS.This issue affects SimpleSchema: from n/a through 1.7.6.9.	2024-11-30	6.5	CVE-2024-53771
Sharp Corporation--Multiple MFPs (multifunction printers)	Affected devices create coredump files when crashed, storing them with world-readable permission. Any local user of the device can examine the coredump files, and research the memory contents. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	2024-11-26	5.9	CVE-2024-28955
Sharp Corporation--Multiple MFPs (multifunction printers)	User passwords are decrypted and stored on memory before any user logged in. Those decrypted passwords can be retrieved from the coredump file. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	2024-11-26	5.9	CVE-2024-29146
Sharp Corporation--Multiple MFPs (multifunction	User passwords are decrypted and stored on memory before any user logged in. Those decrypted passwords can be retrieved from the coredump file. As for the	2024-11-26	5.9	CVE-2024-29978

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
printers)	details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].			
Sharp Corporation--Multiple MFPs (multifunction printers)	User passwords are decrypted and stored on memory before any user logged in. Those decrypted passwords can be retrieved from the coredump file. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	2024-11-26	5.9	CVE-2024-32151
Sharp Corporation--Multiple MFPs (multifunction printers)	Admin authentication can be bypassed with some specific invalid credentials, which allows logging in with an administrative privilege. Sharp Corporation states the telnet feature is implemented on older models only, and is planning to provide the firmware update to remove the feature. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	2024-11-26	5.3	CVE-2024-33616
Sharp Corporation--Multiple MFPs (multifunction printers)	The web interface of the affected devices is designed to hide the LDAP credentials even for administrative users. But configuring LDAP authentication to "SIMPLE", the device communicates with the LDAP server in clear-text. The LDAP password can be retrieved from this clear-text communication. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	2024-11-26	5.3	CVE-2024-34162
Siempelkamp--UmweltOffice	A low privileged remote attacker can insert a SQL injection in the web application due to improper handling of HTTP request input data which allows to exfiltrate all data.	2024-11-28	6.5	CVE-2024-8308
sigstore--sigstore-java	sigstore-java is a sigstore java client for interacting with sigstore infrastructure. sigstore-java has insufficient verification for a situation where a validly-signed but "mismatched" bundle is presented as proof of inclusion into a transparency log. This bug impacts clients using any variation of KeylessVerifier.verify(). The verifier may accept a bundle with an unrelated log entry, cryptographically verifying everything but fails to ensure the log entry applies to the artifact in question, thereby "verifying" a bundle without any proof the signing event was logged. This allows the creation of a bundle without fulcio certificate and private key combined with an unrelated but time-correct log entry to fake logging of a signing event. A malicious actor using a compromised identity may want to do this to prevent discovery via rekor's log monitors. The signer's identity will still be available to the verifier. The signature on the bundle must still be on the correct artifact for the verifier to pass. sigstore-gradle-plugin and sigstore-maven-plugin are not affected by this as they only provide signing functionality. This issue has been patched in v1.1.0 release with PR #856. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-11-26	5.5	CVE-2024-53267
Skybootstrap--Elementor Image Gallery Plugin	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Skybootstrap Elementor Image Gallery Plugin allows Stored XSS.This issue affects Elementor Image Gallery Plugin: from n/a through 1.0.3.	2024-12-01	6.5	CVE-2024-53744
SMA--Sunny Central SC 1760-US	An authenticated attacker with low privileges may use a SQL Injection vulnerability in the affected products administration panel to gain read and write access to a specific log file of the device.	2024-11-27	5.4	CVE-2024-11025
smub--Sugar Calendar Event Calendar, Event Tickets, and Event Management Platform	The Sugar Calendar - Simple Event Management 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, 3.3.0. 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.	2024-11-26	6.1	CVE-2024-10878

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SocialEvolution--WP Find Your Nearest	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SocialEvolution WP Find Your Nearest allows Stored XSS.This issue affects WP Find Your Nearest: from n/a through 0.3.1.	2024-11-30	6.5	CVE-2024-53757
SoftHopper--Softtemplates For Elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SoftHopper Softtemplates For Elementor allows DOM-Based XSS.This issue affects Softtemplates For Elementor: from n/a through 1.0.8.	2024-11-30	6.5	CVE-2024-53764
SourceCodester--Best House Rental Management System	A vulnerability classified as critical has been found in SourceCodester Best House Rental Management System 1.0. This affects an unknown part of the file /rental/ajax.php?action=delete_tenant of the component POST Request Handler. The manipulation of the argument id leads to improper authorization. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-27	6.5	CVE-2024-11860
SourceCodester--Best House Rental Management System	A vulnerability, which was classified as problematic, was found in SourceCodester Best House Rental Management System 1.0. Affected is an unknown function of the file /rental/ajax.php?action=delete_user of the component POST Request Handler. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-26	4.3	CVE-2024-11743
Sparkle WP--Sparkle Elementor Kit	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sparkle WP Sparkle Elementor Kit allows DOM-Based XSS.This issue affects Sparkle Elementor Kit: from n/a through 2.0.9.	2024-11-30	6.5	CVE-2024-53774
streamweasels--StreamWeasels YouTube Integration	The StreamWeasels YouTube Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'sw-youtube-embed' shortcode in all versions up to, and including, 1.3.6 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.	2024-11-28	6.4	CVE-2024-11788
subratamal--Wallet for WooCommerce	The Wallet for WooCommerce plugin for WordPress is vulnerable to incorrect conversion between numeric types in all versions up to, and including, 1.5.6. This is due to a numerical logic flaw when transferring funds to another user. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create funds during a transfer and distribute these funds to any number of other users or their own account, rendering products free. Attackers could also request to withdraw funds if the Wallet Withdrawal extension is used and the request is approved by an administrator.	2024-11-28	6.5	CVE-2024-7747
SUSE--hackweek	Missing sanitation of inputs allowed arbitrary users to conduct a stored XSS attack that triggers for users that view a certain project	2024-11-28	5.7	CVE-2024-52283
SUSE--SUSE Manager Server 5.0	The uyuni-server-attestation systemd service needs a database_password environment variable. This file has 640 permission, and cannot be shown users, but the environment is still exposed by systemd to non-privileged users.	2024-11-28	5.5	CVE-2024-22037
Tenda--FH451	A vulnerability classified as problematic was found in Tenda FH451, FH1201, FH1202 and FH1206 up to 20241129. Affected by this vulnerability is the function websReadEvent of the file /goform/GetIPTV. The manipulation of the argument Content-Length leads to null pointer dereference. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-30	4.3	CVE-2024-12002
Tenda--i9	A vulnerability was found in Tenda i9 1.0.0.8(3828) and classified as critical. This issue affects the function websReadEvent of the file /goform/GetIPTV. The	2024-11-25	6.5	CVE-2024-11650

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	manipulation leads to null pointer dereference. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.			
Terry Lin--WP MathJax	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Terry Lin WP MathJax allows Stored XSS.This issue affects WP MathJax: from n/a through 1.0.1.	2024-11-30	6.5	CVE-2024-53758
Terry Lin--WP Mermaid	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Terry Lin WP Mermaid allows Stored XSS.This issue affects WP Mermaid: from n/a through 1.0.2.	2024-12-01	6.5	CVE-2024-53748
themeisle--Otter Blocks Gutenberg Blocks, Page Builder for Gutenberg Editor & FSE	The Otter Blocks - Gutenberg Blocks, Page Builder for Gutenberg Editor & FSE plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 3.0.6 via the get_image function. This makes it possible for unauthenticated attackers to view arbitrary images on the server, which can contain sensitive information.	2024-11-27	5.3	CVE-2024-11219
treeverse--lakeFS	lakeFS is an open-source tool that transforms object storage into a Git-like repository. Existing lakeFS users who have issued credentials to users who have been deleted are affected by this vulnerability. When creating a new user with the same username as a deleted user, that user will inherit all of the previous user's credentials. This issue has been addressed in release version 1.33.0 and all users are advised to upgrade. The only known workaround for those who cannot upgrade is to not reuse usernames.	2024-11-26	5.7	CVE-2024-43784
tychesoftwares--Product Input Fields for WooCommerce	The Product Input Fields for WooCommerce plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.9 via the handle_downloads() function due to insufficient file path validation/sanitization. This makes it possible for authenticated attackers, with Contributor-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	2024-11-26	6.5	CVE-2024-10857
Unknown--adBuddy+ (AdBlocker Detection) by NetfunkDesign	The adBuddy+ (AdBlocker Detection) by NetfunkDesign WordPress plugin through 1.1.3 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).	2024-11-28	4.8	CVE-2024-10510
Unknown--Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows)	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) WordPress plugin before 5.10.3 does not validate and escape some of its block options 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.	2024-11-28	5.4	CVE-2024-10493
Unknown--Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid, Carousel and Remote Arrows)	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid, Carousel and Remote Arrows) WordPress plugin before 5.10.3 does not validate and escape some of its Cookie Consent block options 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.	2024-11-29	5.4	CVE-2024-10980

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Unknown--Everest Forms	The Everest Forms WordPress plugin before 3.0.4.2 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).	2024-11-26	4.8	CVE-2024-10471
Unknown--Logo Slider	The Logo Slider WordPress plugin before 4.5.0 does not sanitise and escape some of its Logo Settings when outputing them in pages where the Logo Slider shortcode is embed, which could allow users with a role as low as Author to perform Cross-Site Scripting attacks.	2024-11-28	5.4	CVE-2024-10473
Unknown--Logo Slider	The Logo Slider WordPress plugin before 4.5.0 does not sanitise and escape some of its Logo and Slider settings, which could allow high privilege users such as Contributor to perform Stored Cross-Site Scripting	2024-11-28	5.4	CVE-2024-10896
Unknown--Photo Gallery by 10Web	The Photo Gallery by 10Web WordPress plugin before 1.8.31 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).	2024-11-29	4.8	CVE-2024-10704
Unknown--Photo Gallery, Sliders, Proofing and Themes	The Photo Gallery, Sliders, Proofing and WordPress plugin before 3.59.5 does not sanitise and escape some of its Images 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)	2024-11-25	4.8	CVE-2024-6393
Unknown--WPForms	The WPForms WordPress plugin before 1.9.1.6 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).	2024-11-25	4.8	CVE-2024-7056
Unknown--YaDisk Files	The YaDisk Files WordPress plugin through 1.2.5 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	2024-11-25	6.8	CVE-2024-10709
vinoth06--Random Banner	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in vinoth06 Random Banner allows Stored XSS.This issue affects Random Banner: from n/a through 4.2.9.	2024-11-30	6.5	CVE-2024-53787
VMware--VMware Aria Operations	VMware Aria Operations contains a stored cross-site scripting vulnerability. A malicious actor with editing access to email templates might inject malicious script leading to stored cross-site scripting in the product VMware Aria Operations.	2024-11-26	6.8	CVE-2024-38833
VMware--VMware Aria Operations	VMware Aria Operations contains a stored cross-site scripting vulnerability. A malicious actor with editing access to cloud provider might be able to inject malicious script leading to stored cross-site scripting in the product VMware Aria Operations.	2024-11-26	6.5	CVE-2024-38834
welliamcao--OpsManage	A vulnerability was found in welliamcao OpsManage 3.0.1/3.0.2/3.0.3/3.0.4/3.0.5. It has been rated as critical. This issue affects the function deploy_host_vars of the file /apps/api/views/deploy_api.py of the component API Endpoint. The manipulation leads to deserialization. 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.	2024-11-25	6.3	CVE-2024-11662
WP Mailster--WP Mailster	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Mailster allows Stored XSS.This issue affects WP Mailster: from n/a through 1.8.16.0.	2024-11-28	6.5	CVE-2024-53737
wpdevteam--EmbedPress Embed PDF, PDF 3D FlipBook,	The EmbedPress - Embed PDF, 3D Flipbook, Social Feeds, Google Docs, Vimeo, Wistia, YouTube Videos, Audios, Google Maps in Gutenberg Block & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'provider_name parameter in all versions up to, and including, 4.1.3 due to	2024-11-28	6.4	CVE-2024-11203

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Instagram Social Feeds, Google Docs, Vimeo, Wistia, YouTube Videos, Maps & Upload PDF Documents	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.			
wphostingdev--Login with Vipps and MobilePay	The Login with Vipps and MobilePay plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'continue-with-vipps' shortcode in all versions up to, and including, 1.3.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-28	6.4	CVE-2024-11786
wpmudev--Hustle Email Marketing, Lead Generation, Optins, Popups	The Hustle - Email Marketing, Lead Generation, Optins, Popups plugin for WordPress is vulnerable to unauthorized form submissions due to a missing capability check on the submit_form() function in all versions up to, and including, 7.8.5. This makes it possible for unauthenticated attackers to submit unpublished forms.	2024-11-27	5.3	CVE-2024-10580
wpmudev--Hustle Email Marketing, Lead Generation, Optins, Popups	The Hustle - Email Marketing, Lead Generation, Optins, Popups plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the preview_module() function in all versions up to, and including, 7.8.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view unpublished forms.	2024-11-26	4.3	CVE-2024-10579
wproyal--Royal Elementor Addons and Templates	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.7.1003 via the 'wpr-template' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created via Elementor that they should not have access to.	2024-11-28	4.3	CVE-2024-10798
Zabbix--Zabbix	The implementation of atob in "Zabbix JS" allows to create a string with arbitrary content and use it to access internal properties of objects.	2024-11-26	6.5	CVE-2024-36463
Zabbix--Zabbix	There was discovered a use after free bug in browser.c in the es_browser_get_variant function	2024-11-27	4.4	CVE-2024-42326
115cms -- 115cms	A vulnerability was found in 115cms up to 20240807 and classified as problematic. This issue affects some unknown processing of the file /app/admin/view/web_user.html. The manipulation of the argument ks leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-20	6.1	CVE-2024-11488
115cms -- 115cms	A vulnerability was found in 115cms up to 20240807. It has been classified as problematic. Affected is an unknown function of the file /index.php/admin/web/file.html. The manipulation of the argument ks leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-20	6.1	CVE-2024-11489
115cms -- 115cms	A vulnerability was found in 115cms up to 20240807. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /index.php/admin/web/set.html. The manipulation of the argument type leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-20	6.1	CVE-2024-11490

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
115cms -- 115cms	A vulnerability classified as problematic has been found in 115cms up to 20240807. This affects an unknown part of the file /index.php/admin/web/appurladd.html. The manipulation of the argument tid leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-20	6.1	CVE-2024-11492
115cms -- 115cms	A vulnerability classified as problematic was found in 115cms up to 20240807. This vulnerability affects unknown code of the file /index.php/setpage/admin/pageAE.html. The manipulation of the argument tid leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-20	6.1	CVE-2024-11493
cesanta -- mongoose	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and force the application to read unintended heap memory space.	2024-11-18	5.3	CVE-2024-42387
cesanta -- mongoose	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and force the application to read unintended heap memory space.	2024-11-18	5.3	CVE-2024-42388
cesanta -- mongoose	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and force the application to read unintended heap memory space.	2024-11-18	5.3	CVE-2024-42389
cesanta -- mongoose	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and force the application to read unintended heap memory space.	2024-11-18	5.3	CVE-2024-42390
cesanta -- mongoose	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and force the application to read unintended heap memory space.	2024-11-18	5.3	CVE-2024-42391
code4berry -- decoration_management_system	A vulnerability, which was classified as problematic, was found in Code4Berry Decoration Management System 1.0. This affects an unknown part of the file /decoration/admin/user_permission.php of the component User Permission Handler. The manipulation leads to permission issues. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-20	4.3	CVE-2024-11486
django-cms -- django_cms	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in django CMS Association django-cms allows Cross-Site Scripting (XSS).This issue affects django-cms: 3.11.7, 3.11.8, 4.1.2, 4.1.3.	2024-11-18	4.8	CVE-2024-11319
dlink -- di-8003_firmware	D-LINK DI-8003 v16.07.16A1 was discovered to contain a buffer overflow via the fn parameter in the tgfile_htm function.	2024-11-20	4.9	CVE-2024-52754
dlink -- di-8003_firmware	D-LINK DI-8003 v16.07.26A1 was discovered to contain a buffer overflow via the host_ip parameter in the ipsec_road_asp function.	2024-11-21	4.9	CVE-2024-52755
dlink -- di-8003_firmware	D-LINK DI-8003 v16.07.16A1 was discovered to contain a buffer overflow via the notify parameter in the arp_sys_asp function.	2024-11-20	4.9	CVE-2024-52757
f4dev -- f4_improvements	The F4 Improvements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.9.0 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.	2024-11-21	5.4	CVE-2024-9442

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fedoralovespython -- lxml_html_clean	lxml_html_clean is a project for HTML cleaning functionalities copied from `lxml.html.clean`. Prior to version 0.4.0, the HTML Parser in lxml does not properly handle context-switching for special HTML tags such as `<svg>`, `<math>` and `<noscript>`. This behavior deviates from how web browsers parse and interpret such tags. Specifically, content in CSS comments is ignored by lxml_html_clean but may be interpreted differently by web browsers, enabling malicious scripts to bypass the cleaning process. This vulnerability could lead to Cross-Site Scripting (XSS) attacks, compromising the security of users relying on lxml_html_clean in default configuration for sanitizing untrusted HTML content. Users employing the HTML cleaner in a security-sensitive context should upgrade to lxml 0.4.0, which addresses this issue. As a temporary mitigation, users can configure lxml_html_clean with the following settings to prevent the exploitation of this vulnerability. Via `remove_tags`, one may specify tags to remove - their content is moved to their parents' tags. Via `kill_tags`, one may specify tags to be removed completely. Via `allow_tags`, one may restrict the set of permissible tags, excluding context-switching tags like `<svg>`, `<math>` and `<noscript>`.	2024-11-19	6.1	CVE-2024-52595
google -- android	In SMF_ParseMetaEvent of eas_smf.c, there is a possible integer overflow. This could lead to remote denial of service due to resource exhaustion with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-19	6.5	CVE-2018-9348
google -- android	In parse of M3UParser.cpp there is a possible resource exhaustion due to improper input validation. This could lead to denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-19	6.5	CVE-2018-9440
google -- android	In the Mediatek Preloader, there are out of bounds reads and writes due to an exposed interface that allows arbitrary peripheral memory mapping with insufficient blacklisting/whitelisting. This could lead to local elevation of privilege, given physical access to the device with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-19	6.4	CVE-2018-9371
google -- android	In ResStringPool::setTo of ResourceTypes.cpp, it's possible for an attacker to control the value of mStringPoolSize to be out of bounds, causing information disclosure.	2024-11-19	5.5	CVE-2018-9340
google -- android	In BnAudioPolicyService::onTransact of AudioPolicyService.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	5.5	CVE-2018-9345
google -- android	In BnAudioPolicyService::onTransact of AudioPolicyService.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	5.5	CVE-2018-9346
google -- android	In analyzeAxes of FontUtils.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	5.5	CVE-2018-9410
google -- android	In removeUnsynchronization of ID3.cpp there is a possible resource exhaustion due to improper input validation. This could lead to denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-11-19	5.5	CVE-2018-9412
google -- android	In BnCameraService::onTransact of CameraService.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-19	5.5	CVE-2018-9420
google -- android	In writeInplace of Parcel.cpp, there is a possible information leak across processes, using Binder, due to uninitialized data. This could lead to local information	2024-11-19	5.5	CVE-2018-9421

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.			
hyscaler -- wp_roles_at_registration	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NetTantra WP Roles at Registration allows Stored XSS.This issue affects WP Roles at Registration: from n/a through 0.23.	2024-11-19	4.8	CVE-2023-27609
idccms -- idccms	A vulnerability was found in idcCMS 1.60. It has been classified as problematic. This affects the function GetCityOptionJs of the file /inc/classProvCity.php. The manipulation of the argument idName 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.	2024-11-21	6.1	CVE-2024-11587
inspireui -- mstore_api	The MStore API - Create Native Android & iOS Apps On The Cloud plugin for WordPress is vulnerable to SQL Injection via the 'status_type' parameter in all versions up to, and including, 4.15.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-11-20	6.5	CVE-2024-11179
lightspeedwp -- lsx_tour_operator	The LSX Tour Operator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.4.9 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.	2024-11-21	5.4	CVE-2024-9851
linear -- linear	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Linear Oy Linear linear allows DOM-Based XSS.This issue affects Linear: from n/a through 2.7.11.	2024-11-18	5.4	CVE-2024-52426
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ocfs2: remove entry once instead of null-ptr-dereference in ocfs2_xa_remove() Syzkaller is able to provoke null-ptr-dereference in ocfs2_xa_remove(): [57.319872] (a.out,1161,7):ocfs2_xa_remove:2028 ERROR: status = -12 [57.320420] (a.out,1161,7):ocfs2_xa_cleanup_value_truncate:1999 ERROR: Partial truncate while removing xattr overlay.upper. Leaking 1 clusters and removing the entry [57.321727] BUG: kernel NULL pointer dereference, address: 0000000000000004 [...] [57.325727] RIP: 0010:ocfs2_xa_block_wipe_namevalue+0x2a/0xc0 [...] [57.331328] Call Trace: [57.331477] <TASK> [...] [57.333511] ? do_user_addr_fault+0x3e5/0x740 [57.333778] ? exc_page_fault+0x70/0x170 [57.334016] ? asm_exc_page_fault+0x2b/0x30 [57.334263] ? __pfx_ocfs2_xa_block_wipe_namevalue+0x10/0x10 [57.334596] ? ocfs2_xa_block_wipe_namevalue+0x2a/0xc0 [57.334913] ocfs2_xa_remove_entry+0x23/0xc0 [57.335164] ocfs2_xa_set+0x704/0xcf0 [57.335381] ? _raw_spin_unlock+0x1a/0x40 [57.335620] ? ocfs2_inode_cache_unlock+0x16/0x20 [57.335915] ? trace_preempt_on+0x1e/0x70 [57.336153] ? start_this_handle+0x16c/0x500 [57.336410] ? preempt_count_sub+0x50/0x80 [57.336656] ? _raw_read_unlock+0x20/0x40 [57.336906] ? start_this_handle+0x16c/0x500 [57.337162] ocfs2_xattr_block_set+0xa6/0x1e0 [57.337424] __ocfs2_xattr_set_handle+0x1fd/0x5d0 [57.337706] ? ocfs2_start_trans+0x13d/0x290 [57.337971] ocfs2_xattr_set+0xb13/0xfb0 [57.338207] ? dput+0x46/0x1c0 [57.338393] ocfs2_xattr_trusted_set+0x28/0x30 [57.338665] ? ocfs2_xattr_trusted_set+0x28/0x30 [57.338948] __vfs_removexattr+0x92/0xc0 [57.339182] __vfs_removexattr_locked+0xd5/0x190 [57.339456] ? preempt_count_sub+0x50/0x80 [57.339705] vfs_removexattr+0x5f/0x100 [...] Reproducer uses faultinject facility to fail ocfs2_xa_remove() -> ocfs2_xa_value_truncate() with -ENOMEM. In this case the comment mentions	2024-11-19	5.5	CVE-2024-50265

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	that we can return 0 if ocfs2_xa_cleanup_value_truncate() is going to wipe the entry anyway. But the following 'rc' check is wrong and execution flow do 'ocfs2_xa_remove_entry(loc);' twice: * 1st: in ocfs2_xa_cleanup_value_truncate(); * 2nd: returning back to ocfs2_xa_remove() instead of going to 'out'. Fix this by skipping the 2nd removal of the same entry and making syzkaller repro happy.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: clk: qcom: videocc-sm8350: use HW_CTRL_TRIGGER for vcodec GDSCs A recent change in the venus driver results in a stuck clock on the Lenovo ThinkPad X13s, for example, when streaming video in firefox: video_cc_mvs0_clk status stuck at 'off' WARNING: CPU: 6 PID: 2885 at drivers/clk/qcom/clk-branch.c:87 clk_branch_wait+0x144/0x15c ... Call trace: clk_branch_wait+0x144/0x15c clk_branch2_enable+0x30/0x40 clk_core_enable+0xd8/0x29c clk_enable+0x2c/0x4c vcodec_clks_enable.isra.0+0x94/0xd8 [venus_core] coreid_power_v4+0x464/0x628 [venus_core] vdec_start_streaming+0xc4/0x510 [venus_dec] vb2_start_streaming+0x6c/0x180 [videobuf2_common] vb2_core_streamon+0x120/0x1dc [videobuf2_common] vb2_streamon+0x1c/0x6c [videobuf2_v4l2] v4l2_m2m_ioctl_streamon+0x30/0x80 [v4l2_mem2mem] v4l_streamon+0x24/0x30 [videodev] using the out-of-tree sm8350/sc8280xp venus support. [1] Update also the sm8350/sc8280xp GDSC definitions so that the hw control mode can be changed at runtime as the venus driver now requires.	2024-11-19	5.5	CVE-2024-50266
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: KEYS: trusted: dcp: fix NULL dereference in AEAD crypto operation When sealing or unsealing a key blob we currently do not wait for the AEAD cipher operation to finish and simply return after submitting the request. If there is some load on the system we can exit before the cipher operation is done and the buffer we read from/write to is already removed from the stack. This will e.g. result in NULL pointer dereference errors in the DCP driver during blob creation. Fix this by waiting for the AEAD cipher operation to finish before resuming the seal and unseal calls.	2024-11-19	5.5	CVE-2024-50281
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: media: v4l2-tpg: prevent the risk of a division by zero As reported by Coverity, the logic at tpg_precalculate_line() blindly rescales the buffer even when scaled_witdh is equal to zero. If this ever happens, this will cause a division by zero. Instead, add a WARN_ON_ONCE() to trigger such cases and return without doing any precalculation.	2024-11-19	5.5	CVE-2024-50287
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: sctp: properly validate chunk size in sctp_sf_ootb() A size validation fix similar to that in Commit 50619dbf8db7 ("sctp: add size validation when walking chunks") is also required in sctp_sf_ootb() to address a crash reported by syzbot: BUG: KMSAN: uninit-value in sctp_sf_ootb+0x7f5/0xce0 net/sctp/sm_statefuns.c:3712 sctp_sf_ootb+0x7f5/0xce0 net/sctp/sm_statefuns.c:3712 sctp_do_sm+0x181/0x93d0 net/sctp/sm_sideeffect.c:1166 sctp_endpoint_bh_rcv+0xc38/0xf90 net/sctp/endpointola.c:407 sctp_inq_push+0x2ef/0x380 net/sctp/inqueue.c:88 sctp_rcv+0x3831/0x3b20 net/sctp/input.c:243 sctp4_rcv+0x42/0x50 net/sctp/protocol.c:1159 ip_protocol_deliver_rcu+0xb51/0x13d0 net/ipv4/ip_input.c:205 ip_local_deliver_finish+0x336/0x500 net/ipv4/ip_input.c:233	2024-11-19	5.5	CVE-2024-50299
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: regulator: rtq2208: Fix uninitialized use of regulator_config Fix rtq2208 driver uninitialized use to cause kernel error.	2024-11-19	5.5	CVE-2024-50300
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: mctp i2c: handle NULL header address daddr can be NULL if there is no neighbour table entry present, in that case the tx packet should be dropped. saddr will usually be set by MCTP core, but check for NULL in case a packet is transmitted by a different protocol.	2024-11-19	5.5	CVE-2024-53043

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: slub/kunit: fix a WARNING due to unwrapped __kmalloc_cache_noprof 'modprobe slub_kunit' will have a warning as shown below. The root cause is that __kmalloc_cache_noprof was directly used, which resulted in no alloc_tag being allocated. This caused current->alloc_tag to be null, leading to a warning in alloc_tag_add_check. Let's add an alloc_hook layer to __kmalloc_cache_noprof specifically within lib/slub_kunit.c, which is the only user of this internal slub function outside kmalloc implementation itself. [58162.947016] WARNING: CPU: 2 PID: 6210 at ./include/linux/alloc_tag.h:125 alloc_tagging_slab_alloc_hook+0x268/0x27c [58162.957721] Call trace: [58162.957919] alloc_tagging_slab_alloc_hook+0x268/0x27c [58162.958286] __kmalloc_cache_noprof+0x14c/0x344 [58162.958615] test_kmalloc_redzone_access+0x50/0x10c [slub_kunit] [58162.959045] kunit_try_run_case+0x74/0x184 [kunit] [58162.959401] kunit_generic_run_threadfn_adapter+0x2c/0x4c [kunit] [58162.959841] kthread+0x10c/0x118 [58162.960093] ret_from_fork+0x10/0x20 [58162.960363] ---[end trace 0000000000000000]---	2024-11-19	5.5	CVE-2024-53049
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/i915/hdcp: Add encoder check in hdcp2_get_capability Add encoder check in intel_hdcp2_get_capability to avoid null pointer error.	2024-11-19	5.5	CVE-2024-53050
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/i915/hdcp: Add encoder check in intel_hdcp_get_capability Sometimes during hotplug scenario or suspend/resume scenario encoder is not always initialized when intel_hdcp_get_capability add a check to avoid kernel null pointer dereference.	2024-11-19	5.5	CVE-2024-53051
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Fix another deadlock during RTC update If ufshcd_rtc_work calls ufshcd_rpm_put_sync() and the pm's usage_count is 0, we will enter the runtime suspend callback. However, the runtime suspend callback will wait to flush ufshcd_rtc_work, causing a deadlock. Replace ufshcd_rpm_put_sync() with ufshcd_rpm_put() to avoid the deadlock.	2024-11-19	5.5	CVE-2024-53053
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: cgroup/bpf: use a dedicated workqueue for cgroup bpf destruction A hung_task problem shown below was found: INFO: task kworker/0:0:8 blocked for more than 327 seconds. "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. Workqueue: events cgroup_bpf_release Call Trace: <TASK> __schedule+0x5a2/0x2050 ? find_held_lock+0x33/0x100 ? wq_worker_sleeping+0x9e/0xe0 schedule+0x9f/0x180 schedule_preempt_disabled+0x25/0x50 __mutex_lock+0x512/0x740 ? cgroup_bpf_release+0x1e/0x4d0 ? cgroup_bpf_release+0xcf/0x4d0 ? process_scheduled_works+0x161/0x8a0 ? cgroup_bpf_release+0x1e/0x4d0 ? mutex_lock_nested+0x2b/0x40 ? __pfx_delay_tsc+0x10/0x10 mutex_lock_nested+0x2b/0x40 cgroup_bpf_release+0xcf/0x4d0 ? process_scheduled_works+0x161/0x8a0 ? trace_event_raw_event_workqueue_execute_start+0x64/0xd0 ? process_scheduled_works+0x161/0x8a0 process_scheduled_works+0x23a/0x8a0 worker_thread+0x231/0x5b0 ? __pfx_worker_thread+0x10/0x10 kthread+0x14d/0x1c0 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x59/0x70 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1b/0x30 </TASK> This issue can be reproduced by the following pressuse test: 1. A large number of cpuset cgroups are deleted. 2. Set cpu on and off repeatly. 3. Set watchdog_thresh repeatly. The scripts can be obtained at LINK mentioned above the signature. The reason for this issue is cgroup_mutex and cpu_hotplug_lock are acquired in different tasks, which may lead to deadlock. It can lead to a deadlock through the following steps: 1. A large number of cpusets are deleted asynchronously, which puts a large number of cgroup_bpf_release works into system_wq. The max_active of system_wq is WQ_DFL_ACTIVE(256). Consequently, all active works are cgroup_bpf_release	2024-11-19	5.5	CVE-2024-53054

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	works, and many cgroup_bpf_release works will be put into inactive queue. As illustrated in the diagram, there are 256 (in the acvtive queue) + n (in the inactive queue) works. 2. Setting watchdog_thresh will hold cpu_hotplug_lock.read and put smp_call_on_cpu work into system_wq. However step 1 has already filled system_wq, 'sscs.work' is put into inactive queue. 'sscs.work' has to wait until the works that were put into the inacvtive queue earlier have executed (n cgroup_bpf_release), so it will be blocked for a while. 3. Cpu offline requires cpu_hotplug_lock.write, which is blocked by step 2. 4. Cpusets that were deleted at step 1 put cgroup_release works into cgroup_destroy_wq. They are competing to get cgroup_mutex all the time. When cgroup_metux is acqured by work at css_killed_work_fn, it will call cpuset_css_offline, which needs to acqure cpu_hotplug_lock.read. However, cpuset_css_offline will be blocked for step 3. 5. At this moment, there are 256 works in active queue that are cgroup_bpf_release, they are attempting to acquire cgroup_mutex, and as a result, all of them are blocked. Consequently, sscs.work can not be executed. Ultimately, this situation leads to four processes being blocked, forming a deadlock. system_wq(step1) WatchDog(step2) cpu offline(step3) cgroup_destroy_wq(step4) ... 2000+ cgroups deleted asyn 256 actives + n inactives __lockup_detector_reconfigure P(cpu_hotplug_lock.read) put sscs.work into system_wq 256 + n + 1(sscs.work) sscs.work wait to be executed warting sscs.work finish percpu_down_write P(cpu_hotplug_lock.write) ...blocking... css_killed_work_fn P(cgroup_mutex) cpuset_css_offline P(cpu_hotplug_lock.read) ...blocking... 256 cgroup_bpf_release mutex_lock(&cgroup_mutex); ..blocking... To fix the problem, place cgroup_bpf_release works on a dedicated workqueue which can break the loop and solve the problem. System wqs are for misc things which shouldn't create a large number of concurrent work items. If something is going to generate > ---truncated---			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: fix 6 GHz scan construction If more than 255 colocated APs exist for the set of all APs found during 2.4/5 GHz scanning, then the 6 GHz scan construction will loop forever since the loop variable has type u8, which can never reach the number found when that's bigger than 255, and is stored in a u32 variable. Also move it into the loops to have a smaller scope. Using a u32 there is fine, we limit the number of APs in the scan list and each has a limit on the number of RNR entries due to the frame size. With a limit of 1000 scan results, a frame size upper bound of 4096 (really it's more like ~2300) and a TBTT entry size of at least 11, we get an upper bound for the number of ~372k, well in the bounds of a u32.	2024-11-19	5.5	CVE-2024-53055
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: Fix potential NULL dereference in mtk_crtc_destroy() In mtk_crtc_create(), if the call to mbox_request_channel() fails then we set the "mtk_crtc->cmdq_client.chan" pointer to NULL. In that situation, we do not call cmdq_pkt_create(). During the cleanup, we need to check if the "mtk_crtc->cmdq_client.chan" is NULL first before calling cmdq_pkt_destroy(). Calling cmdq_pkt_destroy() is unnecessary if we didn't call cmdq_pkt_create() and it will result in a NULL pointer dereference.	2024-11-19	5.5	CVE-2024-53056
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: TSO: Fix unbalanced DMA map/unmap for non-paged SKB data In case the non-paged data of a SKB carries protocol header and protocol payload to be transmitted on a certain platform that the DMA AXI address width is configured to 40-bit/48-bit, or the size of the non-paged data is bigger than TSO_MAX_BUFF_SIZE on a certain platform that the DMA AXI address width is configured to 32-bit, then this SKB requires at least two DMA transmit descriptors to serve it. For example, three descriptors are allocated to split one DMA buffer mapped from one piece of non-paged data: dma_desc[N + 0], dma_desc[N + 1], dma_desc[N + 2]. Then three elements of tx_q->tx_skbuff_dma[] will be allocated to hold extra information to be reused in stmmac_tx_clean(): tx_q->tx_skbuff_dma[N + 0], tx_q->tx_skbuff_dma[N + 1], tx_q->tx_skbuff_dma[N + 2].	2024-11-19	5.5	CVE-2024-53058

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Now we focus on tx_q->tx_skbuff_dma[entry].buf, which is the DMA buffer address returned by DMA mapping call. stmmac_tx_clean() will try to unmap the DMA buffer _ONLY_IF_ tx_q->tx_skbuff_dma[entry].buf is a valid buffer address. The expected behavior that saves DMA buffer address of this non-paged data to tx_q->tx_skbuff_dma[entry].buf is: tx_q->tx_skbuff_dma[N + 0].buf = NULL; tx_q->tx_skbuff_dma[N + 1].buf = NULL; tx_q->tx_skbuff_dma[N + 2].buf = dma_map_single(); Unfortunately, the current code misbehaves like this: tx_q->tx_skbuff_dma[N + 0].buf = dma_map_single(); tx_q->tx_skbuff_dma[N + 1].buf = NULL; tx_q->tx_skbuff_dma[N + 2].buf = NULL; On the stmmac_tx_clean() side, when dma_desc[N + 0] is closed by the DMA engine, tx_q->tx_skbuff_dma[N + 0].buf is a valid buffer address obviously, then the DMA buffer will be unmapped immediately. There may be a rare case that the DMA engine does not finish the pending dma_desc[N + 1], dma_desc[N + 2] yet. Now things will go horribly wrong, DMA is going to access a unmapped/unreferenced memory region, corrupted data will be transmited or iommu fault will be triggered :(In contrast, the for-loop that maps SKB fragments behaves perfectly as expected, and that is how the driver should do for both non-paged data and paged frags actually. This patch corrects DMA map/unmap sequences by fixing the array index for tx_q->tx_skbuff_dma[entry].buf when assigning DMA buffer address. Tested and verified on DWXGMAC CORE 3.20a			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: media: dvbdev: prevent the risk of out of memory access The dvbdev contains a static variable used to store dvb minors. The behavior of it depends if CONFIG_DVB_DYNAMIC_MINORS is set or not. When not set, dvb_register_device() won't check for boundaries, as it will rely that a previous call to dvb_register_adapter() would already be enforcing it. On a similar way, dvb_device_open() uses the assumption that the register functions already did the needed checks. This can be fragile if some device ends using different calls. This also generate warnings on static check analysers like Coverity. So, add explicit guards to prevent potential risk of OOM issues.	2024-11-19	5.5	CVE-2024-53063
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: idpf: fix idpf_vc_core_init error path In an event where the platform running the device control plane is rebooted, reset is detected on the driver. It releases all the resources and waits for the reset to complete. Once the reset is done, it tries to build the resources back. At this time if the device control plane is not yet started, then the driver timeouts on the virtchnl message and retries to establish the mailbox again. In the retry flow, mailbox is deinitialized but the mailbox workqueue is still alive and polling for the mailbox message. This results in accessing the released control queue leading to null-ptr-deref. Fix it by unrolling the work queue cancellation and mailbox deinitialization in the reverse order which they got initialized.	2024-11-19	5.5	CVE-2024-53064
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: mm/slab: fix warning caused by duplicate kmem_cache creation in kmem_buckets_create Commit b035f5a6d852 ("mm: slab: reduce the kmalloc() minimum alignment if DMA bouncing possible") reduced ARCH_KMALLOC_MINALIGN to 8 on arm64. However, with KASAN_HW_TAGS enabled, arch_slab_minalign() becomes 16. This causes kmalloc_caches[*][8] to be aliased to kmalloc_caches[*][16], resulting in kmem_buckets_create() attempting to create a kmem_cache for size 16 twice. This duplication triggers warnings on boot: [2.325108] ------------[cut here]------------ [2.325135] kmem_cache of name 'memdup_user-16' already exists [2.325783] WARNING: CPU: 0 PID: 1 at mm/slab_common.c:107 __kmem_cache_create_args+0xb8/0x3b0 [2.327957] Modules linked in: [2.328550] CPU: 0 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.12.0-rc5mm-unstable-arm64+ #12 [2.328683] Hardware name: QEMU QEMU Virtual Machine, BIOS 2024.02-2 03/11/2024 [2.328790] pstate: 61000009 (nZCv daif -PAN -UAO -TCO +DIT -SSBS BTYPE=--) [2.328911] pc : __kmem_cache_create_args+0xb8/0x3b0 [2.328930] lr :	2024-11-19	5.5	CVE-2024-53065

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	__kmem_cache_create_args+0xb8/0x3b0 [2.328942] sp : ffff800083d6fc50 [2.328961] x29: ffff800083d6fc50 x28: f2ff0000c1674410 x27: ffff8000820b0598 [2.329061] x26: 000000007fffffff x25: 0000000000000010 x24: 0000000000002000 [2.329101] x23: ffff800083d6fce8 x22: ffff8000832222e8 x21: ffff800083222388 [2.329118] x20: f2ff0000c1674410 x19: f5ff0000c16364c0 x18: ffff800083d80030 [2.329135] x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 [2.329152] x14: 0000000000000000 x13: 0a73747369786520 x12: 79646165726c6120 [2.329169] x11: 656820747563205b x10: 2d2d2d2d2d2d2d2d x9 : 0000000000000000 [2.329194] x8 : 0000000000000000 x7 : 0000000000000000 x6 : 0000000000000000 [2.329210] x5 : 0000000000000000 x4 : 0000000000000000 x3 : 0000000000000000 [2.329226] x2 : 0000000000000000 x1 : 0000000000000000 x0 : 0000000000000000 [2.329291] Call trace: [2.329407] __kmem_cache_create_args+0xb8/0x3b0 [2.329499] kmem_buckets_create+0xfc/0x320 [2.329526] init_user_buckets+0x34/0x78 [2.329540] do_one_initcall+0x64/0x3c8 [2.329550] kernel_init_freeable+0x26c/0x578 [2.329562] kernel_init+0x3c/0x258 [2.329574] ret_from_fork+0x10/0x20 [2.329698] ---[end trace 0000000000000000]--- [2.403704] ------------[cut here]------------ [2.404716] kmem_cache of name 'msg_msg-16' already exists [2.404801] WARNING: CPU: 2 PID: 1 at mm/slab_common.c:107 __kmem_cache_create_args+0xb8/0x3b0 [2.404842] Modules linked in: [2.404971] CPU: 2 UID: 0 PID: 1 Comm: swapper/0 Tainted: G W 6.12.0-rc5mm-unstable-arm64+ #12 [2.405026] Tainted: [W]=WARN [2.405043] Hardware name: QEMU QEMU Virtual Machine, BIOS 2024.02-2 03/11/2024 [2.405057] pstate: 60400009 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [2.405079] pc : __kmem_cache_create_args+0xb8/0x3b0 [2.405100] lr : __kmem_cache_create_args+0xb8/0x3b0 [2.405111] sp : ffff800083d6fc50 [2.405115] x29: ffff800083d6fc50 x28: fbff0000c1674410 x27: ffff8000820b0598 [2.405135] x26: 000000000000ffd0 x25: 0000000000000010 x24: 0000000000006000 [2.405153] x23: ffff800083d6fce8 x22: ffff8000832222e8 x21: ffff800083222388 [2.405169] x20: fbff0000c1674410 x19: fdff0000c163d6c0 x18: ffff800083d80030 [2.405185] x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 [2.405201] x14: 0000000000000000 x13: 0a73747369786520 x12: 79646165726c6120 [2.405217] x11: 656820747563205b x10: 2d2d2d2d2d2d2d2d x9 : 0000000000000000 [2.405233] x8 : 0000000000000000 x7 : 0000000000000000 x6 : 0000000000000000 [2.405248] x5 : 0000000000000000 x4 : 0000000000000000 x3 : 0000000000000000 [2.405271] x2 : 0000000000000000 x1 : 0000000000000000 x0 : 0000000000000000 [2.405287] Call trace: [2 ---truncated---				
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: nfs: Fix KMSAN warning in decode_getfattr_attrs() Fix the following KMSAN warning: CPU: 1 UID: 0 PID: 7651 Comm: cp Tainted: G B Tainted: [B]=BAD_PAGE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009) ===== ===== BUG: KMSAN: uninit-value in decode_getfattr_attrs+0x2d6d/0x2f90 decode_getfattr_attrs+0x2d6d/0x2f90 decode_getfattr_generic+0x806/0xb00 nfs4_xdr_dec_getattr+0x1de/0x240 rpcauth_unwrap_resp_decode+0xab/0x100 rpcauth_unwrap_resp+0x95/0xc0 call_decode+0x4ff/0xb50 __rpc_execute+0x57b/0x19d0 rpc_execute+0x368/0x5e0 rpc_run_task+0xcfe/0xee0 nfs4_proc_getattr+0x5b5/0x990 __nfs_revalidate_inode+0x477/0xd00 nfs_access_get_cached+0x1021/0x1cc0 nfs_do_access+0x9f/0xae0 nfs_permission+0x1e4/0x8c0 inode_permission+0x356/0x6c0 link_path_walk+0x958/0x1330 path_lookupat+0xce/0x6b0 filename_lookup+0x23e/0x770 vfs_statx+0xe7/0x970 vfs_fstatat+0x1f2/0x2c0 __se_sys_newfstatat+0x67/0x880 __x64_sys_newfstatat+0xbd/0x120 x64_sys_call+0x1826/0x3cf0 do_syscall_64+0xd0/0x1b0 entry_SYSCALL_64_after_hwframe+0x77/0x7f The KMSAN warning is triggered in decode_getfattr_attrs(), when calling	2024-11-19	5.5	CVE-2024-53066

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	decode_attr_mdsthreshold(). It appears that fattr->mdsthreshold is not initialized. Fix the issue by initializing fattr->mdsthreshold to NULL in nfs_fattr_init().			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Start the RTC update work later The RTC update work involves runtime resuming the UFS controller. Hence, only start the RTC update work after runtime power management in the UFS driver has been fully initialized. This patch fixes the following kernel crash: Internal error: Oops: 0000000096000006 [#1] PREEMPT SMP Workqueue: events ufshcd_rtc_work Call trace: _raw_spin_lock_irqsave+0x34/0x8c (P) pm_runtime_get_if_active+0x24/0x9c (L) pm_runtime_get_if_active+0x24/0x9c ufshcd_rtc_work+0x138/0x1b4 process_one_work+0x148/0x288 worker_thread+0x2cc/0x3d4 kthread+0x110/0x114 ret_from_fork+0x10/0x20	2024-11-19	5.5	CVE-2024-53067
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: firmware: qcom: scm: fix a NULL-pointer dereference Some SCM calls can be invoked with __scm being NULL (the driver may not have been and will not be probed as there's no SCM entry in device-tree). Make sure we don't dereference a NULL pointer.	2024-11-19	5.5	CVE-2024-53069
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: fix fault at system suspend if device was already runtime suspended If the device was already runtime suspended then during system suspend we cannot access the device registers else it will crash. Also we cannot access any registers after dwc3_core_exit() on some platforms so move the dwc3_enable_susphy() call to the top.	2024-11-19	5.5	CVE-2024-53070
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: platform/x86/amd/pmc: Detect when STB is not available Loading the amd_pmc module as: amd_pmc enable_stb=1 ...can result in the following messages in the kernel ring buffer: amd_pmc AMDI0009:00: SMU cmd failed. err: 0xff ioremap on RAM at 0x0000000000000000 - 0x000000000fffffff WARNING: CPU: 10 PID: 2151 at arch/x86/mm/ioremap.c:217 __ioremap_caller+0x2cd/0x340 Further debugging reveals that this occurs when the requests for S2D_PHYS_ADDR_LOW and S2D_PHYS_ADDR_HIGH return a value of 0, indicating that the STB is inaccessible. To prevent the ioremap warning and provide clarity to the user, handle the invalid address and display an error message.	2024-11-19	5.5	CVE-2024-53072
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: NFSD: Never decrement pending_async_copies on error The error flow in nfsd4_copy() calls cleanup_async_copy(), which already decrements nn->pending_async_copies.	2024-11-19	5.5	CVE-2024-53073
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: don't leak a link on AP removal Release the link mapping resource in AP removal. This impacted devices that do not support the MLD API (9260 and down). On those devices, we couldn't start the AP again after the AP has been already started and stopped.	2024-11-19	5.5	CVE-2024-53074
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: riscv: Prevent a bad reference count on CPU nodes When populating cache leaves we previously fetched the CPU device node at the very beginning. But when ACPI is enabled we go through a specific branch which returns early and does not call 'of_node_put' for the node that was acquired. Since we are not using a CPU device node for the ACPI code anyways, we can simply move the initialization of it just passed the ACPI block, and we are guaranteed to have an 'of_node_put' call for the acquired node. This prevents a bad reference count of the CPU device node. Moreover, the previous function did not check for errors when acquiring the device node, so a return -ENOENT has been added for that case.	2024-11-19	5.5	CVE-2024-53075
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: iio: gts-helper: Fix memory leaks for the error path of iio_gts_build_avail_scale_table() If per_time_scales[i] or per_time_gains[i] kcalloc fails in the for loop of	2024-11-19	5.5	CVE-2024-53076

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	iio_gts_build_avail_scale_table(), the err_free_out will fail to call kfree() each time when i is reduced to 0, so all the per_time_scales[0] and per_time_gains[0] will not be freed, which will cause memory leaks. Fix it by checking if i >= 0.			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: rpcrdma: Always release the rpcrdma_device's xa_array Dai pointed out that the xa_init_flags() in rpcrdma_add_one() needs to have a matching xa_destroy() in rpcrdma_remove_one() to release underlying memory that the xarray might have accrued during operation.	2024-11-19	5.5	CVE-2024-53077
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/tegra: Fix NULL vs IS_ERR() check in probe() The iommu_paging_domain_alloc() function doesn't return NULL pointers, it returns error pointers. Update the check to match.	2024-11-19	5.5	CVE-2024-53078
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: i40e: fix race condition by adding filter's intermediate sync state Fix a race condition in the i40e driver that leads to MAC/VLAN filters becoming corrupted and leaking. Address the issue that occurs under heavy load when multiple threads are concurrently modifying MAC/VLAN filters by setting mac and port VLAN. 1. Thread T0 allocates a filter in i40e_add_filter() within i40e_ndo_set_vf_port_vlan(). 2. Thread T1 concurrently frees the filter in __i40e_del_filter() within i40e_ndo_set_vf_mac(). 3. Subsequently, i40e_service_task() calls i40e_sync_vsi_filters(), which refers to the already freed filter memory, causing corruption. Reproduction steps: 1. Spawn multiple VFs. 2. Apply a concurrent heavy load by running parallel operations to change MAC addresses on the VFs and change port VLANs on the host. 3. Observe errors in dmesg: "Error I40E_AQ_RC_ENOSPC adding RX filters on VF XX, please set promiscuous on manually for VF XX". Exact code for stable reproduction Intel can't open-source now. The fix involves implementing a new intermediate filter state, I40E_FILTER_NEW_SYNC, for the time when a filter is on a tmp_add_list. These filters cannot be deleted from the hash list directly but must be removed using the full process.	2024-11-19	4.7	CVE-2024-53088
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: io_uring/rw: fix missing NOWAIT check for O_DIRECT start write When io_uring starts a write, it'll call kiocb_start_write() to bump the super block rwsem, preventing any freezes from happening while that write is in-flight. The freeze side will grab that rwsem for writing, excluding any new writers from happening and waiting for existing writes to finish. But io_uring unconditionally uses kiocb_start_write(), which will block if someone is currently attempting to freeze the mount point. This causes a deadlock where freeze is waiting for previous writes to complete, but the previous writes cannot complete, as the task that is supposed to complete them is blocked waiting on starting a new write. This results in the following stuck trace showing that dependency with the write blocked starting a new write: task:fio state:D stack:0 pid:886 tgid:886 ppid:876 Call trace: __switch_to+0x1d8/0x348 __schedule+0x8e8/0x2248 schedule+0x110/0x3f0 percpu_rwsem_wait+0x1e8/0x3f8 __percpu_down_read+0xe8/0x500 io_write+0xbb8/0xff8 io_issue_sqe+0x10c/0x1020 io_submit_sqes+0x614/0x2110 __arm64_sys_io_uring_enter+0x524/0x1038 invoke_syscall+0x74/0x268 el0_svc_common.constprop.0+0x160/0x238 do_el0_svc+0x44/0x60 el0_svc+0x44/0xb0 el0t_64_sync_handler+0x118/0x128 el0t_64_sync+0x168/0x170 INFO: task fsfreeze:7364 blocked for more than 15 seconds. Not tainted 6.12.0-rc5-00063-g76aaf945701c #7963 with the attempting freezer stuck trying to grab the rwsem: task:fsfreeze state:D stack:0 pid:7364 tgid:7364 ppid:995 Call trace: __switch_to+0x1d8/0x348 __schedule+0x8e8/0x2248 schedule+0x110/0x3f0 percpu_down_write+0x2b0/0x680 freeze_super+0x248/0x8a8 do_vfs_ioctl+0x149c/0x1b18 __arm64_sys_ioctl+0xd0/0x1a0 invoke_syscall+0x74/0x268 el0_svc_common.constprop.0+0x160/0x238 do_el0_svc+0x44/0x60 el0_svc+0x44/0xb0 el0t_64_sync_handler+0x118/0x128 el0t_64_sync+0x168/0x170 Fix this by having the io_uring side honor	2024-11-19	4.4	CVE-2024-53052

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	IOCB_NOWAIT, and only attempt a blocking grab of the super block rwsem if it isn't set. For normal issue where IOCB_NOWAIT would always be set, this returns -EAGAIN which will have io_uring core issue a blocking attempt of the write. That will in turn also get completions run, ensuring forward progress. Since freezing requires CAP_SYS_ADMIN in the first place, this isn't something that can be triggered by a regular user.			
maheshwaghmare -- copy_anything_to_clipboard	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Clipboard Team Copy Anything to Clipboard allows Stored XSS.This issue affects Copy Anything to Clipboard: from n/a through 4.0.3.	2024-11-18	5.4	CVE-2024-52419
moodle -- moodle	A vulnerability was found in Moodle. It is possible for users with the "send message" capability to view other users' names that they may not otherwise have access to via an error message in Messaging. Note: The name returned follows the full name format configured on the site.	2024-11-18	4.3	CVE-2024-48896
moodle -- moodle	A vulnerability was found in Moodle. Additional checks are required to ensure users can only edit or delete RSS feeds that they have permission to modify.	2024-11-18	4.3	CVE-2024-48897
moodle -- moodle	A vulnerability was found in Moodle. Users with access to delete audiences from reports could delete audiences from other reports that they do not have permission to delete from.	2024-11-18	4.3	CVE-2024-48898
moodle -- moodle	A vulnerability was found in Moodle. Additional checks are required to ensure users can only access the schedule of a report if they have permission to edit that report.	2024-11-18	4.3	CVE-2024-48901
motopress -- getwid	The Getwid - Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `template-post-custom-field` block in all versions up to, and including, 2.0.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-20	5.4	CVE-2024-10872
n/a -- n/a	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in django CMS Association django CMS Attributes Fields allows Stored XSS.This issue affects django CMS Attributes Fields: before 4.0.	2024-11-20	6.9	CVE-2024-11406
n/a -- n/a	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to read arbitrary files on the underlying filesystem of an affected system. This vulnerability is due to insufficient access control for sensitive information that is written to an affected system. An attacker could exploit this vulnerability by accessing sensitive information that they are not authorized to access on an affected system. A successful exploit could allow the attacker to gain access to devices and other network management systems that they should not have access to.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-18	6.5	CVE-2021-1232
n/a -- n/a	Multiple vulnerabilities in the Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) implementations for Cisco IP Phone Series 68xx/78xx/88xx could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP phone. These vulnerabilities are due to missing checks when the IP phone processes a Cisco Discovery Protocol or LLDP packet. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol or LLDP packet to the targeted IP phone. A successful exploit could allow the attacker to execute code on the affected IP phone or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition.Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the	2024-11-18	6.5	CVE-2021-1379

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	affected device (Layer 2 adjacent).Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.			
n/a -- n/a	The ProfileGrid - User Profiles, Groups and Communities plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the pm_remove_file_attachment() function in all versions up to, and including, 5.9.3.6. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary user meta which can do things like deny an administrator's access to their site. .	2024-11-20	6.5	CVE-2024-10900
n/a -- n/a	A low privileged remote attacker can overwrite an arbitrary file on the filesystem whichÂ may lead to an arbitrary file read with root privileges.	2024-11-18	6.5	CVE-2024-41972
n/a -- n/a	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.	2024-11-21	6.5	CVE-2024-45663
n/a -- n/a	The Twitter Follow Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'username' parameter in all versions up to, and including, 0.2 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.	2024-11-23	6.4	CVE-2024-10116
n/a -- n/a	The Premium Packages - Sell Digital Products Securely plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpdmpp_pay_link shortcode in all versions up to, and including, 5.9.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-21	6.4	CVE-2024-10164
n/a -- n/a	The WPBakery Visual Composer WHMCS Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's void_wbwhmcse_laouts_search shortcode in all versions up to, and including, 1.0.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-21	6.4	CVE-2024-10172
n/a -- n/a	The Beds24 Online Booking plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's beds24-link shortcode in all versions up to, and including, 2.0.26 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-21	6.4	CVE-2024-10177
n/a -- n/a	The MP3 Audio Player - Music Player, Podcast Player & Radio by Sonaar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's sonaar_audioplayer shortcode in all versions up to, and including, 5.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-19	6.4	CVE-2024-10268
n/a -- n/a	The Elfsight Telegram Chat CC plugin for WordPress is vulnerable to unauthorized modification of data to a missing capability check on the 'updatePreferences' function in all versions up to, and including, 1.1.0. This makes it possible for	2024-11-18	6.4	CVE-2024-10390

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
n/a -- n/a	The Gutenberg Blocks with AI by Kadence WP - Page Builder Features plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Countdown' widget in all versions up to, and including, 3.3.3 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.	2024-11-21	6.4	CVE-2024-10785
n/a -- n/a	The Quotes llama plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'quotes-llama' shortcode in all versions up to, and including, 3.0.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-23	6.4	CVE-2024-10874
n/a -- n/a	The Tribute Testimonials - WordPress Testimonial Grid/Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'tribute_testimonials_slider' shortcode in all versions up to, and including, 1.0.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-23	6.4	CVE-2024-10886
n/a -- n/a	The GD Rating System plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'extra_class' parameter in all versions up to, and including, 3.6.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-19	6.4	CVE-2024-11198
n/a -- n/a	The Rescue Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's rescue_progressbar shortcode in all versions up to, and including, 2.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-23	6.4	CVE-2024-11199
n/a -- n/a	The Parallax Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'position' parameter in all versions up to, and including, 1.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-19	6.4	CVE-2024-11224
n/a -- n/a	The Memberlite Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's memberlite_accordion shortcode in all versions up to, and including, 1.3.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-23	6.4	CVE-2024-11227
n/a -- n/a	The ????? ?? ???? - ???? ?? ???? plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's pafw_instant_payment shortcode in all versions up to, and including, 5.1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-23	6.4	CVE-2024-11228

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a -- n/a	The ???? ??? plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's add_plus_friends and add_plus_talk shortcodes in all versions up to, and including, 1.1.18 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-23	6.4	CVE-2024-11229
n/a -- n/a	The ???? ????? plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's mnp_purchase shortcode in all versions up to, and including, 3.3.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-23	6.4	CVE-2024-11231
n/a -- n/a	The HIPAA Compliant Forms with Drag'n'Drop HIPAA Form Builder. Sign HIPAA documents plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'hipaatizer' shortcode in all versions up to, and including, 1.3.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-23	6.4	CVE-2024-11332
n/a -- n/a	The Control horas plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ch_registro' shortcode in all versions up to, and including, 1.0.1 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.	2024-11-22	6.4	CVE-2024-11381
n/a -- n/a	The Pure CSS Circle Progress bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'circle_progress' shortcode in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-21	6.4	CVE-2024-11385
n/a -- n/a	The Easy Liveblogs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'elb_liveblog' shortcode in all versions up to, and including, 2.3.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-23	6.4	CVE-2024-11387
n/a -- n/a	The Dino Game - Embed Google Chrome Dinosaur Game in WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'dino-game' shortcode in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-21	6.4	CVE-2024-11388
n/a -- n/a	The Slotti Ajanvaraus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'slotti' shortcode in all versions up to, and including, 1.3.0 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.	2024-11-23	6.4	CVE-2024-11408
n/a -- n/a	The Shine PDF Embeder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'shinepdf' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied	2024-11-21	6.4	CVE-2024-11412

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
n/a -- n/a	The RecipePress Reloaded plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Recipe Ingredients in all versions up to, and including, 2.12.0 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.	2024-11-21	6.4	CVE-2024-11414
n/a -- n/a	The Slick Sitemap plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'slick-sitemap' shortcode in all versions up to, and including, 2.0.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-21	6.4	CVE-2024-11424
n/a -- n/a	The AutoListicle: Automatically Update Numbered List Articles plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'auto-list-number' shortcode in all versions up to, and including, 1.2.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-23	6.4	CVE-2024-11426
n/a -- n/a	The Lazy load videos and sticky control plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'lazy-load-videos-and-sticky-control' shortcode in all versions up to, and including, 3.0.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-21	6.4	CVE-2024-11428
n/a -- n/a	The SuevaFree Essential Kit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'counter' shortcode in all versions up to, and including, 1.1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-21	6.4	CVE-2024-11432
n/a -- n/a	The StreamWeasels Online Status Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'sw-status-bar' shortcode in all versions up to, and including, 2.1.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-21	6.4	CVE-2024-11438
n/a -- n/a	The Grey Owl Lightbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'gol_button' shortcode in all versions up to, and including, 1.6.1 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.	2024-11-21	6.4	CVE-2024-11440
n/a -- n/a	The Include Mastodon Feed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'include-mastodon-feed' shortcode in all versions up to, and including, 1.9.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-21	6.4	CVE-2024-11455

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a -- n/a	The Product Designer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.35 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.	2024-11-21	6.4	CVE-2024-9111
n/a -- n/a	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to view, modify, and delete data without proper authorization. The vulnerability is due to a failure to limit access to resources that are intended for users with Administrator privileges. An attacker could exploit this vulnerability by convincing a user to click a malicious URL. A successful exploit could allow a low-privileged attacker to list, view, create, edit, and delete templates in the same manner as a user with Administrator privileges.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-18	6.3	CVE-2020-3539
n/a -- n/a	A vulnerability in the web-based management interface of Cisco Small Business RV042 Dual WAN VPN Routers and Cisco Small Business RV042G Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-18	6.1	CVE-2020-3431
n/a -- n/a	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.This advisory is part of the October 2021 release of the Cisco ASA, FTD, and FMC Security Advisory Bundled publication. For a complete list of the advisories and links to them, see .	2024-11-18	6.1	CVE-2021-1444
n/a -- n/a	The Wishlist for WooCommerce: Multi Wishlists Per Customer PRO plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'wtab' parameter in versions 3.0.8 to 3.1.2 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. Note: Only WordPress installations with versions of PHP <=7.4 are affected by this vulnerability.	2024-11-23	6.1	CVE-2024-10519
n/a -- n/a	The Co-marquage service-public.fr 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, 0.5.76. 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.	2024-11-21	6.1	CVE-2024-10522

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a -- n/a	The ForumEngine theme for WordPress is vulnerable to Reflected Cross-Site Scripting via a URL in all versions up to, and including, 1.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-11-21	6.1	CVE-2024-10623
n/a -- n/a	The affiliate-toolkit plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via a URL in all versions up to, and including, 3.6.7 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.	2024-11-21	6.1	CVE-2024-10675
n/a -- n/a	The Announcement & Notification Banner - Bulletin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg and remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.11.7. 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.	2024-11-21	6.1	CVE-2024-10682
n/a -- n/a	The Friendly Functions for Welcart plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.4. This is due to missing or incorrect nonce validation on the settings update functionality. This makes it possible for unauthenticated attackers to inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-11-21	6.1	CVE-2024-10726
n/a -- n/a	The Easiest Funnel Builder For WordPress & WooCommerce by WPFunnels plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'post_id' parameter in all versions up to, and including, 3.5.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. This was partially patched in 3.5.4 and fully patched in 3.5.5.	2024-11-21	6.1	CVE-2024-10792
n/a -- n/a	The WordPress Brute Force Protection - Stop Brute Force Attacks 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, 2.2.6. 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.	2024-11-23	6.1	CVE-2024-10869
n/a -- n/a	The JobBoardWP - Job Board Listings and Submissions 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, 1.3.0. 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.	2024-11-23	6.1	CVE-2024-10880
n/a -- n/a	The WPAdverts - Classifieds Plugin 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, 2.1.7. 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.	2024-11-21	6.1	CVE-2024-10890
n/a -- n/a	The Formidable Forms - Contact Form Plugin, Survey, Quiz, Payment, Calculator Form & Custom Form Builder plugin for WordPress is vulnerable to POST-Based Reflected Cross-Site Scripting via the Custom HTML Form parameters in all versions up to, and including, 6.16.1.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary	2024-11-23	6.1	CVE-2024-11188

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.			
n/a -- n/a	The Premium Packages - Sell Digital Products Securely 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, 5.9.3. 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.	2024-11-22	6.1	CVE-2024-11225
n/a -- n/a	The 404 Solution plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via URLs in all versions up to, and including, 2.35.19 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.	2024-11-20	6.1	CVE-2024-11277
n/a -- n/a	The GD bbPress Attachments 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, 4.7.2. 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.	2024-11-20	6.1	CVE-2024-11278
n/a -- n/a	The Custom CSS, JS & PHP 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, 2.3.0. 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.	2024-11-23	6.1	CVE-2024-11330
n/a -- n/a	The Page Parts plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of remove_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.	2024-11-21	6.1	CVE-2024-11360
n/a -- n/a	The PDF Invoices & Packing Slips Generator 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, 2.2.1. 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.	2024-11-23	6.1	CVE-2024-11361
n/a -- n/a	The Payments Plugin and Checkout Plugin for WooCommerce: Stripe, PayPal, Square, Authorize.net 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, 1.112.0. 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.	2024-11-23	6.1	CVE-2024-11362
n/a -- n/a	The Crypto and DeFi Widgets - Web3 Cryptocurrency Shortcodes 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, 1.1.6. 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.	2024-11-21	6.1	CVE-2024-11365
n/a -- n/a	The Subaccounts 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, 1.6.0. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that	2024-11-21	6.1	CVE-2024-11370

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execute if they can successfully trick a user into performing an action such as clicking on a link.			
n/a -- n/a	The Theater for WordPress 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, 0.18.6.2. 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.	2024-11-21	6.1	CVE-2024-11371
n/a -- n/a	The WIP Incoming Lite plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.1. This is due to missing or incorrect nonce validation on the save_option() function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-11-21	6.1	CVE-2024-11416
n/a -- n/a	The salavat counter Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'page' parameter in all versions up to, and including, 0.9.1 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.	2024-11-21	6.1	CVE-2024-11435
n/a -- n/a	The Chessgame Shizzle plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'cs_nonce' parameter in all versions up to, and including, 1.3.0 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.	2024-11-23	6.1	CVE-2024-11446
n/a -- n/a	The Community by PeepSo - Download from PeepSo.com plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'filter' parameter in all versions up to, and including, 6.4.6.2 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.	2024-11-21	6.1	CVE-2024-11447
n/a -- n/a	The Run Contests, Raffles, and Giveaways with ContestsWP 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, 2.0.3. 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.	2024-11-21	6.1	CVE-2024-11456
n/a -- n/a	The DeBounce Email Validator plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'from', 'to', and 'key' parameters in all versions up to, and including, 5.6.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-11-23	6.1	CVE-2024-11463
n/a -- n/a	The MailChimp Forms by MailMunch 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, 3.2.3. 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.	2024-11-20	6.1	CVE-2024-8726

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a -- n/a	The MailMunch - Grow your Email List 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, 3.1.8. 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.	2024-11-22	6.1	CVE-2024-8735
n/a -- n/a	The Booster for WooCommerce 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, 7.2.3. 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.	2024-11-20	6.1	CVE-2024-9239
n/a -- n/a	The Branda - White Label & Branding, Custom Login Page Customizer plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.4.19. 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.	2024-11-21	6.1	CVE-2024-9371
n/a -- n/a	The Checkout with Cash App on WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the '_wp_http_referer' parameter in several files in all versions up to, and including, 6.0.2 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.	2024-11-23	6.1	CVE-2024-9635
n/a -- n/a	The Restaurant Menu - Food Ordering System - Table Reservation plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'action' parameter in all versions up to, and including, 2.4.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-11-20	6.1	CVE-2024-9653
n/a -- n/a	The Ashe theme 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, 2.243. 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.	2024-11-19	6.1	CVE-2024-9777
n/a -- n/a	A low privileged remote attacker may gain access to forbidden diagnostic data due to incorrect permission assignment for critical resources.	2024-11-18	5.7	CVE-2024-41970
n/a -- n/a	The Gallery Blocks with Lightbox. Image Gallery, (HTML5 video , YouTube, Vimeo) Video Gallery and Lightbox for native gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the gallery link text parameter in all versions up to, and including, 3.2.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Editor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-22	5.5	CVE-2024-10034
n/a -- n/a	The SVG Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REST API SVG File uploads in all versions up to, and including, 1.1.24 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-11-19	5.5	CVE-2024-11098

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a -- n/a	Unrestricted Upload of File with Dangerous Type, Improper Input Validation, Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in django CMS Association django Filer allows Input Data Manipulation, Stored XSS.This issue affects django Filer: from 3 before 3.3.	2024-11-20	5.5	CVE-2024-11404
n/a -- n/a	InDesign Desktop versions 19.0, 20.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-21	5.5	CVE-2024-49529
n/a -- n/a	Substance3D - Stager versions 3.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-22	5.5	CVE-2024-52998
n/a -- n/a	A vulnerability in the web-based interface of Cisco Webex Teams could allow an authenticated, remote attacker to conduct cross-site scripting attacks. The vulnerability is due to improper validation of usernames. An attacker could exploit this vulnerability by creating an account that contains malicious HTML or script content and joining a space using the malicious account name. A successful exploit could allow the attacker to conduct cross-site scripting attacks and potentially gain access to sensitive browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-18	5.4	CVE-2020-26067
n/a -- n/a	The Yaad Sarig Payment Gateway For WC plugin for WordPress is vulnerable to unauthorized modification & access of data due to a missing capability check on the yaadpay_view_log_callback() and yaadpay_delete_log_callback() functions in all versions up to, and including, 2.2.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view and delete logs.	2024-11-20	5.4	CVE-2024-10665
n/a -- n/a	A low privileged remote attacker may modify the docker settings setup of the device, leading to a limited DoS.	2024-11-18	5.4	CVE-2024-41968
n/a -- n/a	The Product Table for WooCommerce by CodeAstrology (wooproducttable.com) plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.5.1 via the var_dump_table parameter. This makes it possible for unauthenticated attackers var data.	2024-11-23	5.3	CVE-2024-10813
n/a -- n/a	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.	2024-11-23	5.3	CVE-2024-41761
n/a -- n/a	A flaw was found in Avahi-daemon, which relies on fixed source ports for wide-area DNS queries. This issue simplifies attacks where malicious DNS responses are injected.	2024-11-21	5.3	CVE-2024-52615
n/a -- n/a	A flaw was found in the Avahi-daemon, where it initializes DNS transaction IDs randomly only once at startup, incrementing them sequentially after that. This predictable behavior facilitates DNS spoofing attacks, allowing attackers to guess transaction IDs.	2024-11-21	5.3	CVE-2024-52616
n/a -- n/a	IBM PowerVM Platform KeyStore (IBM PowerVM Hypervisor FW950.00 through FW950.90, FW1030.00 through FW1030.60 FW1050.00 through FW1050.20, and FW1060.00 through FW1060.10 functionality can be compromised if an attacker gains service access to the HMC. An attacker that gains service access to the HMC can locate and through a series of service procedures decrypt data contained in the Platform KeyStore.	2024-11-22	5.1	CVE-2024-41781

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a -- n/a	A vulnerability in a certain REST API endpoint of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to perform a path traversal attack on an affected device. The vulnerability is due to insufficient path restriction enforcement. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to overwrite or list arbitrary files on the affected device.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-18	4.6	CVE-2020-3538
n/a -- n/a	A vulnerability in the distribution list feature of Cisco Webex Meetings could allow an authenticated, remote attacker to modify a distribution list that belongs to another user of their organization. The vulnerability is due to insufficient authorization enforcement for requests to update distribution lists. An attacker could exploit this vulnerability by sending a crafted request to the Webex Meetings interface to modify an existing distribution list. A successful exploit could allow the attacker to modify a distribution list that belongs to a user other than themselves.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-18	4.3	CVE-2021-1410
n/a -- n/a	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Content Security Management Appliance (SMA) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability exists because confidential information is being included in HTTP requests that are exchanged between the user and the device. An attacker could exploit this vulnerability by looking at the raw HTTP requests that are sent to the interface. A successful exploit could allow the attacker to obtain some of the passwords that are configured throughout the interface.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-18	4.3	CVE-2021-1425
n/a -- n/a	The WP User Manager - User Profile Builder & Membership plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'add_sidebar' and 'remove_sidebar' functions in all versions up to, and including, 2.9.11. This makes it possible for authenticated attackers, with Subscriber-level access and above, to add or remove a Carbon Fields custom sidebar if the Carbon Fields (carbon-fields) plugin is installed.	2024-11-23	4.3	CVE-2024-10216
n/a -- n/a	The Stratum - Elementor Widgets plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.4 in includes/templates/content-switcher.php. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft template data.	2024-11-21	4.3	CVE-2024-10316
n/a -- n/a	The The Plus Addons for Elementor - Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 6.0.3 via the render function in modules/widgets/tp_carousel_anything.php, modules/widgets/tp_page_scroll.php, and other widgets. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft template data.	2024-11-20	4.3	CVE-2024-10365
n/a -- n/a	The Ultimate Member - User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to unauthorized profile picture updates due to a missing capability check on the wp_ajax_um_resize_image() and ajax_resize_image() functions in all versions up to, and including, 2.8.9. This makes it possible for authenticated attackers, with subscriber-level access and above, to update the profile pictures of other users.	2024-11-21	4.3	CVE-2024-10528
n/a -- n/a	The Bard Extra plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the bardxtra_import_xml() function in all	2024-11-21	4.3	CVE-2024-10532

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	versions up to, and including, 1.2.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to import demo data.			
n/a -- n/a	The WP User Manager - User Profile Builder & Membership plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the validate_user_meta_key() function in all versions up to, and including, 2.9.11. This makes it possible for authenticated attackers, with Subscriber-level access and above, to enumerate user meta keys.	2024-11-23	4.3	CVE-2024-10537
n/a -- n/a	The WP Travel Engine - Tour Booking Plugin - Tour Operator Software plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the wpte_onboard_save_function_callback() function in all versions up to, and including, 6.2.1. This makes it possible for authenticated attackers, with contributor-level access and above, to modify several settings that could have an impact such as lost revenue and page updates.	2024-11-23	4.3	CVE-2024-10606
n/a -- n/a	The Easy Twitter Feed - Twitter feeds plugin for WP plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.2.6 via the [etf] shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from password protected, private, or draft posts that they should not have access to.	2024-11-22	4.3	CVE-2024-10666
n/a -- n/a	The Button Block - Get fully customizable & multi-functional buttons plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.1.4 via the [btn_block] shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from password protected, private, or draft posts that they should not have access to.	2024-11-21	4.3	CVE-2024-10671
n/a -- n/a	The UltraAddons - Elementor Addons (Header Footer Builder, Custom Font, Custom CSS,Woo Widget, Menu Builder, Anywhere Elementor Shortcode) plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.1.8 via the show_template due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Contributor-level access and above, to expose the contents of draft, private, and pending posts.	2024-11-21	4.3	CVE-2024-10696
n/a -- n/a	The Theme Builder For Elementor plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.2.2 via the 'elementor-template' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created by Elementor that they should not have access to.	2024-11-21	4.3	CVE-2024-10782
n/a -- n/a	The If-So Dynamic Content Personalization plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.9.2.1 via the 'ifso-show-post' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created via Elementor that they should not have access to.	2024-11-21	4.3	CVE-2024-10796
n/a -- n/a	The Enter Addons - Ultimate Template Builder for Elementor plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 2.1.9 via the Advanced Tabs widget due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created by Elementor that they should not have access to.	2024-11-23	4.3	CVE-2024-10868
n/a -- n/a	The Increase Maximum Upload File Size | Increase Execution Time plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.1.3. This is due to returning image upload error messages with full path information. This makes it possible for authenticated attackers, with author-level	2024-11-23	4.3	CVE-2024-11265

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	permissions and above, to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.			
n/a -- n/a	The My Contador lesr plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the exportar_registros() function in all versions up to, and including, 2.0. This makes it possible for unauthenticated attackers to export user data.	2024-11-21	4.3	CVE-2024-11334
n/a -- n/a	The Ultimate YouTube Video & Shorts Player With Vimeo plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the del_ytsingvid() function in all versions up to, and including, 3.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete single playlists.	2024-11-21	4.3	CVE-2024-11354
n/a -- n/a	The Ultimate YouTube Video & Shorts Player With Vimeo plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the get_setting() function in all versions up to, and including, 3.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view settings for playlists.	2024-11-22	4.3	CVE-2024-11355
n/a -- n/a	IBM Watson Query on Cloud Pak for Data 1.8, 2.0, 2.1, 2.2 and IBM Db2 Big SQL on Cloud Pak for Data 7.3, 7.4, 7.5, and 7.6 could allow an authenticated user to obtain sensitive information due to insufficient session expiration.	2024-11-23	4.3	CVE-2024-35160
n/a -- n/a	IBM Concert Software 1.0.0, 1.0.1, 1.0.2, and 1.0.2.1 could allow an authenticated user to obtain sensitive information that could aid in further attacks against the system.	2024-11-19	4.3	CVE-2024-37070
n/a -- n/a	The WPDash Notes plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'wp_ajax_post_it_list_comment' function in all versions up to, and including, 1.3.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to view comments on any post, including private and password protected posts, and pending and draft posts if they were previously published. The vulnerability was partially patched in version 1.3.5.	2024-11-23	4.3	CVE-2024-9223
n/a -- n/a	The Lock User Account plugin for WordPress is vulnerable to user lock bypass in all versions up to, and including, 1.0.5. This is due to permitting application password logins when user accounts are locked. This makes it possible for authenticated attackers, with existing application passwords, to interact with the vulnerable site via an API such as XML-RPC or REST despite their account being locked.	2024-11-21	4.2	CVE-2024-11197
pluginus -- woocommerce_products_filter	The HUSKY - Products Filter Professional for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the really_curr_tax parameter in all versions up to, and including, 1.3.6.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-11-19	6.1	CVE-2024-11400
smarttek -- smart_doctor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Smarttek Informatics Smart Doctor allows Stored XSS.This issue affects Smart Doctor: through 21.11.2024. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-21	5.4	CVE-2024-7016
sureshkumar -- wp-login_customizer	Cross-Site Request Forgery (CSRF) vulnerability in Suresh Kumar wp-login customizer allows Stored XSS.This issue affects wp-login customizer: from n/a through 1.0.	2024-11-18	6.1	CVE-2024-52424

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
terryl -- wp_githuber_md	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Terry Lin WP Githuber MD allows Stored XSS.This issue affects WP Githuber MD: from n/a through 1.16.3.	2024-11-18	5.4	CVE-2024-52422
themify -- builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themify Themify Builder allows Stored XSS.This issue affects Themify Builder: from n/a through 7.6.3.	2024-11-18	5.4	CVE-2024-52423
trcore -- dvc	The DVC from TRCore encrypts files using a hardcoded key. Attackers can use this key to decrypt the files and restore the original content.	2024-11-18	5.5	CVE-2024-11308
urchenko -- drozd	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Urchenko Drozd - Addons for Elementor allows Stored XSS.This issue affects Drozd - Addons for Elementor: from n/a through 1.1.1.	2024-11-18	5.4	CVE-2024-52425
w3speedster -- w3speedster	Cross-Site Request Forgery (CSRF) vulnerability in W3speedster W3SPEEDSTER.This issue affects W3SPEEDSTER: from n/a through 7.25.	2024-11-19	6.5	CVE-2024-52392
wowdevs -- sky_addons_for_elementor	The Sky Addons for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.6.1 via the render function in modules/content-switcher/widgets/content-switcher.php. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft Elementor template data.	2024-11-21	4.3	CVE-2024-9542
wpzoom -- beaver_builder_addons	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPZOOM Beaver Builder Addons by WPZOOM allows Stored XSS.This issue affects Beaver Builder Addons by WPZOOM: from n/a through 1.3.4.	2024-11-19	5.4	CVE-2024-30424
--Lingdang CRM	A vulnerability classified as critical was found in ä¸Šæµ·ç¤µå½¢ä¿¡æ¯ç§‘æœ€é™å…¬å¸ Lingdang CRM up to 8.6.4.3. Affected by this vulnerability is an unknown functionality of the file /crm/WeiXinApp/marketing/index.php?module=Users&action=getActionList. The manipulation of the argument userid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-12	6.3	CVE-2024-11121
--Lingdang CRM	A vulnerability, which was classified as critical, has been found in ä¸Šæµ·ç¤µå½¢ä¿¡æ¯ç§‘æœ€é™å…¬å¸ Lingdang CRM up to 8.6.4.3. Affected by this issue is some unknown functionality of the file /crm/wechatSession/index.php?msgid=1&operation=upload. The manipulation of the argument file leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-12	6.3	CVE-2024-11122
--Lingdang CRM	A vulnerability, which was classified as problematic, was found in ä¸Šæµ·ç¤µå½¢ä¿¡æ¯ç§‘æœ€é™å…¬å¸ Lingdang CRM up to 8.6.4.3. This affects an unknown part of the file /crm/data/pdf.php. The manipulation of the argument url with the input ../config.inc.php leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-12	4.3	CVE-2024-11123
1000 Projects-- Beauty Parlour Management System	A vulnerability was found in 1000 Projects Beauty Parlour Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/search-invoices.php. The manipulation of the argument searchdata leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-12	4.7	CVE-2024-11101

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
10up--Simple Local Avatars	The Simple Local Avatars plugin for WordPress is vulnerable to unauthorized modification of datadue to a missing capability check on the sla_clear_user_cache function in all versions up to, and including, 2.7.11. This makes it possible for authenticated attackers, with Subscriber-level access and above, to clear user caches.	2024-11-16	4.3	CVE-2024-10786
aaron13100--404 Solution	The 404 Solution plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.35.17 via the export feature. This makes it possible for unauthenticated attackers to extract sensitive data such as redirects including GET parameters which may reveal sensitive information.	2024-11-16	5.3	CVE-2024-11094
Abdullah--Extender All In One For Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Abdullah Extender All In One For Elementor allows Stored XSS.This issue affects Extender All In One For Elementor: from n/a through 1.0.3.	2024-11-11	6.5	CVE-2024-51575
adobe -- after_effects	After Effects versions 23.6.9, 24.6.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47444
adobe -- after_effects	After Effects versions 23.6.9, 24.6.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47445
adobe -- after_effects	After Effects versions 23.6.9, 24.6.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47446
adobe -- audition	Audition versions 23.6.9, 24.4.6 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47449
adobe -- bridge	Bridge versions 13.0.9, 14.1.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-45147
adobe -- bridge	Bridge versions 13.0.9, 14.1.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47458
adobe -- illustrator	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47453
adobe -- illustrator	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47454
adobe -- illustrator	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47455

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- illustrator	Illustrator versions 28.7.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47456
adobe -- illustrator	Illustrator versions 28.7.1 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47457
adobe -- indesign	InDesign Desktop versions ID18.5.3, ID19.5 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-49510
adobe -- indesign	InDesign Desktop versions ID18.5.3, ID19.5 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-49511
adobe -- indesign	InDesign Desktop versions ID18.5.3, ID19.5 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-49512
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47435
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47436
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47437
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by a Write-what-where Condition vulnerability that could lead to a memory leak. This vulnerability allows an attacker to write a controlled value at a controlled memory location, which could result in the disclosure of sensitive memory content. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47438
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47439
adobe -- substance_3d_painter	Substance3D - Painter versions 10.1.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-47440

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Animate	Animate versions 23.0.7, 24.0.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-12	5.5	CVE-2024-49527
Adobe--Audition	Audition versions 23.6.9, 24.4.6 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-11-15	5.5	CVE-2024-49536
airties -- air4443_firmware	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AirTies Air4443 Firmware allows Cross-Site Scripting (XSS).This issue affects Air4443 Firmware: through 14102024. NOTE: The vendor was contacted and it was learned that the product classified as End-of-Life and End-of-Support.	2024-11-13	6.1	CVE-2024-9477
amd -- ryzen_ai_software	Improper validation of user input in the NPU driver could allow an attacker to provide a buffer with unexpected size, potentially leading to system crash.	2024-11-12	5.5	CVE-2024-21949
AMI--AptioV	APTIOV contains a vulnerability in BIOS where may cause Improper Access Control by a local attacker. Successful exploitation of this vulnerability may lead to unexpected SPI flash modifications and BIOS boot kit launches, also impacting the availability.	2024-11-12	6.3	CVE-2024-2315
AMI--AptioV	APTIOV contains a vulnerability in BIOS where an attacker may cause an Improper Restriction of Operations within the Bounds of a Memory Buffer by local. Successful exploitation of this vulnerability may lead to privilege escalation and potentially arbitrary code execution, and impact Integrity.	2024-11-12	4.8	CVE-2024-33658
AMI--AptioV	An exploit is possible where an actor with physical access can manipulate SPI flash without being detected.	2024-11-12	4.3	CVE-2024-33660
ampache -- ampache	Ampache is a web based audio/video streaming application and file manager. The current implementation of token parsing does not adequately validate CSRF tokens when users delete messages. This vulnerability could be exploited to forge CSRF attacks, allowing an attacker to delete messages to any user, including administrators, if they interact with a malicious request. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-11-11	5.4	CVE-2024-51488
ampache -- ampache	Ampache is a web based audio/video streaming application and file manager. The current implementation of token parsing does not adequately validate CSRF tokens when users send messages to one another. This vulnerability could be exploited to forge CSRF attacks, allowing an attacker to send messages to any user, including administrators, if they interact with a malicious request. This issue has been addressed in version 7.0.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-11-11	5.4	CVE-2024-51489
andsonsdesign -- wp-contest	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SONS Creative Development WP Contest allows SQL Injection.This issue affects WP Contest: from n/a through 1.0.0.	2024-11-11	6.5	CVE-2024-51837
anisha -- jonnys_liquor	A Reflected cross-site scripting (XSS) vulnerability in browse.php of Code-projects Jonnys Liquor 1.0 allows remote attackers to inject arbitrary web scripts or HTML via the search parameter.	2024-11-13	6.1	CVE-2024-50969
Apereo--CAS	A vulnerability was found in Apereo CAS 6.6. It has been classified as critical. This affects an unknown part of the file /login?service of the component 2FA. The manipulation leads to improper authentication. It is possible to initiate the attack	2024-11-14	6.3	CVE-2024-11209

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.			
Apereo--CAS	A vulnerability has been found in Apereo CAS 6.6 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /login. The manipulation of the argument redirect_uri leads to open redirect. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-14	4.3	CVE-2024-11207
augustinfotech--SVG Case Study	The SVG Case Study 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.	2024-11-16	6.4	CVE-2024-9850
ays-pro--Popup Box Create Countdown, Coupon, Video, Contact Form Popups	The Popup Box - Create Countdown, Coupon, Video, Contact Form Popups plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the deactivate_plugin_option() function in all versions up to, and including, 4.9.7. This makes it possible for unauthenticated attackers to update the 'ays_pb_upgrade_plugin' option with arbitrary data.	2024-11-16	5.3	CVE-2024-10861
bilbud--404 Error Monitor	The 404 Error Monitor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1. This is due to missing or incorrect nonce validation on the updatePluginSettings() function. This makes it possible for unauthenticated attackers to make changes to plugin settings and clear up all the error logs via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-11-16	5.3	CVE-2024-11118
BlackBerry--SecuSUITE	A local privilege escalation vulnerability in the SecuSUITE Server (System Configuration) of SecuSUITE versions 5.0.420 and earlier could allow a successful attacker that had gained control of code running under one of the system accounts listed in the configuration file to potentially issue privileged script commands.	2024-11-12	6.4	CVE-2024-51722
BlackBerry--SecuSUITE	An insufficient entropy vulnerability in the SecuSUITE Secure Client Authentication (SCA) Server of SecuSUITE versions 5.0.420 and earlier could allow an attacker to potentially enroll an attacker-controlled device to the victim's account and telephone number.	2024-11-12	4.8	CVE-2024-51720
Brocade--Fabric OS	A vulnerability in Brocade Fabric OS versions before 9.2.2 could allow man-in-the-middle attackers to conduct remote Service Session Hijacking that may arise from the attacker's ability to forge an SSH key while the Brocade Fabric OS Switch is performing various remote operations initiated by a switch admin.	2024-11-12	4.8	CVE-2024-7516
bu -- bu_slideshow	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Boston University (IS&T) BU Slideshow allows Stored XSS.This issue affects BU Slideshow: from n/a through 2.3.10.	2024-11-11	5.4	CVE-2024-52351
Business Directory Team by RadiusTheme--Classified Listing	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Business Directory Team by RadiusTheme Classified Listing classified-listing allows PHP Local File Inclusion.This issue affects Classified Listing: from n/a through 3.1.15.1.	2024-11-16	5.3	CVE-2024-52386
chatwoot--chatwoot/chatwoot	A Session Fixation vulnerability exists in chatwoot/chatwoot versions prior to 2.4.0. The application does not invalidate existing sessions on other devices when a user changes their password, allowing old sessions to persist. This can lead to unauthorized access if an attacker has obtained a session token.	2024-11-15	6.8	CVE-2021-3740

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cisco--Cisco Analog Telephone Adaptor (ATA) Software	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Adaptive Telephone Adapter firmware could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to an out-of-bounds read when processing Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol packets to an affected device. A successful exploit could allow the attacker to cause a service restart.Cisco has released firmware updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	5.3	CVE-2022-20766
Cisco--Cisco BroadWorks	A vulnerability in the web management interface of Cisco BroadWorks Hosted Thin Receptionist could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	5.4	CVE-2022-20948
Cisco--Cisco Catalyst SD-WAN Manager	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization checking and gain access to sensitive information on an affected system. This vulnerability is due to insufficient authorization checks. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to bypass authorization checking and gain access to sensitive information on the affected system.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	6.4	CVE-2021-1482
Cisco--Cisco Catalyst SD-WAN Manager	A vulnerability in the web UI of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to gain read and write access to information that is stored on an affected system. This vulnerability is due to improper handling of XML External Entity (XXE) entries when the affected software parses certain XML files. An attacker could exploit this vulnerability by persuading a user to import a crafted XML file with malicious entries. A successful exploit could allow the attacker to read and write files within the affected application.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	6.4	CVE-2021-1483
Cisco--Cisco Catalyst SD-WAN Manager	A vulnerability in the web UI of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to inject arbitrary commands on an affected system and cause a denial of service (DoS) condition. This vulnerability is due to improper input validation of user-supplied input to the device template configuration. An attacker could exploit this vulnerability by submitting crafted input to the device template configuration. A successful exploit could allow the attacker to cause a DoS condition on the affected system.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	6.5	CVE-2021-1484
Cisco--Cisco Catalyst SD-WAN Manager	A vulnerability in Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization checking and gain restricted access to the configuration information of an affected system. This vulnerability exists because the affected software has insufficient input validation for certain commands. An attacker could exploit this vulnerability by sending crafted requests to the affected commands of an affected system. A successful exploit could allow the attacker to bypass authorization checking and gain restricted access to the configuration data of the affected	2024-11-15	5	CVE-2021-1464

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	system.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.			
Cisco--Cisco Catalyst SD-WAN Manager	A vulnerability in the vDaemon service of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to cause a buffer overflow on an affected system, resulting in a denial of service (DoS) condition. The vulnerability is due to incomplete bounds checks for data that is provided to the vDaemon service of an affected system. An attacker could exploit this vulnerability by sending malicious data to the vDaemon listening service on the affected system. A successful exploit could allow the attacker to cause a buffer overflow condition on the affected system, which could allow the attacker to cause the vDaemon listening service to reload and result in a DoS condition.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	5.4	CVE-2021-1466
Cisco--Cisco Catalyst SD-WAN Manager	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability is due to improper input validation of SQL queries to an affected system. An attacker could exploit this vulnerability by authenticating to the application and sending malicious SQL queries to an affected system. A successful exploit could allow the attacker to modify values on or return values from the vManage database or the underlying operating system.Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.	2024-11-15	4.9	CVE-2021-1470
Cisco--Cisco Catalyst SD-WAN Manager	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct Cypher query language injection attacks on an affected system. This vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the interface of an affected system. A successful exploit could allow the attacker to obtain sensitive information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	4.3	CVE-2021-1481
Cisco--Cisco Enterprise Chat and Email	A vulnerability in the web-based management interface of Cisco ECE could allow an unauthenticated, remote attacker to conduct an XSS attack against a user of the interface of an affected device. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious script code in a chat window. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	6.1	CVE-2022-20631
Cisco--Cisco Enterprise Chat and Email	A vulnerability in the web-based management interface of Cisco ECE could allow an unauthenticated, remote attacker to conduct an XSS attack against a user of the interface of an affected device. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	6.1	CVE-2022-20632
Cisco--Cisco Enterprise Chat	A vulnerability in the web-based management interface of Cisco ECE could allow an unauthenticated, remote attacker to perform a username enumeration attack against an affected device.	2024-11-15	5.3	CVE-2022-20633

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
and Email	This vulnerability is due to differences in authentication responses that are sent back from the application as part of an authentication attempt. An attacker could exploit this vulnerability by sending authentication requests to an affected device. A successful exploit could allow the attacker to confirm existing user accounts, which could be used in further attacks. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.			
Cisco--Cisco Enterprise Chat and Email	A vulnerability in the web-based management interface of Cisco ECE could allow an unauthenticated, remote attacker to redirect a user to an undesired web page. This vulnerability is due to improper input validation of the URL parameters in an HTTP request that is sent to an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to cause the interface to redirect the user to a specific, malicious URL. This type of vulnerability is known as an open redirect and is used in phishing attacks that get users to unknowingly visit malicious sites.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	4.7	CVE-2022-20634
Cisco--Cisco Evolved Programmable Network Manager (EPNM)	A vulnerability in the web-based management interface of Cisco PI and Cisco EPNM could allow an authenticated, remote attacker to conduct a path traversal attack on an affected device. To exploit this vulnerability, the attacker must have valid credentials on the system. This vulnerability is due to insufficient input validation of the HTTPS URL by the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request that contains directory traversal character sequences to an affected device. A successful exploit could allow the attacker to write arbitrary files to the host system. Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.	2024-11-15	6.5	CVE-2022-20656
Cisco--Cisco Evolved Programmable Network Manager (EPNM)	A vulnerability in the web-based management interface of Cisco PI and Cisco EPNM could allow an unauthenticated, remote attacker to conduct an XSS attack against a user of the interface of an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.	2024-11-15	6.1	CVE-2022-20657
Cisco--Cisco Firepower Management Center	A vulnerability in the administrative web-based GUI configuration manager of Cisco Firepower Management Center Software could allow an authenticated, remote attacker to access sensitive configuration information. The attacker would require low privilege credentials on an affected device. This vulnerability is due to lack of proper encryption of sensitive information stored within the GUI configuration manager. An attacker could exploit this vulnerability by logging into the FMC GUI and navigating to certain sensitive configurations. A successful exploit could allow the attacker to view sensitive configuration parameters in clear text.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.[[Publication_URL{Layout()}]]This advisory is part of the October 2021 release of the Cisco ASA, FTD, and FMC Security Advisory Bundled publication. For a complete list of the advisories and links to them, see .	2024-11-15	4.3	CVE-2021-34750
Cisco--Cisco Firepower	A vulnerability in the administrative web-based GUI configuration manager of Cisco Firepower Management Center (FMC) Software could allow an authenticated,	2024-11-15	4.3	CVE-2021-34751

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management Center	remote attacker to access sensitive configuration information. The attacker would require low privilege credentials on an affected device. This vulnerability exists because of improper encryption of sensitive information stored within the GUI configuration manager. An attacker could exploit this vulnerability by logging into the GUI of Cisco FMC Software and navigating to certain sensitive configurations. A successful exploit could allow the attacker to view sensitive configuration parameters in clear text.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.[[Publication_URL{Layout()}]]This advisory is part of the October 2021 release of the Cisco ASA, FTD, and FMC Security Advisory Bundled publication. For a complete list of the advisories and links to them, see .			
Cisco--Cisco Firepower Threat Defense Software	A vulnerability in the CLI of Cisco FTD Software could allow an authenticated, local attacker with administrative privileges to execute arbitrary commands with root privileges on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user-supplied command arguments. An attacker could exploit this vulnerability by submitting crafted input to the affected commands. A successful exploit could allow the attacker to execute commands with root privileges on the underlying operating system. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	6.7	CVE-2021-34752
Cisco--Cisco Firepower Threat Defense Software	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of specific HTTP header parameters. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured file policy for HTTP packets and deliver a malicious payload.	2024-11-15	5.8	CVE-2021-1494
Cisco--Cisco Firepower Threat Defense Software	A vulnerability in the payload inspection for Ethernet Industrial Protocol (ENIP) traffic for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass configured rules for ENIP traffic. This vulnerability is due to incomplete processing during deep packet inspection for ENIP packets. An attacker could exploit this vulnerability by sending a crafted ENIP packet to the targeted interface. A successful exploit could allow the attacker to bypass configured access control and intrusion policies that should trigger and drop for the ENIP packet.	2024-11-15	5.8	CVE-2021-34753
Cisco--Cisco Industrial Network Director	A vulnerability in Cisco IND could allow an authenticated, local attacker to read application data. This vulnerability is due to insufficient default file permissions that are applied to the application data directory. An attacker could exploit this vulnerability by accessing files in the application data directory. A successful exploit could allow the attacker to view sensitive information. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	5.5	CVE-2023-20039
Cisco--Cisco IOS XE Catalyst SD-WAN	A vulnerability in the implementation of the Simple Network Management Protocol (SNMP) IPv4 access control list (ACL) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to perform SNMP polling of an affected device, even if it is configured to deny SNMP traffic. This vulnerability exists because Cisco IOS Software and Cisco IOS XE Software do not support extended IPv4 ACLs for SNMP, but they do allow administrators to configure extended named IPv4 ACLs that are attached to the SNMP server configuration without a warning message. This can result in no ACL being applied to the SNMP listening process. An attacker could exploit this vulnerability by	2024-11-15	5.3	CVE-2024-20373

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	performing SNMP polling of an affected device. A successful exploit could allow the attacker to perform SNMP operations that should be denied. The attacker has no control of the SNMP ACL configuration and would still need a valid SNMP version 2c (SNMPv2c) community string or SNMP version 3 (SNMPv3) user credentials. SNMP with IPv6 ACL configurations is not affected. For more information, see the section of this advisory.			
Cisco--Cisco IOS XR Software	A vulnerability in the TL1 function of Cisco Network Convergence System (NCS) 4000 Series could allow an authenticated, local attacker to cause a memory leak in the TL1 process. This vulnerability is due to TL1 not freeing memory under some conditions. An attacker could exploit this vulnerability by connecting to the device and issuing TL1 commands after being authenticated. A successful exploit could allow the attacker to cause the TL1 process to consume large amounts of memory. When the memory reaches a threshold, the Resource Monitor (Resmon) process will begin to restart or shutdown the top five consumers of memory, resulting in a denial of service (DoS).Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.This advisory is part of the September 2022 release of the Cisco IOS XR Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see .	2024-11-15	6	CVE-2022-20845
Cisco--Cisco IOS XR Software	A vulnerability in the Broadband Network Gateway PPP over Ethernet (PPPoE) feature of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause the PPPoE process to continually crash. This vulnerability exists because the PPPoE feature does not properly handle an error condition within a specific crafted packet sequence. An attacker could exploit this vulnerability by sending a sequence of specific PPPoE packets from controlled customer premises equipment (CPE). A successful exploit could allow the attacker to cause the PPPoE process to continually restart, resulting in a denial of service condition (DoS).Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.This advisory is part of the September 2022 release of the Cisco IOS XR Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see .	2024-11-15	6.1	CVE-2022-20849
Cisco--Cisco IOS XR Software	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause the Cisco Discovery Protocol process to reload on an affected device. This vulnerability is due to a heap buffer overflow in certain Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a heap overflow, which could cause the Cisco Discovery Protocol process to reload on the device. The bytes that can be written in the buffer overflow are restricted, which limits remote code execution.Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.This advisory is part of the September 2022 release of the Cisco IOS XR Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see .	2024-11-15	4.3	CVE-2022-20846
Cisco--Cisco Prime Access Registrar	A vulnerability in the web-based management interface of Cisco Prime Access Registrar Appliance could allow an authenticated, remote attacker to conduct a cross-site scripting attack against a user of the interface. The attacker would require valid credentials for the device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could	2024-11-15	5.5	CVE-2022-20626

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.			
Cisco--Cisco Prime Collaboration Deployment	A vulnerability in the web-based management interface of Cisco Prime Collaboration Deployment could allow an unauthenticated, remote attacker to conduct a cross-site scripting attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco plans to release software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	6.1	CVE-2023-20060
Cisco--Cisco Redundancy Configuration Manager	A vulnerability in a debug function for Cisco RCM for Cisco StarOS Software could allow an unauthenticated, remote attacker to perform debug actions that could result in the disclosure of confidential information that should be restricted. This vulnerability exists because of a debug service that incorrectly listens to and accepts incoming connections. An attacker could exploit this vulnerability by connecting to the debug port and executing debug commands. A successful exploit could allow the attacker to view sensitive debugging information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	5.3	CVE-2022-20648
Cisco--Cisco RoomOS Software	A vulnerability in pairing process of Cisco TelePresence CE Software and RoomOS Software for Cisco Touch 10 Devices could allow an unauthenticated, remote attacker to impersonate a legitimate device and pair with an affected device. This vulnerability is due to insufficient identity verification. An attacker could exploit this vulnerability by impersonating a legitimate device and responding to the pairing broadcast from an affected device. A successful exploit could allow the attacker to access the affected device while impersonating a legitimate device.There are no workarounds that address this vulnerability.	2024-11-15	6.8	CVE-2022-20793
Cisco--Cisco RoomOS Software	A vulnerability in Cisco TelePresence CE and RoomOS could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to improper access control on certain CLI commands. An attacker could exploit this vulnerability by running a series of crafted commands. A successful exploit could allow the attacker to elevate privileges to root. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	6.7	CVE-2023-20090
Cisco--Cisco RoomOS Software	Three vulnerabilities in the CLI of Cisco TelePresence CE and RoomOS could allow an authenticated, local attacker to overwrite arbitrary files on the local file system of an affected device. These vulnerabilities are due to improper access controls on files that are on the local file system. An attacker could exploit these vulnerabilities by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. To exploit these vulnerabilities, an attacker would need to have a remote support user account. Note: CVE-2023-20092 does not affect Cisco DX70, DX80, TelePresence MX Series, or TelePresence SX Series devices.	2024-11-15	4.4	CVE-2023-20004

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.			
Cisco--Cisco RoomOS Software	Three vulnerabilities in the CLI of Cisco TelePresence CE and RoomOS could allow an authenticated, local attacker to overwrite arbitrary files on the local file system of an affected device. These vulnerabilities are due to improper access controls on files that are on the local file system. An attacker could exploit these vulnerabilities by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. To exploit these vulnerabilities, an attacker would need to have a remote support user account. Note: CVE-2023-20092 does not affect Cisco DX70, DX80, TelePresence MX Series, or TelePresence SX Series devices. Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.	2024-11-15	4.4	CVE-2023-20092
Cisco--Cisco RoomOS Software	Three vulnerabilities in the CLI of Cisco TelePresence CE and RoomOS could allow an authenticated, local attacker to overwrite arbitrary files on the local file system of an affected device. These vulnerabilities are due to improper access controls on files that are on the local file system. An attacker could exploit these vulnerabilities by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. To exploit these vulnerabilities, an attacker would need to have a remote support user account. Note: CVE-2023-20092 does not affect Cisco DX70, DX80, TelePresence MX Series, or TelePresence SX Series devices. Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.	2024-11-15	4.4	CVE-2023-20093
Cisco--Cisco RoomOS Software	A vulnerability in Cisco TelePresence CE and RoomOS could allow an unauthenticated, adjacent attacker to view sensitive information on an affected device. This vulnerability exists because the affected software performs improper bounds checks. An attacker could exploit this vulnerability by sending a crafted request to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read that discloses sensitive information. Note: This vulnerability only affects Cisco Webex Desk Hub. There are no workarounds that address this vulnerability.	2024-11-15	4.3	CVE-2023-20094
Cisco--Cisco Secure Network Analytics	A vulnerability in the web-based management interface of Cisco Secure Network Analytics, formerly Stealthwatch Enterprise, could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.Attention: Simplifying the Cisco portfolio includes the renaming of security products under one brand: Cisco Secure. For more information, see .	2024-11-15	6.1	CVE-2022-20663

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cisco--Cisco Secure Web Appliance	A vulnerability in the web management interface of Cisco AsyncOS for Cisco Secure Web Appliance, formerly Cisco Web Security Appliance (WSA), could allow an authenticated, remote attacker to perform a command injection and elevate privileges to root. This vulnerability is due to insufficient validation of user-supplied input for the web interface. An attacker could exploit this vulnerability by authenticating to the system and sending a crafted HTTP packet to the affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root. To successfully exploit this vulnerability, an attacker would need at least read-only credentials.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.Attention: Simplifying the Cisco portfolio includes the renaming of security products under one brand: Cisco Secure. For more information, see .	2024-11-15	6.3	CVE-2022-20871
Cisco--Cisco Secure Workload	A vulnerability in the web-based management interface and in the API subsystem of Cisco Tetration could allow an authenticated, remote attacker to inject arbitrary commands to be executed with root-level privileges on the underlying operating system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by submitting a crafted HTTP message to the affected system. A successful exploit could allow the attacker to execute commands with root-level privileges. To exploit this vulnerability, an attacker would need valid administrator-level credentials.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	6.5	CVE-2022-20652
Cisco--Cisco Smart Software Manager On-Prem	A vulnerability in the web-based management interface of Cisco Smart Software Manager On-Prem could allow an authenticated, remote attacker to elevate privileges on an affected system. This vulnerability is due to inadequate protection of sensitive user information. An attacker could exploit this vulnerability by accessing certain logs on an affected system. A successful exploit could allow the attacker to use the obtained information to elevate privileges to System Admin.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	4.3	CVE-2022-20939
Cisco--Cisco TelePresence Endpoint Software (TC/CE)	A vulnerability in the version control of Cisco TelePresence CE Software for Cisco Touch 10 Devices could allow an unauthenticated, adjacent attacker to install an older version of the software on an affected device. This vulnerability is due to insufficient version control. An attacker could exploit this vulnerability by installing an older version of Cisco TelePresence CE Software on an affected device. A successful exploit could allow the attacker to take advantage of vulnerabilities in older versions of the software.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	6.5	CVE-2022-20931
Cisco--Cisco TelePresence Endpoint Software (TC/CE)	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS could allow an authenticated, local attacker to overwrite arbitrary files on the local file system of an affected device. This vulnerability is due to improper access controls on files that are on the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. To exploit this vulnerability, an attacker would need to have a remote support user account. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	5.1	CVE-2023-20091

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cisco--Cisco Webex Meetings	A vulnerability in the web-based interface of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based interface of Cisco Webex Meetings. An attacker could exploit this vulnerability by persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2024-11-15	6.1	CVE-2022-20654
cmanon--WP-Strava	The WP-Strava plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.12.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-11-13	6.1	CVE-2024-10038
code-projects--Farmacia	A vulnerability classified as critical was found in code-projects Farmacia 1.0. This vulnerability affects unknown code of the file /editar-cliente.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-15	6.3	CVE-2024-11244
code-projects--Farmacia	A vulnerability, which was classified as critical, has been found in code-projects Farmacia 1.0. This issue affects some unknown processing of the file /editar-produto.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-15	6.3	CVE-2024-11245
code-projects--Inventory Management	A vulnerability was found in code-projects Inventory Management up to 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /model/editProduct.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-15	6.3	CVE-2024-11250
code-projects--Online Shop Store	A vulnerability classified as problematic has been found in code-projects Online Shop Store 1.0. This affects an unknown part of the file /signup.php. The manipulation of the argument m2 with the input <svg%20onload=alert(document.cookie)> 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.	2024-11-15	4.3	CVE-2024-11243
code-projects--Task Manager	A vulnerability, which was classified as critical, was found in code-projects Task Manager 1.0. This affects an unknown part of the file /newProject.php. The manipulation of the argument projectName leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-12	6.3	CVE-2024-11096
coolplugins -- web_stories_widgets_for_elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Cool Plugins Web Stories Widgets For Elementor allows Stored XSS.This issue affects Web Stories Widgets For Elementor: from n/a through 1.1.	2024-11-11	5.4	CVE-2024-52354
crm2go -- crm2go	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CRM 2go allows DOM-Based XSS.This issue affects CRM 2go: from n/a through 1.0.	2024-11-11	5.4	CVE-2024-52350
cscode--EleForms All In One Form Integration including DB for	The EleForms - All In One Form Integration including DB for Elementor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.9.9.9. This is due to missing or incorrect nonce validation when deleting form submissions. This makes it possible for unauthenticated attackers to	2024-11-16	4.3	CVE-2024-6628

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Elementor	delete form submissions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.			
cyberchimps -- responsive_addons_for_elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Cyberchimps Responsive Addons for Elementor allows DOM-Based XSS.This issue affects Responsive Addons for Elementor: from n/a through 1.5.4.	2024-11-11	5.4	CVE-2024-52358
dhoppe--Gallery Manager	The Gallery Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of remove_Query_Arg without appropriate escaping on the URL in all versions up to, and including, 1.6.58. 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.	2024-11-16	6.1	CVE-2024-10875
duongancol--Boostify Header Footer Builder for Elementor	The Boostify Header Footer Builder for Elementor plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.3.6 via the 'bhf' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created via Elementor that they should not have access to.	2024-11-13	4.3	CVE-2024-10794
EasyPHP--EasyPHP web server	Absolute path traversal (incorrect restriction of a path to a restricted directory) vulnerability in the EasyPHP web server, affecting version 14.1. This vulnerability could allow remote users to bypass SecurityManager restrictions and retrieve any file stored on the server by setting only consecutive strings '/...%5c'.	2024-11-14	6.5	CVE-2024-11215
egolacrima--Hide Links	The Hide Links plugin for WordPress is vulnerable to unauthorized shortcode execution due to do_shortcode being hooked through the comment_text filter in all versions up to and including 1.4.2. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes available on the target site.	2024-11-13	5.3	CVE-2024-9578
ehues -- gboy_custom_google_map	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ehues Gboy Custom Google Map allows Blind SQL Injection.This issue affects Gboy Custom Google Map: from n/a through 1.2.	2024-11-11	6.5	CVE-2024-51882
element-hq--element-web	Element is a Matrix web client built using the Matrix React SDK. A malicious homeserver can send invalid messages over federation which can prevent Element Web and Desktop from rendering single messages or the entire room containing them. This was patched in Element Web and Desktop 1.11.85.	2024-11-12	5	CVE-2024-51750
engelen--BulkPress	The BulkPress 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, 0.3.5. 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.	2024-11-16	6.1	CVE-2024-9615
erzhongxmu--Jeewms	A vulnerability was found in erzhongxmu Jeewms up to 20241108. It has been rated as critical. This issue affects some unknown processing of the file cgReportController.do of the component AuthInterceptor. The manipulation of the argument begin_date leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. Other parameters might be affected as well.	2024-11-15	6.3	CVE-2024-11251
fbtopcn--(Fat Rat Collect) ,	The ????(Fat Rat Collect) ????????????????, ???????????????????????????? plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to missing escaping on a 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	2024-11-13	6.1	CVE-2024-10577

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	if they can successfully trick a user into performing an action such as clicking on a link.			
fortinet -- forticlient	An improper verification of cryptographic signature vulnerability [CWE-347] in FortiClient MacOS version 7.4.0, version 7.2.4 and below, version 7.0.10 and below, version 6.4.10 and below may allow a local authenticated attacker toÂ swap the installer with a malicious package via a race condition during the installation process.	2024-11-12	6.7	CVE-2024-40592
fortinet -- fortiweb	An exposure of sensitive system information to an unauthorized control sphere vulnerability [CWE-497] in FortiWeb version 7.6.0, version 7.4.3 and below, version 7.2.10 and below, version 7.0.10 and below, version 6.3.23 and below may allow an authenticated attacker to access the encrypted passwords of other administrators via the "Log Access Event" logs page.	2024-11-12	4.4	CVE-2024-36509
Fortinet-- FortiAnalyzer	Multiple improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerabilities [CWE-78] in Fortinet FortiManager version 7.4.0 through 7.4.2 and before 7.2.5, Fortinet FortiAnalyzer version 7.4.0 through 7.4.2 and before 7.2.5 and Fortinet FortiAnalyzer-BigData before 7.4.0 allows an authenticated privileged attacker to execute unauthorized code or commands via crafted CLI requests.	2024-11-12	6.7	CVE-2024-32118
Fortinet-- FortiAnalyzer	Multiple relative path traversal vulnerabilities [CWE-23] in Fortinet FortiManager version 7.4.0 through 7.4.2 and before 7.2.5, FortiAnalyzer version 7.4.0 through 7.4.2 and before 7.2.5 and FortiAnalyzer-BigData version 7.4.0 and before 7.2.7 allows a privileged attacker to delete files from the underlying filesystem via crafted CLI requests.	2024-11-12	5.1	CVE-2024-32116
Fortinet-- FortiAnalyzer	A heap-based buffer overflow in Fortinet FortiAnalyzer version 7.4.0 through 7.4.2, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, FortiManager version 7.4.0 through 7.4.2, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14 allows attacker to escalation of privilege via specially crafted http requests	2024-11-12	5.6	CVE-2024-33505
Fortinet-- FortiManager	A stack-based buffer overflow vulnerability [CWE-121] in Fortinet FortiManager version 7.4.0 through 7.4.2 and before 7.2.5, FortiAnalyzer version 7.4.0 through 7.4.2 and before 7.2.5 and FortiAnalyzer-BigData 7.4.0 and before 7.2.7 allows a privileged attacker to execute unauthorized code or commands via crafted CLI requests.	2024-11-12	6.7	CVE-2024-31496
Fortinet-- FortiManager	A missing authentication for critical function in Fortinet FortiManager version 7.4.0 through 7.4.2, 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.14, FortiPAM version 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.9, 7.0.0 through 7.0.17, 2.0.0 through 2.0.14, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiSwitchManager version 7.2.0 through 7.2.3, 7.0.0 through 7.0.3, FortiPortal version 6.0.0 through 6.0.14, FortiOS version 7.4.0 through 7.4.3, 7.2.0 through 7.2.7, 7.0.0 through 7.0.14, 6.4.0 through 6.4.15, 6.2.0 through 6.2.16, 6.0.0 through 6.0.18 allows attacker to execute unauthorized code or commands via specially crafted packets.	2024-11-12	5.3	CVE-2024-26011
Fortinet-- FortiManager	An exposure of sensitive information to an unauthorized actor [CWE-200] in Fortinet FortiManager before 7.4.2, FortiAnalyzer before 7.4.2 and FortiAnalyzer-BigData before 7.2.5 may allow a privileged attacker with administrative read permissions to read event logs of another adom via crafted HTTP or HTTPs requests.	2024-11-12	4.1	CVE-2023-44255
Fortinet-- FortiManager	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability [CWE-22] in Fortinet FortiManager version 7.4.0 through 7.4.2 and below 7.2.5, FortiAnalyzer version 7.4.0 through 7.4.2 and below 7.2.5 & FortiAnalyzer-BigData version 7.4.0 and below 7.2.7 allows a privileged attacker to read arbitrary files from the underlying system via crafted HTTP or HTTPs requests.	2024-11-12	4.9	CVE-2024-32117

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Fortinet--FortiOS	AnÂ improper neutralization of special elements in output used by a downstream component ('Injection') vulnerability [CWE-74] in FortiOS version 7.4.3 and below, version 7.2.8 and below, version 7.0.16 and below; FortiProxy version 7.4.3 and below, version 7.2.9 and below, version 7.0.16 and below; FortiSASE version 24.2.b SSL-VPN web user interface may allow a remote unauthenticated attacker to perform phishing attempts via crafted requests.	2024-11-12	4.3	CVE-2024-33510
Fortinet--FortiPortal	An authorization bypass through user-controlled key vulnerability [CWE-639] in Fortinet FortiPortal version 7.0.0 through 7.0.3 allows an authenticated attacker to interact with ressources of other organizations via HTTP or HTTPS requests.	2024-11-12	5.4	CVE-2023-47543
Fortra--Digital Guardian Agent	A security bypass vulnerability exists in the Removable Media Encryption (RME)component of Digital Guardian Windows Agents prior to version 8.2.0. This allows a user to circumvent encryption controls by modifying metadata on the USB device thereby compromising the confidentiality of the stored data.	2024-11-15	4.3	CVE-2024-3334
futuriowp -- futurio_extra	The Futurio Extra plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 2.0.13 via the 'elementor-template' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts that they should not have access to.	2024-11-12	4.3	CVE-2024-10695
get-simple -- getsimplecms	A vulnerability was found in GetSimpleCMS 3.3.16 and classified as problematic. This issue affects some unknown processing of the file /admin/profile.php. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-12	4.3	CVE-2024-11125
getumbrel--umbrel	Umbrel is a home server OS for self-hosting. The login functionality of Umbrel before version 1.2.2 contains a reflected cross-site scripting (XSS) vulnerability in use-auth.tsx. An attacker can specify a malicious redirect query parameter to trigger the vulnerability. If a JavaScript URL is passed to the redirect parameter the attacker provided JavaScript will be executed after the user entered their password and clicked on login. This vulnerability is fixed in 1.2.2.	2024-11-13	5.4	CVE-2024-49379
GitLab--GitLab	An issue was discovered in GitLab CE/EE affecting all versions starting from 17.2 prior to 17.3.7, starting from 17.4 prior to 17.4.4 and starting from 17.5 prior to 17.5.2, which could have allowed an attacker gaining full API access as the victim via the Device OAuth flow.	2024-11-14	6.8	CVE-2024-7404
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 16 before 17.3.7, 17.4 before 17.4.4, and 17.5 before 17.5.2. The vulnerability could allow an attacker to inject malicious JavaScript code in Analytics Dashboards through a specially crafted URL.	2024-11-14	6.1	CVE-2024-8648
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions from 17.3 before 17.3.7, 17.4 before 17.4.4, and 17.5 before 17.5.2. Improper output encoding could lead to XSS if CSP is not enabled.	2024-11-14	5.4	CVE-2024-8180
glpi-project--glpi	GLPI is a free asset and IT management software package. An unauthenticated user can provide a malicious link to a GLPI technician in order to exploit a reflected XSS vulnerability. Upgrade to 10.0.17.	2024-11-15	6.5	CVE-2024-41678
glpi-project--glpi	GLPI is a free asset and IT management software package. An authenticated user can exploit a SQL injection vulnerability from the ticket form. Upgrade to 10.0.17.	2024-11-15	6.5	CVE-2024-41679
glpi-project--glpi	GLPI is a free asset and IT management software package. An unauthenticated user can provide a malicious link to a GLPI technician in order to exploit a reflected XSS vulnerability located in the Software form. Upgrade to 10.0.17.	2024-11-15	6.5	CVE-2024-43417

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
glpi-project--glpi	GLPI is a free asset and IT management software package. An unauthenticated user can provide a malicious link to a GLPI technician in order to exploit a reflected XSS vulnerability. Upgrade to 10.0.17.	2024-11-15	6.5	CVE-2024-43418
glpi-project--glpi	GLPI is a free asset and IT management software package. An authenticated user can perfom a SQL injection by changing its preferences. Upgrade to 10.0.17.	2024-11-15	6.5	CVE-2024-45608
glpi-project--glpi	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. An unauthenticated user can provide a malicious link to a GLPI technician in order to exploit a reflected XSS vulnerability located in the reports pages. Upgrade to 10.0.17.	2024-11-15	6.5	CVE-2024-45609
glpi-project--glpi	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. An unauthenticated user can provide a malicious link to a GLPI technician in order to exploit a reflected XSS vulnerability located in the Cable form. Upgrade to 10.0.17.	2024-11-15	6.5	CVE-2024-45610
glpi-project--glpi	GLPI is a free asset and IT management software package. Starting in 9.2.0 and prior to 11.0.0, it is possible to download a document from the API without appropriate rights. Upgrade to 10.0.16.	2024-11-15	5.3	CVE-2024-38370
glpi-project--glpi	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. An authenticated user can bypass the access control policy to create a private RSS feed attached to another user account and use a malicious payload to triggger a stored XSS. Upgrade to 10.0.17.	2024-11-15	5.7	CVE-2024-45611
Google--Android	In readEncryptedData of ConscryptEngine.java, there is a possible plaintext leak due to improperly used crypto. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-15	6.2	CVE-2017-13309
Google--Android	In validate of WifiConfigurationUtil.java , there is a possible persistent denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	6.2	CVE-2024-43083
Google--Android	In visitUris of multiple files, there is a possible information disclosure due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	6.2	CVE-2024-43084
Google--Android	In onActivityResult of EditUserPhotoController.java, there is a possible cross-user media read due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	5.5	CVE-2024-43082
Google--Android	In validateAccountsInternal of AccountManagerService.java, there is a possible way to leak account credentials to a third party app due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-11-13	5.5	CVE-2024-43086
Google--Android	In multiple locations, there is a possible cross-user image read due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation.	2024-11-13	5	CVE-2024-43090
Google--Chrome	Inappropriate implementation in Extensions in Google Chrome prior to 131.0.6778.69 allowed a remote attacker to bypass site isolation via a crafted Chrome Extension. (Chromium security severity: High)	2024-11-12	6.5	CVE-2024-11110
Google--Chrome	Inappropriate implementation in Autofill in Google Chrome prior to 131.0.6778.69 allowed a remote attacker who convinced a user to engage in specific UI gestures	2024-11-12	4.3	CVE-2024-11111

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)			
Google--Chrome	Inappropriate implementation in Blink in Google Chrome prior to 131.0.6778.69 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2024-11-12	4.3	CVE-2024-11116
Google--Chrome	Inappropriate implementation in FileSystem in Google Chrome prior to 131.0.6778.69 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page. (Chromium security severity: Low)	2024-11-12	4.3	CVE-2024-11117
goToMain--libosdp	libosdp is an implementation of IEC 60839-11-5 OSDP (Open Supervised Device Protocol) and provides a C library with support for C++, Rust and Python3. At ospd_common.c, on the osdp_reply_name function, any reply id between REPLY_ACK and REPLY_XRD is valid, but names array do not declare all of the range. On a case of an undefined reply id within the range, name will be null (name = names[reply_id - REPLY_ACK];). Null name will casue a crash on next line: if (name[0] == '\0') as null[0] is invalid. As this logic is not limited to a secure connection, attacker may trigger this vulnerability without any prior knowledge. This issue is fixed in 2.4.0.	2024-11-12	6.5	CVE-2024-52296
goToMain--libosdp	libosdp is an implementation of IEC 60839-11-5 OSDP (Open Supervised Device Protocol) and provides a C library with support for C++, Rust and Python3. In affected versions an unexpected `REPLY_CCRYPT` or `REPLY_RMAC_I` may be introduced into an active stream when they should not be. Once RMAC_I message can be sent during a session, attacker with MITM access to the communication may intercept the original RMAC_I reply and save it. While the session continues, the attacker will record all of the replies and save them, till capturing the message to be replied (can be detected by ID, length or time based on inspection of visual activity next to the reader) Once attacker captures a session with the message to be replayed, he stops resetting the connection and waits for signal to perform the replay to of the PD to CP message (ex: by signaling remotely to the MIMT device or setting a specific timing). In order to replay, the attacker will craft a specific RMAC_I message in the proper seq of the execution, which will result in reverting the RMAC to the beginning of the session. At that phase - attacker can replay all the messages from the beginning of the session. This issue has been addressed in commit `298576d9` which is included in release version 3.0.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-11-11	5.1	CVE-2024-52288
gpac--gpac/gpac	A use after free vulnerability exists in GPAC version 2.3-DEV-revrelease, specifically in the gf_filterpacket_del function in filter_core/filter.c at line 38. This vulnerability can lead to a double-free condition, which may cause the application to crash.	2024-11-15	5.9	CVE-2023-4679
Grand Vice info--Webopac	Webopac from Grand Vice info has Stored Cross-site Scripting vulnerability. Remote attackers with regular privileges can inject arbitrary JavaScript code into the server. When users visit the compromised page, the code is automatically executed in their browser.	2024-11-11	5.4	CVE-2024-11021
Grand Vice info--Webopac7	Webopac from Grand Vice info has a Reflected Cross-site Scripting vulnerability, allowing unauthenticated remote attackers to execute arbitrary JavaScript code in the user's browser through phishing techniques.	2024-11-11	6.1	CVE-2024-11019
hashthemes--Hash Elements	The Hash Elements plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the hash_elements_get_posts_title_by_id() function in all versions up to, and including, 1.4.7. This makes it possible for unauthenticated attackers to retrieve draft post titles that should not be accessible to unauthenticated users.	2024-11-13	5.3	CVE-2024-10802
HCL Software--HCL Traveler for Microsoft Outlook	HCL Traveler for Microsoft Outlook (HTMO) is susceptible to a control flow vulnerability. The application does not sufficiently manage its control flow during	2024-11-12	5.3	CVE-2024-30133

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
(HTMO)	execution, creating conditions in which the control flow can be modified in unexpected ways.			
hyumika -- openstreetmap	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Hyumika OSM - OpenStreetMap allows Stored XSS.This issue affects OSM - OpenStreetMap: from n/a through 6.1.2.	2024-11-11	5.4	CVE-2024-52355
ibm -- security_qradar_edr	IBM Security ReaQta 3.12 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2024-11-14	5.3	CVE-2024-45642
ibm -- security_qradar_edr	IBM Security ReaQta 3.12 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2024-11-14	4.8	CVE-2024-45099
IBM--Concert Software	IBM Concert Software 1.0.0 through 1.0.1 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2024-11-15	6.1	CVE-2024-41785
IBM--Concert Software	IBM Concert Software 1.0.0 through 1.0.1 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.	2024-11-15	5.9	CVE-2024-43189
IBM--Maximo Asset Management	IBM Maximo Asset Management 7.6.1.3 is vulnerable to stored cross-site scripting. This vulnerability allows authenticated users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2024-11-11	6.4	CVE-2024-45088
IBM--WebSphere Application Server	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2024-11-11	4.8	CVE-2024-45087
ivanti -- connect_secure	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.3 and Ivanti Policy Secure before version 22.7R1.2 allows a remote authenticated attacker with admin privileges to cause a denial of service.	2024-11-12	4.9	CVE-2024-47905
ivanti -- connect_secure	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.3 and Ivanti Policy Secure before version 22.7R1.2 allows a remote authenticated attacker with admin privileges to cause a denial of service.	2024-11-12	4.9	CVE-2024-47909
ivanti -- secure_access_client	A race condition in Ivanti Secure Access Client before version 22.7R4 allows a local authenticated attacker to modify sensitive configuration files.	2024-11-13	4.7	CVE-2024-29211
Ivanti--Secure Access Client	A buffer over-read in Ivanti Secure Access Client before 22.7R4 allows a local unauthenticated attacker to cause a denial of service.	2024-11-12	5	CVE-2024-9843
ivole--Customer Reviews for WooCommerce	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the cancel_import() function in all versions up to, and including, 5.61.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to cancel and import or check on the status.	2024-11-16	4.3	CVE-2024-10614
Jenkins Project--Jenkins Script	Jenkins Script Security Plugin 1367.vdf2fc45f229c and earlier, except 1365.1367.va_3b_b_89f8a_95b_ and 1362.1364.v4cf2dc5d8776, does not perform a permission check in a method implementing form validation, allowing attackers	2024-11-13	4.3	CVE-2024-52549

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Security Plugin	with Overall/Read permission to check for the existence of files on the controller file system.			
JetBrains--WebStorm	In JetBrains WebStorm before 2024.3 code execution in Untrusted Project mode was possible via type definitions installer script	2024-11-15	6.3	CVE-2024-52555
jetmonsters--JetWidgets For Elementor	The JetWidgets For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REST API SVG File uploads in all versions up to, and including, 1.0.18 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-11-12	6.4	CVE-2024-10323
Jinher Network--Collaborative Management Platform	A vulnerability classified as critical has been found in Jinher Network Collaborative Management Platform é□□å□Œæ□°å□å□Œæ™ºè□½åš□å..¬å¹³å□° 1.0. Affected is an unknown function of the file /C6/JHSoft.Web.AcceptAip/AcceptShow.aspx/. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-11	6.3	CVE-2024-11060
johndarrel--Hide My WP Ghost Security & Firewall	The Hide My WP Ghost - Security & Firewall plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the URL in all versions up to, and including, 5.3.01 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 an administrative user into performing an action such as clicking on a link.	2024-11-15	6.1	CVE-2024-10825
jorisderuiter--ConvertCalculator for WordPress	The ConvertCalculator for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' and 'type' parameters in all versions up to, and including, 1.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-16	6.4	CVE-2024-10015
kaminskym--AJAX Login and Registration modal popup + inline form	The AJAX Login and Registration modal popup + inline form 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, 2.24. 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.	2024-11-13	6.1	CVE-2024-8874
kasperta--Bounce Handler MailPoet 3	The Bounce Handler MailPoet 3 plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'page' parameter in all versions up to, and including, 1.3.21 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.	2024-11-16	6.1	CVE-2024-9938
kimberlynorris--Social Proof (Testimonial) Slider	The Social Proof (Testimonial) Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's spslider-block shortcode in all versions up to, and including, 2.2.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-13	6.4	CVE-2024-8985
kognetiks -- kognetiks_chatbot	The Kognetiks Chatbot for WordPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'dir' parameter in all versions up to, and including, 2.1.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-11-13	6.1	CVE-2024-10684

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kognetiks -- kognetiks_chatbot	The Kognetiks Chatbot for WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the delete_assistant() function in all versions up to, and including, 2.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete GTP assistants.	2024-11-13	5.3	CVE-2024-10529
kognetiks -- kognetiks_chatbot	The Kognetiks Chatbot for WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the add_new_assistant() function in all versions up to, and including, 2.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to create new GTP assistants.	2024-11-13	4.3	CVE-2024-10530
kognetiks -- kognetiks_chatbot	The Kognetiks Chatbot for WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the update_assistant() function in all versions up to, and including, 2.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to update GTP assistants.	2024-11-13	4.3	CVE-2024-10531
kognetiks -- kognetiks_chatbot	The Kognetiks Chatbot for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1.8. This is due to missing or incorrect nonce validation on the update_assistant, add_new_assistant, and delete_assistant functions. This makes it possible for unauthenticated attackers to modify assistants via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-11-13	4.3	CVE-2024-11143
Landray--EKP	A vulnerability, which was classified as critical, was found in Landray EKP up to 16.0. This affects the function delPreviewFile of the file /sys/ui/sys_ui_component/sysUiComponent.do?method=delPreviewFile. The manipulation of the argument directoryPath leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-15	6.5	CVE-2024-11238
Landray--EKP	A vulnerability has been found in Landray EKP up to 16.0 and classified as critical. This vulnerability affects the function deleteFile of the file /sys/common/import.do?method=deleteFile of the component API Interface. The manipulation of the argument folder leads to path traversal. 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.	2024-11-15	5.4	CVE-2024-11239
leevio -- happy_addons_for_elementor	The Happy Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the before_label parameter in the Image Comparison widget in all versions up to, and including, 3.12.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-12	5.4	CVE-2024-10538
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. User with Admin role can add Notes to a device, the application did not properly sanitize the user input, when the ExamplePlugin enable, if java script code is inside the device's Notes, its will be trigger. This vulnerability is fixed in 24.10.0.	2024-11-15	4.8	CVE-2024-49758
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Manage User Access" page allows authenticated users to inject arbitrary JavaScript through the "bill_name" parameter when creating a new bill. This vulnerability can lead to the execution of malicious code when visiting the "Bill Access" dropdown in the user's "Manage Access" page, potentially compromising user sessions and allowing unauthorized actions. This vulnerability is fixed in 24.10.0.	2024-11-15	4.8	CVE-2024-49759

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Capture Debug Information" page allows authenticated users to inject arbitrary JavaScript through the "hostname" parameter when creating a new device. This vulnerability results in the execution of malicious code when the "Capture Debug Information" page is visited, redirecting the user and sending non-httponly cookies to an attacker-controlled domain. This vulnerability is fixed in 24.10.0.	2024-11-15	4.8	CVE-2024-49764
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Port Settings" page allows authenticated users to inject arbitrary JavaScript through the "name" parameter when creating a new Port Group. This vulnerability results in the execution of malicious code when the "Port Settings" page is visited after the affected Port Group is added to a device, potentially compromising user sessions and allowing unauthorized actions. This vulnerability is fixed in 24.10.0.	2024-11-15	4.8	CVE-2024-50350
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Reflected Cross-Site Scripting (XSS) vulnerability in the "section" parameter of the "logs" tab of a device allows attackers to inject arbitrary JavaScript. This vulnerability results in the execution of malicious code when a user accesses the page with a malicious "section" parameter, potentially compromising their session and enabling unauthorized actions. The issue arises from a lack of sanitization in the "report_this()" function. This vulnerability is fixed in 24.10.0.	2024-11-15	4.8	CVE-2024-50351
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Services" section of the Device Overview page allows authenticated users to inject arbitrary JavaScript through the "name" parameter when adding a service to a device. This vulnerability could result in the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and enabling unauthorized actions. This vulnerability is fixed in 24.10.0.	2024-11-15	4.8	CVE-2024-50352
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. User with Admin role can edit the Display Name of a device, the application did not properly sanitize the user input in the device Display Name, if java script code is inside the name of the device Display Name, its can be trigger from different sources. This vulnerability is fixed in 24.10.0.	2024-11-15	4.8	CVE-2024-50355
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Port Settings" page allows authenticated users to inject arbitrary JavaScript through the "descr" parameter when editing a device's port settings. This vulnerability can lead to the execution of malicious code when the "Port Settings" page is visited, potentially compromising the user's session and allowing unauthorized actions. This vulnerability is fixed in 24.10.0.	2024-11-15	4.8	CVE-2024-51494
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the Device Overview page allows authenticated users to inject arbitrary JavaScript through the "overwrite_ip" parameter when editing a device. This vulnerability results in the execution of malicious code when the device overview page is visited, potentially compromising the accounts of other users. This vulnerability is fixed in 24.10.0.	2024-11-15	4.8	CVE-2024-51495
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Reflected Cross-Site Scripting (XSS) vulnerability in the "metric" parameter of the "/wireless" and "/health" endpoints allows attackers to inject arbitrary JavaScript. This vulnerability results in the execution of malicious code when a user accesses the page with a malicious "metric" parameter, potentially compromising their session and allowing unauthorized actions. This vulnerability is fixed in 24.10.0.	2024-11-15	4.8	CVE-2024-51496

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Custom OID" tab of a device allows authenticated users to inject arbitrary JavaScript through the "unit" parameter when creating a new OID. This vulnerability can lead to the execution of malicious code in the context of other users' sessions, compromising their accounts and enabling unauthorized actions. This vulnerability is fixed in 24.10.0.	2024-11-15	4.8	CVE-2024-51497
librenms--librenms	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Services" tab of the Device page allows authenticated users to inject arbitrary JavaScript through the "descr" parameter when adding a service to a device. This vulnerability could result in the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and enabling unauthorized actions. This vulnerability is fixed in 24.10.0.	2024-11-15	4.8	CVE-2024-52526
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: fork: only invoke khugepaged, ksm hooks if no error There is no reason to invoke these hooks early against an mm that is in an incomplete state. The change in commit d24062914837 ("fork: use __mt_dup() to duplicate maple tree in dup_mmap()") makes this more pertinent as we may be in a state where entries in the maple tree are not yet consistent. Their placement early in dup_mmap() only appears to have been meaningful for early error checking, and since functionally it'd require a very small allocation to fail (in practice 'too small to fail') that'd only occur in the most dire circumstances, meaning the fork would fail or be OOM'd in any case. Since both khugepaged and KSM tracking are there to provide optimisations to memory performance rather than critical functionality, it doesn't really matter all that much if, under such dire memory pressure, we fail to register an mm with these. As a result, we follow the example of commit d2081b2bf819 ("mm: khugepaged: make khugepaged_enter() void function") and make ksm_fork() a void function also. We only expose the mm to these functions once we are done with them and only if no error occurred in the fork operation.	2024-11-11	5.5	CVE-2024-50263
lqd -- liquid_blocks	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LIQUID DESIGN Ltd. LIQUID BLOCKS allows Stored XSS.This issue affects LIQUID BLOCKS: from n/a through 1.2.0.	2024-11-11	5.4	CVE-2024-52357
lsquared -- l_squared_hub	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in L Squared Support L Squared Hub WP allows SQL Injection.This issue affects L Squared Hub WP: from n/a through 1.0.	2024-11-11	6.5	CVE-2024-51820
mailmunch--Constant Contact Forms by MailMunch	The Constant Contact Forms by MailMunch 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, 2.1.2. 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.	2024-11-13	6.1	CVE-2024-9614
mapster--Mapster WP Maps	The Mapster WP Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the popup class parameter in all versions up to, and including, 1.6.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject	2024-11-16	6.4	CVE-2024-10592

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
MasterBip--MasterBip para Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MasterBip MasterBip para Elementor allows DOM-Based XSS.This issue affects MasterBip para Elementor: from n/a through 1.6.3.	2024-11-11	6.5	CVE-2024-51571
matrix-org--matrix-appservice-irc	matrix-appservice-irc is a Node.js IRC bridge for the Matrix messaging protocol. The provisioning API of the matrix-appservice-irc bridge up to version 3.0.2 contains a vulnerability which can lead to arbitrary IRC command execution as the bridge IRC bot. The vulnerability has been patched in matrix-appservice-irc version 3.0.3.	2024-11-14	5.4	CVE-2024-52505
Matthew Lillistone--ML Responsive Audio player with playlist Shortcode	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Matthew Lillistone ML Responsive Audio player with playlist Shortcode allows Stored XSS.This issue affects ML Responsive Audio player with playlist Shortcode: from n/a through 0.2.	2024-11-11	6.5	CVE-2024-51573
maxwellberkel--WP Log Viewer	The WP Log Viewer plugin for WordPress is vulnerable to unauthorized use of functionality due to a missing capability check on several AJAX actions in all versions up to, and including, 1.2.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to access logs, update plugin-related user settings and general plugin settings.	2024-11-16	5.4	CVE-2024-11085
mendix -- mendix	A vulnerability has been identified in Mendix Runtime V10 (All versions < V10.16.0 only if the basic authentication mechanism is used by the application), Mendix Runtime V10.12 (All versions < V10.12.7 only if the basic authentication mechanism is used by the application), Mendix Runtime V10.6 (All versions < V10.6.15 only if the basic authentication mechanism is used by the application), Mendix Runtime V8 (All versions), Mendix Runtime V9 (All versions < V9.24.29 only if the basic authentication mechanism is used by the application). The basic authentication implementation of affected applications contains a race condition vulnerability which could allow unauthenticated remote attackers to circumvent default account lockout measures.	2024-11-12	4.8	CVE-2024-50313
michelwppi--xili-tidy-tags	The xili-tidy-tags plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'action' parameter in all versions up to, and including, 1.12.04 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.	2024-11-12	6.1	CVE-2024-9357
microsoft -- visual_studio_2022	Visual Studio Elevation of Privilege Vulnerability	2024-11-12	6.7	CVE-2024-49044
microsoft -- windows_10_1507	NTLM Hash Disclosure Spoofing Vulnerability	2024-11-12	6.5	CVE-2024-43451
Microsoft--Microsoft Edge (Chromium-based)	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2024-11-14	5.4	CVE-2024-49025
Microsoft--Windows 10 Version 1809	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	2024-11-12	6.8	CVE-2024-43634

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1809	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	2024-11-12	6.8	CVE-2024-43638
Microsoft--Windows 10 Version 1809	Windows Defender Application Control (WDAC) Security Feature Bypass Vulnerability	2024-11-12	6.7	CVE-2024-43645
Microsoft--Windows 11 version 22H2	Windows Hyper-V Denial of Service Vulnerability	2024-11-12	6.5	CVE-2024-43633
Microsoft--Windows Server 2022	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	2024-11-12	6.7	CVE-2024-43631
Microsoft--Windows Server 2025	Windows Package Library Manager Information Disclosure Vulnerability	2024-11-12	6.2	CVE-2024-38203
Microsoft--Windows Server 2025	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	2024-11-12	6.8	CVE-2024-43449
Microsoft--Windows Server 2025	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	2024-11-12	6.8	CVE-2024-43643
Microsoft--Windows Server 2025	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	2024-11-12	6.7	CVE-2024-43646
Microsoft--Windows Server 2025	Microsoft Virtual Hard Disk (VHDX) Denial of Service Vulnerability	2024-11-12	5.9	CVE-2024-38264
miloco --postcasa_shortcode	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Andrew Milo Postcasa Shortcode allows DOM-Based XSS.This issue affects Postcasa Shortcode: from n/a through 1.0.	2024-11-11	5.4	CVE-2024-52352
MongoDB Inc--MongoDB Server	An authorized user may trigger crashes or receive the contents of buffer over-reads of Server memory by issuing specially crafted requests that construct malformed BSON in the MongoDB Server. This issue affects MongoDB Server v5.0 versions prior to 5.0.30 , MongoDB Server v6.0 versions prior to 6.0.19, MongoDB Server v7.0 versions prior to 7.0.15 and MongoDB Server v8.0 versions prior to and including 8.0.2.	2024-11-14	6.8	CVE-2024-10921
moodle--moodle	A flaw was found in moodle. Some hidden user profile fields are visible in gradebook reports, which could result in users without the "view hidden user fields" capability having access to the information.	2024-11-11	5.3	CVE-2024-43429

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
moodle--moodle	A flaw was found in moodle. External API access to Quiz can override contained insufficient access control.	2024-11-11	5.3	CVE-2024-43430
moodle--moodle	A flaw was found in moodle. The cURL wrapper in Moodle strips HTTPAUTH and USERPWD headers during emulated redirects, but retains other original request headers, so HTTP authorization header information could be unintentionally sent in requests to redirect URLs.	2024-11-11	5.3	CVE-2024-43432
moodle--moodle	A flaw was found in moodle. Matrix room membership and power levels are incorrectly applied and revoked for suspended Moodle users.	2024-11-11	5.3	CVE-2024-43433
moodle--moodle	A flaw was found in moodle. Insufficient capability checks make it possible for users with access to restore glossaries in courses to restore them into the global site glossary.	2024-11-11	5.3	CVE-2024-43435
moodle--moodle	A flaw was found in moodle. H5P error messages require additional sanitizing to prevent a reflected cross-site scripting (XSS) risk.	2024-11-11	5.4	CVE-2024-43439
mutt -- mutt	In neomutt and mutt, the To and Cc email headers are not validated by cryptographic signing which allows an attacker that intercepts a message to change their value and include himself as a one of the recipients to compromise message confidentiality.	2024-11-12	5.9	CVE-2024-49393
mutt -- mutt	In mutt and neomutt the In-Reply-To email header field is not protected by cryptographic signing which allows an attacker to reuse an unencrypted but signed email message to impersonate the original sender.	2024-11-12	5.3	CVE-2024-49394
mutt -- mutt	In mutt and neomutt, PGP encryption does not use the --hidden-recipient mode which may leak the Bcc email header field by inferring from the recipients info.	2024-11-12	5.3	CVE-2024-49395
n/a--4th and 5th Generation Intel(R) Xeon(R) Processors	Improper finite state machines (FSMs) in the hardware logic in some 4th and 5th Generation Intel(R) Xeon(R) Processors may allow an authorized user to potentially enable denial of service via local access.	2024-11-13	4.7	CVE-2024-21853
n/a--ACAT software maintained by Intel(R) for Windows	Uncontrolled search path for some ACAT software maintained by Intel(R) for Windows before version 3.11.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-37024
n/a--BigDL software maintained by Intel(R)	Cleartext transmission of sensitive information for some BigDL software maintained by Intel(R) before version 2.5.0 may allow an authenticated user to potentially enable denial of service via adjacent access.	2024-11-13	5.4	CVE-2024-28169
n/a--BigDL software maintained by Intel(R)	Improper access control for some BigDL software maintained by Intel(R) before version 2.5.0 may allow an authenticated user to potentially enable escalation of privilege via adjacent access.	2024-11-13	5.5	CVE-2024-29085
n/a--EyouCMS	A vulnerability was found in EyouCMS 1.51. It has been rated as critical. This issue affects the function editFile of the file application/admin/logic/FilemanagerLogic.php. The manipulation of the argument activepath leads to path traversal. 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.	2024-11-14	5.4	CVE-2024-11210

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--EyouCMS	A vulnerability classified as critical has been found in EyouCMS up to 1.6.7. Affected is an unknown function of the component Website Logo Handler. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-14	4.7	CVE-2024-11211
n/a--Harbor	Harbor fails to validate the user permissions when updating a robot account thatÂ belongs to a project that the authenticated user doesn't have access to.Â By sending a request that attempts to update a robot account, and specifying a robotÂ account id and robot account name that belongs to a different project that the userÂ doesn't have access to, it was possible to revoke the robot account permissions.	2024-11-14	6.4	CVE-2022-31667
n/a--Harbor	Harbor fails to validate the user permissions when updating tag immutability policies.Â By sending a request to update a tag immutability policy with an id that belongs to a project that the currently authenticated user doesn't have access to, the attacker could modify tag immutability policies configured in other projects.	2024-11-14	6.4	CVE-2022-31669
n/a--Intel(R) Advanced Link Analyzer Standard Edition software installer	Incorrect execution-assigned permissions in some Intel(R) Advanced Link Analyzer Standard Edition software installer before version 23.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-37025
n/a--Intel(R) Arc(TM) Pro Graphics for Windows drivers	Improper access control for some Intel(R) Arc(TM) Pro Graphics for Windows drivers before version 31.0.101.5319 may allow an authenticated user to potentially enable escalation of privilege via adjacent access.	2024-11-13	6.8	CVE-2024-32044
n/a--Intel(R) Binary Configuration Tool software for Windows	Uncontrolled search path for some Intel(R) Binary Configuration Tool software for Windows before version 3.4.5 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-23312
n/a--Intel(R) Binary Configuration Tool software for Windows	Incorrect default permissions for some Intel(R) Binary Configuration Tool software for Windows before version 3.4.5 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-25647
n/a--Intel(R) CIP software	Insecure inherited permissions for some Intel(R) CIP software before version 2.4.10852 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-36276
n/a--Intel(R) CST software	Uncaught exception for some Intel(R) CST software before version 8.7.10803 may allow an authenticated user to potentially enable denial of service via local access.	2024-11-13	5.5	CVE-2024-29076
n/a--Intel(R) Distribution for Python software	Incorrect default permissions in some Intel(R) Distribution for Python software before version 2024.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-29083

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--Intel(R) Distribution of OpenVINO(TM) Model Server software	Improper input validation in the Intel(R) Distribution of OpenVINO(TM) Model Server software before version 2024.0 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2024-11-13	6.5	CVE-2024-32048
n/a--Intel(R) DSA software	Insecure inherited permissions for some Intel(R) DSA software before version 24.3.26.8 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-36294
n/a--Intel(R) Fortran Compiler Classic software	Uncontrolled search path for some Intel(R) Fortran Compiler Classic software before version 2021.13 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-28881
n/a--Intel(R) Granulate(TM) software	Improper access control in some Intel(R) Granulate(TM) software before version 4.30.1 may allow a authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	4.4	CVE-2024-27200
n/a--Intel(R) Graphics Driver installers	Uncontrolled search path in the Intel(R) Graphics Driver installers for versions 15.40 and 15.45 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-38387
n/a--Intel(R) Graphics Drivers	Improper buffer restrictions in some Intel(R) Graphics Drivers may allow an authenticated user to potentially enable denial of service via local access.	2024-11-13	6.6	CVE-2024-34170
n/a--Intel(R) Graphics Offline Compiler for OpenCL(TM) Code software for Windows	Uncontrolled search path in some Intel(R) Graphics Offline Compiler for OpenCL(TM) Code software for Windows before version 2024.1.0.142, graphics driver 31.0.101.5445 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-34028
n/a--Intel(R) Graphics software	Improper buffer restrictions in some Intel(R) Graphics software may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	5.3	CVE-2024-23919
n/a--Intel(R) High Level Synthesis Compiler software for Intel(R) Quartus(R) Prime Pro Edition Software	Uncontrolled search path in some Intel(R) High Level Synthesis Compiler software for Intel(R) Quartus(R) Prime Pro Edition Software before version 24.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-31407
n/a--Intel(R) IPP software for Windows	Uncontrolled search path for some Intel(R) IPP software for Windows before version 2021.12.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-28952
n/a--Intel(R) MAS software	Uncontrolled search path element in some Intel(R) MAS software before version 2.5 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-34164

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--Intel(R) Neural Compressor software	Improper input validation in some Intel(R) Neural Compressor software before version v3.0 may allow an authenticated user to potentially enable escalation of privilege via adjacent access.	2024-11-13	5.5	CVE-2024-36284
n/a--Intel(R) oneAPI DPC++/C++ Compiler	Uncontrolled search path in some Intel(R) oneAPI DPC++/C++ Compiler before version 2024.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-34165
n/a--Intel(R) oneAPI Math Kernel Library software for Windows	Uncontrolled search path for some Intel(R) oneAPI Math Kernel Library software for Windows before version 2024.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-28950
n/a--Intel(R) Optane(TM) PMem Management software versions	NULL pointer dereference in some Intel(R) Optane(TM) PMem Management software versions before CR_MGMT_02.00.00.4040, CR_MGMT_03.00.00.0499 may allow a authenticated user to potentially enable denial of service via local access.	2024-11-13	6.1	CVE-2024-36275
n/a--Intel(R) PROSet/Wireless Software and Intel(R) Killer(TM) Wi-Fi products	Improper input validation in firmware for some Intel(R) PROSet/Wireless Software and Intel(R) Killer(TM) Wi-Fi products before version 23.40 may allow an unauthenticated user to enable denial of service via adjacent access.	2024-11-13	6.6	CVE-2024-23198
n/a--Intel(R) PROSet/Wireless Software and Intel(R) Killer(TM) Wi-Fi wireless products	Improper input validation in firmware for some Intel(R) PROSet/Wireless Software and Intel(R) Killer(TM) Wi-Fi wireless products before version 23.40 may allow an unauthenticated user to enable denial of service via adjacent access.	2024-11-13	5.7	CVE-2024-28049
n/a--Intel(R) PROSet/Wireless WiFi software for Windows	Uncontrolled search path element in some Intel(R) PROSet/Wireless WiFi software for Windows before version 23.60 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-35245
n/a--Intel(R) PROSet/Wireless WiFi software for Windows	Improper input validation for some Intel(R) PROSet/Wireless WiFi software for Windows before version 23.60 may allow an unauthenticated user to potentially enable denial of service via network access.	2024-11-13	4.3	CVE-2024-33624
n/a--Intel(R) QAT Engine for OpenSSL software	Observable discrepancy in some Intel(R) QAT Engine for OpenSSL software before version v1.6.1 may allow information disclosure via network access.	2024-11-13	5.9	CVE-2024-28885
n/a--Intel(R) QAT Engine for OpenSSL software	Observable timing discrepancy in some Intel(R) QAT Engine for OpenSSL software before version v1.6.1 may allow information disclosure via network access.	2024-11-13	5.9	CVE-2024-31074

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--Intel(R) QAT Engine for OpenSSL software	Insufficient control flow management in some Intel(R) QAT Engine for OpenSSL software before version v1.6.1 may allow information disclosure via network access.	2024-11-13	5.9	CVE-2024-33617
n/a--Intel(R) Quartus(R) Prime Pro Edition software for Windows	Uncontrolled search path for some Intel(R) Quartus(R) Prime Pro Edition software for Windows before version 24.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-38383
n/a--Intel(R) Quartus(R) Prime Standard Edition software for Windows	Uncontrolled search path for some Intel(R) Quartus(R) Prime Standard Edition software for Windows before version 23.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-38668
n/a--Intel(R) Rendering Toolkit software	Uncontrolled search path in some Intel(R) Rendering Toolkit software before version 2024.1.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-26017
n/a--Intel(R) SDP Tool for Windows software	Incorrect default permissions in the Intel(R) SDP Tool for Windows software all versions may allow an authenticated user to enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-35201
n/a--Intel(R) SDP Tool for Windows software	Uncontrolled search path in the Intel(R) SDP Tool for Windows software all version may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-36253
n/a--Intel(R) Server Board S2600ST Family BIOS and Firmware Update software	Uncontrolled search path for the Intel(R) Server Board S2600ST Family BIOS and Firmware Update software all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-34167
n/a--Intel(R) Server M20NTP BIOS	Use after free in the UEFI firmware of some Intel(R) Server M20NTP BIOS may allow a privileged user to potentially enable escalation of privilege via local access.	2024-11-13	6.4	CVE-2024-40885
n/a--Intel(R) Server M20NTP Family UEFI	Improper input validation in firmware for some Intel(R) Server M20NTP Family UEFI may allow a privileged user to potentially enable escalation of privilege via local access.	2024-11-13	6.3	CVE-2024-39811
n/a--Intel(R) Server M20NTP Family	Improper access control in UEFI firmware in some Intel(R) Server M20NTP Family may allow a privileged user to potentially enable information disclosure via local access.	2024-11-13	5.3	CVE-2024-39285
n/a--Intel(R) SGX SDK software	Out-of-bounds write in some Intel(R) SGX SDK software may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	4.5	CVE-2024-34776
n/a--Intel(R) TDX Seamldr module software	Sensitive information in resource not removed before reuse in some Intel(R) TDX Seamldr module software before version 1.5.02.00 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-11-13	6	CVE-2024-21850

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--Intel(R) VPL software	Integer overflow for some Intel(R) VPL software before version 24.1.4 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	4.8	CVE-2024-21783
n/a--Intel(R) VPL software	Improper buffer restrictions in some Intel(R) VPL software before version 24.1.4 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	4.2	CVE-2024-21808
n/a--Intel(R) VROC software	Insufficient control flow management in some Intel(R) VROC software before version 8.6.0.3001 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.8	CVE-2024-29079
n/a--Intel(R) VTune(TM) Profiler software	Uncontrolled search path element in some Intel(R) VTune(TM) Profiler software before version 2024.2.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-36245
n/a--Intel(R) VTune(TM) Profiler software	Improper Input validation in some Intel(R) VTune(TM) Profiler software before version 2024.2.0 may allow an authenticated user to potentially enable denial of service via local access.	2024-11-13	6.1	CVE-2024-37027
n/a--Intel(R) Wireless Bluetooth(R) products for Windows	Improper input validation for some Intel(R) Wireless Bluetooth(R) products for Windows before version 23.40 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2024-11-13	6.5	CVE-2024-24984
n/a--JAM STAPL Player software	Improper access control in some JAM STAPL Player software before version 2.6.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-29077
n/a--n/a	Cross Site Scripting vulnerability in DLink DWR 2000M 5G CPE With Wifi 6 Ax1800 and Dlink DWR 5G CPE DWR-2000M_1.34ME allows a local attacker to obtain sensitive information via a crafted payload to the WiFi SSID Name field.	2024-11-12	6.6	CVE-2024-28728
n/a--n/a	A heap-based buffer overflow was found in the SDHCI device emulation of QEMU. The bug is triggered when both `s->data_count` and the size of `s->fifo_buffer` are set to 0x200, leading to an out-of-bound access. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition.	2024-11-14	6	CVE-2024-3447
n/a--n/a	A stack-based buffer over-read in tsMuxer version nightly-2024-03-14-01-51-12 allows attackers to cause Information Disclosure via a crafted TS video file.	2024-11-14	6.5	CVE-2024-41206
n/a--n/a	A heap-based buffer overflow in tsMuxer version nightly-2024-05-10-02-00-45 allows attackers to cause Denial of Service (DoS) via a crafted MKV video file.	2024-11-14	6.5	CVE-2024-41217
n/a--n/a	A negative-size-param in tsMuxer version nightly-2024-04-05-01-53-02 allows attackers to cause Denial of Service (DoS) via a crafted TS video file.	2024-11-14	6.5	CVE-2024-49776
n/a--n/a	Persistent and reflected XSS vulnerabilities in the themeMode cookie and _h URL parameter of Axigen Mail Server up to version 10.5.28 allow attackers to execute arbitrary Javascript. Exploitation could lead to session hijacking, data leakage, and further exploitation via a multi-stage attack. Fixed in versions 10.3.3.67, 10.4.42, and 10.5.29.	2024-11-11	6.1	CVE-2024-50601
n/a--n/a	A Reflected Cross Site Scriptng (XSS) vulnerability was found in /omrs/user/search.php in PHPGurukul Online Marriage Registration System v1.0, which allows remote attackers to execute arbitrary code via the "searchdata" POST request parameter.	2024-11-11	6.1	CVE-2024-50990

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	Cross Site Scripting vulnerability in Online Shop Store v.1.0 allows a remote attacker to execute arbitrary code via the login.php component.	2024-11-11	6.1	CVE-2024-51213
n/a--n/a	Sercomm Model Etisalat Model S3- AC2100 is affected by Cross Site Scripting (XSS) via the firmware update page.	2024-11-12	5.4	CVE-2021-27703
n/a--n/a	A use-after-free vulnerability was found in the cyttsp4_core driver in the Linux kernel. This issue occurs in the device cleanup routine due to a possible rearming of the watchdog_timer from the workqueue. This could allow a local user to crash the system, causing a denial of service.	2024-11-14	5.5	CVE-2023-4134
n/a--n/a	A buffer overflow in the ngap_amf_handle_pdu_session_resource_setup_response function of oai-cn5g-amf up to v2.0.0 allows attackers to cause a Denial of Service (DoS) via a PDU Session Resource Setup Response with an empty Response Item list.	2024-11-15	5.3	CVE-2024-24447
n/a--n/a	Stack-based memcpy buffer overflow in the ngap_handle_pdu_session_resource_setup_response routine in OpenAirInterface CN5G AMF <= 2.0.0 allows a remote attacker with access to the N2 interface to carry out denial of service against the AMF and potentially execute code by sending a PDU Session Resource Setup Response with a suffciently large FailedToSetupList IE.	2024-11-15	5.3	CVE-2024-24450
n/a--n/a	Cross Site Scripting vulnerability in Virtuozzo Hybrid Server for WHMCS Open Source v.1.7.1 allows a remote attacker to obtain sensitive information via modification of the hostname parameter.	2024-11-14	5.4	CVE-2024-40579
n/a--n/a	A flaw was found in moodle. Insufficient sanitizing of data when performing a restore could result in a cross-site scripting (XSS) risk from malicious backup files.	2024-11-11	5.4	CVE-2024-43437
n/a--n/a	The DS allvideo.downloader.browser (aka Fast Video Downloader: Browser) application through 1.6-RC1 for Android allows an attacker to execute arbitrary JavaScript code via the allvideo.downloader.browser.DefaultBrowserActivity component.	2024-11-11	5.4	CVE-2024-46965
n/a--n/a	Cross Site Scripting vulnerability in M2000 Smart4Web before v.5.020241004 allows a remote attacker to execute arbitrary code via the error parameter in URL	2024-11-15	5.4	CVE-2024-50800
n/a--n/a	A Stored Cross-Site Scripting (XSS) vulnerability was found in /admin/admin_user.php in KASHIPARA E-learning Management System Project 1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the firstname and username parameters.	2024-11-14	5.4	CVE-2024-50837
n/a--n/a	A Stored Cross-Site Scripting (XSS) vulnerability was found in /admin/department.php in KASHIPARA E-learning Management System Project 1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the d and pi parameters.	2024-11-14	5.4	CVE-2024-50838
n/a--n/a	A Stored Cross-Site Scripting (XSS) vulnerability was found in /admin/add_subject.php in KASHIPARA E-learning Management System Project 1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the subject_code and title parameters.	2024-11-14	5.4	CVE-2024-50839
n/a--n/a	A Stored Cross-Site Scripting (XSS) vulnerability was found in /admin/class.php in KASHIPARA E-learning Management System Project 1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the class_name parameter.	2024-11-14	5.4	CVE-2024-50840
n/a--n/a	A Stored Cross-Site Scripting (XSS) vulnerability was found in /admin/calendar_of_events.php in KASHIPARA E-learning Management System Project 1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the date_start, date_end, and title parameters.	2024-11-14	5.4	CVE-2024-50841

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	A Stored Cross-Site Scripting (XSS) vulnerability was found in /admin/school_year.php in KASHIPARA E-learning Management System Project 1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the school_year parameter.	2024-11-14	5.4	CVE-2024-50842
n/a--n/a	A Directory listing issue was found in PHPGurukul User Registration & Login and User Management System 3.2, which allows remote attackers attacker to access sensitive files and directories via /loginsystem/assets.	2024-11-14	5.3	CVE-2024-50843
n/a--n/a	The NetAdmin IAM system (version 4.0.30319) has a Cross Site Scripting (XSS) vulnerability in the /BalloonSave.ashx endpoint, where it is possible to inject a malicious payload into the Content= field.	2024-11-11	5.4	CVE-2024-51026
n/a--n/a	Cross Site Scripting vulnerability in Chamilo LMS v.1.11.26 allows an attacker to execute arbitrary code via the svkey parameter of the storageapi.php file.	2024-11-15	5.4	CVE-2024-51142
n/a--n/a	A flaw was found within the parsing of extended attributes in the kernel ksmbd module. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this to disclose sensitive information on affected installations of Linux. Only systems with ksmbd enabled are vulnerable to this CVE.	2024-11-14	4	CVE-2023-4458
n/a--n/a	The web interface in RSA NetWitness 11.7.2.0 allows Cross-Site Scripting (XSS) via the Where textbox on the Reports screen during new rule creation.	2024-11-15	4.6	CVE-2024-23169
n/a--n/a	A Cross Site Scripting (XSS) vulnerability was found in /ums-sp/admin/registered-users.php in PHPGurukul User Management System v1.0, which allows remote attackers to execute arbitrary code via the "fname" POST request parameter	2024-11-11	4.8	CVE-2024-50991
n/a--n/a	A Cross Site Scriptng (XSS) vulnerability was found in /omrs/admin/search.php in PHPGurukul Online Marriage Registration System 1.0, which allows remote attackers to execute arbitrary code via the "searchdata" POST request parameter.	2024-11-11	4.8	CVE-2024-51054
n/a--n/a	TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices contain a Store Cross-site scripting (XSS) vulnerability via the firewallRule_Name_1.1.1.0.0 parameter on the /firewall_setting.htm page.	2024-11-11	4.8	CVE-2024-51187
n/a--n/a	TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices contain a Store Cross-site scripting (XSS) vulnerability via the vsRule_VirtualServerName_1.1.10.0.0 parameter on the /virtual_server.htm page.	2024-11-11	4.8	CVE-2024-51188
n/a--n/a	TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices contain a Store Cross-site scripting (XSS) vulnerability via the macList_Name_1.1.1.0.0 parameter on the /filters.htm page.	2024-11-11	4.8	CVE-2024-51189
n/a--n/a	TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices contain a Store Cross-site scripting (XSS) vulnerability via the ptRule_ApplicationName_1.1.6.0.0 parameter on the /special_ap.htm page.	2024-11-11	4.8	CVE-2024-51190
n/a--PostgreSQL	Incomplete tracking in PostgreSQL of tables with row security allows a reused query to view or change different rows from those intended. CVE-2023-2455 and CVE-2016-2193 fixed most interaction between row security and user ID changes. They missed cases where a subquery, WITH query, security invoker view, or SQL-language function references a table with a row-level security policy. This has the same consequences as the two earlier CVEs. That is to say, it leads to potentially incorrect policies being applied in cases where role-specific policies are used and a given query is planned under one role and then executed under other roles. This scenario can happen under security definer functions or when a common user and query is planned initially and then re-used across multiple SET ROLEs. Applying an incorrect policy may permit a user to complete otherwise-forbidden reads and modifications. This affects only databases that have used CREATE POLICY to define a row security policy. An attacker must tailor an attack to a particular application's pattern of query plan reuse, user ID changes, and role-specific row security	2024-11-14	4.2	CVE-2024-10976

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	policies. Versions before PostgreSQL 17.1, 16.5, 15.9, 14.14, 13.17, and 12.21 are affected.			
n/a--PostgreSQL	Incorrect privilege assignment in PostgreSQL allows a less-privileged application user to view or change different rows from those intended. An attack requires the application to use SET ROLE, SET SESSION AUTHORIZATION, or an equivalent feature. The problem arises when an application query uses parameters from the attacker or conveys query results to the attacker. If that query reacts to current_setting('role') or the current user ID, it may modify or return data as though the session had not used SET ROLE or SET SESSION AUTHORIZATION. The attacker does not control which incorrect user ID applies. Query text from less-privileged sources is not a concern here, because SET ROLE and SET SESSION AUTHORIZATION are not sandboxes for unvetted queries. Versions before PostgreSQL 17.1, 16.5, 15.9, 14.14, 13.17, and 12.21 are affected.	2024-11-14	4.2	CVE-2024-10978
n/a--Thunderbolt(TM) Share software	Improper Access Control in some Thunderbolt(TM) Share software before version 1.0.49.9 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	6.7	CVE-2024-34022
n/a--ZZCMS	A vulnerability was found in ZZCMS 2023. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/ad_list.php?action=pass of the component Keyword Filtering. The manipulation of the argument keyword leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-15	4.7	CVE-2024-11242
nasirahmed--AFI The Easiest Integration Plugin	The AFI - The Easiest Integration Plugin 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, 1.92.0. 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.	2024-11-13	6.1	CVE-2024-10877
NetSclaer--NetScaler ADC	Memory safety vulnerability leading to memory corruption and Denial of ServiceÂ in NetScaler ADC and Gateway if the appliance must be configured as a Gateway (VPN Vserver) with RDP Feature enabledÂ OR the appliance must be configured as a Gateway (VPN Vserver) and RDP Proxy Server Profile is created and set to Gateway (VPN Vserver)Â OR the appliance must be configured as a Auth Server (AAA Vserver) with RDP Feature enabled	2024-11-12	5.3	CVE-2024-8534
netty--netty	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. An unsafe reading of environment file could potentially cause a denial of service in Netty. When loaded on an Windows application, Netty attempts to load a file that does not exist. If an attacker creates such a large file, the Netty application crashes. This vulnerability is fixed in 4.1.115.	2024-11-12	5.5	CVE-2024-47535
nextcloud--security-advisories	Nextcloud Tables allows users to to create tables with individual columns. By directly specifying the ID of a table or view, a malicious user could blindly insert new rows into tables they have no access to. It is recommended that the Nextcloud Tables is upgraded to 0.8.0.	2024-11-15	6.3	CVE-2024-52511
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. After an admin enables the default-disabled SVG preview provider, a malicious user could upload a manipulated SVG file referencing paths. If the file would exist the preview of the SVG would preview the other file instead. It is recommended that the Nextcloud Server is upgraded to 27.1.10, 28.0.6 or 29.0.1 and Nextcloud Enterprise Server is upgraded to 24.0.12.15, 25.0.13.10, 26.0.13.4, 27.1.10, 28.0.6 or 29.0.1.	2024-11-15	5.7	CVE-2024-52515

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. Due to a pre-flighted HEAD request, the link reference provider could be tricked into downloading bigger websites than intended, to find open-graph data. It is recommended that the Nextcloud Server is upgraded to 28.0.10 or 29.0.7 and Nextcloud Enterprise Server is upgraded to 27.1.11.8, 28.0.10 or 29.0.7.	2024-11-15	5.7	CVE-2024-52520
nextcloud--security-advisories	The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server with your computer. The Desktop client did not stop with an error but allowed by-passing the signature validation, if a manipulated server sends an empty initial signature. It is recommended that the Nextcloud Desktop client is upgraded to 3.14.2 or later.	2024-11-15	4.2	CVE-2024-52510
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. After a user received a share with some files inside being blocked by the files access control, the user would still be able to copy the intermediate folder inside Nextcloud allowing them to afterwards potentially access the blocked files depending on the user access control rules. It is recommended that the Nextcloud Server is upgraded to 27.1.9, 28.0.5 or 29.0.0 and Nextcloud Enterprise Server is upgraded to 21.0.9.18, 22.2.10.23, 23.0.12.18, 24.0.12.14, 25.0.13.9, 26.0.13.3, 27.1.9, 28.0.5 or 29.0.0.	2024-11-15	4.1	CVE-2024-52514
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. After storing "Global credentials" on the server, the API returns them and adds them into the frontend again, allowing to read them in plain text when an attacker already has access to an active session of a user. It is recommended that the Nextcloud Server is upgraded to 28.0.11, 29.0.8 or 30.0.1 and Nextcloud Enterprise Server is upgraded to 25.0.13.13, 26.0.13.9, 27.1.11.9, 28.0.11, 29.0.8 or 30.0.1.	2024-11-15	4.6	CVE-2024-52517
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. After an attacker got access to the session of a user or administrator, the attacker would be able to create, change or delete external storages without having to confirm the password. It is recommended that the Nextcloud Server is upgraded to 28.0.12, 29.0.9 or 30.0.2.	2024-11-15	4.4	CVE-2024-52518
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. After setting up a user or administrator defined external storage with fixed credentials, the API returns them and adds them into the frontend again, allowing to read them in plain text when an attacker already has access to an active session of a user. It is recommended that the Nextcloud Server is upgraded to 28.0.12, 29.0.9 or 30.0.2 and Nextcloud Enterprise Server is upgraded to 25.0.13.14, 26.0.13.10, 27.1.11.10, 28.0.12, 29.0.9 or 30.0.2.	2024-11-15	4.6	CVE-2024-52523
nicejob--NiceJob	The NiceJob plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of the plugin's shortcodes (nicejob-lead, nicejob-review, nicejob-engage, nicejob-badge, nicejob-stories) in all versions up to, and including, 3.6.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-13	6.4	CVE-2024-10887
ninjateam--WP Chat App	The WP Chat App plugin for WordPress is vulnerable to unauthorized plugin installation due to a missing capability check on the ajax_install_plugin() function in all versions up to, and including, 3.6.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install the filebird plugin.	2024-11-16	4.3	CVE-2024-10533
northmule--Buy one click WooCommerce	The Buy one click WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the buy_one_click_export_options AJAX action in all versions up to, and including, 2.2.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to export plugin settings.	2024-11-13	4.3	CVE-2024-10852
northmule--Buy one click	The Buy one click WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the	2024-11-13	4.3	CVE-2024-10853

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WooCommerce	removeorder AJAX action in all versions up to, and including, 2.2.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete Buy one click WooCommerce orders.			
northmule--Buy one click WooCommerce	The Buy one click WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the buy_one_click_import_options AJAX action in all versions up to, and including, 2.2.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to import plugin settings.	2024-11-13	4.3	CVE-2024-10854
olland -- horsemanager	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Olland.Biz Horsemanager allows Blind SQL Injection.This issue affects Horsemanager: from n/a through 1.3.	2024-11-11	6.5	CVE-2024-51843
opensuse -- mirrorcache	A Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in openSUSE Tumbleweed MirrorCache allows the execution of arbitrary JS via reflected XSS in theÂ REGEX and P parameters. This issue affects MirrorCache before 1.083.	2024-11-13	6.1	CVE-2024-49505
OpenText--ALM Octane Management	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in OpenTextâ„¢ ALM Octane Management allows Stored XSS.Â The vulnerability could result in a remote code execution attack. This issue affects ALM Octane Management: from 16.2.100 through 24.4.	2024-11-12	5.9	CVE-2024-10923
orchidsoftware--platform	Orchid is a @laravel package that allows for rapid application development of back-office applications, admin/user panels, and dashboards. This vulnerability is a method exposure issue (CWE-749: Exposed Dangerous Method or Function) in the Orchid Platform's asynchronous modal functionality, affecting users of Orchid Platform version 8 through 14.42.x. Attackers could exploit this vulnerability to call arbitrary methods within the `Screen` class, leading to potential brute force of database tables, validation checks against user credentials, and disclosure of the server's real IP address. The issue has been patched in the latest release, version 14.43.0, released on November 6, 2024. Users should upgrade to version 14.43.0 or later to address this vulnerability. If upgrading to version 14.43.0 is not immediately possible, users can mitigate the vulnerability by implementing middleware to intercept and validate requests to asynchronous modal endpoints, allowing only approved methods and parameters.	2024-11-11	4.1	CVE-2024-51992
peprodev--PeproDev WooCommerce Receipt Uploader	The PeproDev WooCommerce Receipt Uploader 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, 2.6.9. 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.	2024-11-16	6.1	CVE-2024-8873
Peter Shaw--LH QR Codes	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Peter Shaw LH QR Codes allows Stored XSS.This issue affects LH QR Codes: from n/a through 1.06.	2024-11-11	6.5	CVE-2024-51572
petrichorpost--SVGPlus	The SVGPlus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REST API SVG File uploads 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 Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-11-16	6.4	CVE-2024-11092
phpipam--phpipam/phpipam	phpIPAM version 1.5.1 contains a vulnerability where an attacker can bypass the IP block mechanism to brute force passwords for users by using the 'X-Forwarded-For' header. The issue lies in the 'get_user_ip()' function in 'class.Common.php' at lines 1044 and 1045, where the presence of the 'X-Forwarded-For' header is checked and used instead of 'REMOTE_ADDR'. This vulnerability allows attackers to	2024-11-15	5.3	CVE-2024-0787

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	perform brute force attacks on user accounts, including the admin account. The issue is fixed in version 1.7.0.			
Progress Software Corporation--WS_FTP Server	In WS_FTP Server versions before 8.8.9 (2022.0.9), an Incorrect Implementation of Authentication Algorithm in the Web Transfer Module allows users to skip the second-factor verification and log in with username and password only.	2024-11-12	6.5	CVE-2024-9999
Progress Software--Telerik Document Processing Libraries	In Progress Telerik Document Processing Libraries, versions prior to 2024 Q4 (2024.4.1106), importing a document with unsupported features can lead to excessive processing, leading to excessive use of computing resources leaving the application process unavailable.	2024-11-13	6.5	CVE-2024-8049
Project Worlds--Free Download Online Shopping System	A vulnerability was found in Project Worlds Free Download Online Shopping System up to 192.168.1.88. It has been rated as critical. This issue affects some unknown processing of the file /online-shopping-webvsite-in-php-master/success.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-11	6.3	CVE-2024-11059
publiccms -- publiccms	A vulnerability was found in Public CMS 5.202406.d and classified as problematic. This issue affects some unknown processing of the file /admin/cmsVote/save of the component Voting Management. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The patch is named b9530b9cc1f5cfdad4b637874f59029a6283a65c. It is recommended to apply a patch to fix this issue.	2024-11-13	4.8	CVE-2024-11175
pyload--pyload/pyload	An open redirection vulnerability exists in pyload/pyload version 0.5.0. The vulnerability is due to improper handling of the 'next' parameter in the login functionality. An attacker can exploit this vulnerability to redirect users to malicious sites, which can be used for phishing or other malicious activities. The issue is fixed in pyload-ng 0.5.0b3.dev79.	2024-11-15	4.6	CVE-2024-1240
qriouslad--Admin and Site Enhancements (ASE)	The Admin and Site Enhancements (ASE) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 7.5.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with custom-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. This feature must be enabled, and for specific roles in order to be exploitable.	2024-11-12	5.4	CVE-2024-10790
razormist -- student_record_management_system	A vulnerability has been found in SourceCodester Student Record Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the component Main Menu. The manipulation leads to infinite loop. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used.	2024-11-12	5.5	CVE-2024-11097
razorpay--Razorpay Payment Button Elementor Plugin	The Razorpay Payment Button Elementor Plugin 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, 1.2.5. 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.	2024-11-13	6.1	CVE-2024-10850
razorpay--Razorpay Payment Button Plugin	The Razorpay Payment Button Plugin 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, 2.4.6. 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.	2024-11-13	6.1	CVE-2024-10851

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rclone--rclone	Rclone is a command-line program to sync files and directories to and from different cloud storage providers. Insecure handling of symlinks with --links and --metadata in rclone while copying to local disk allows unprivileged users to indirectly modify ownership and permissions on symlink target files when a superuser or privileged process performs a copy. This vulnerability could enable privilege escalation and unauthorized access to critical system files, compromising system integrity, confidentiality, and availability. This vulnerability is fixed in 1.68.2.	2024-11-15	5.5	CVE-2024-52522
realmag777--WOLF	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in realmag777 WOLF allows Path Traversal.This issue affects WOLF: from n/a through 1.0.8.3.	2024-11-14	4.9	CVE-2024-52396
Red Hat--Red Hat Ansible Automation Platform 2	A flaw was found in Ansible-Core. This vulnerability allows attackers to bypass unsafe content protections using the hostvars object to reference and execute templated content. This issue can lead to arbitrary code execution if remote data or module outputs are improperly templated within playbooks.	2024-11-12	5.5	CVE-2024-11079
Red Hat--Red Hat build of Debezium	A script injection vulnerability was found in the Debezium database connector, where it does not properly sanitize some parameters. This flaw allows an attacker to send a malicious request to inject a parameter that may allow the viewing of unauthorized data.	2024-11-17	5.9	CVE-2023-1419
Red Hat--Red Hat OpenShift Container Platform 4	A vulnerability was found in the OAuth-server. OAuth-server logs the OAuth2 client secret when the logLevel is Debug higher for OIDC/GitHub/GitLab/Google IDPs login options.	2024-11-15	4.9	CVE-2024-11217
Red Hat--Red Hat OpenStack Platform 17.1 for RHEL 8	A flaw was found in OpenStack. When a user tries to delete a non-existing access rule in it's scope, it deletes other existing access rules which are not associated with any application credentials.	2024-11-17	5.5	CVE-2023-6110
Salt--SALT	The Salt-SSH pre-flight option copies the script to the target at a predictable path, which allows an attacker to force Salt-SSH to run their script. If an attacker has access to the target VM and knows the path to the pre-flight script before it runs they can ensure Salt-SSH runs their script with the privileges of the user running Salt-SSH.Â Do not make the copy path on the target predictable and ensure we check return codes of the scp command if the copy fails.	2024-11-14	6.7	CVE-2023-34049
SAP_SE--SAP NetWeaver Application Server ABAP	SAP NetWeaver Application Server ABAP allows an unauthenticated attacker with network access to read files from the server, which otherwise would be restricted.This attack is possible only if a Web Dispatcher or some sort of Proxy Server is in use and the file in question was previously opened or downloaded in an application based on SAP GUI for HTML Technology. This will not compromise the application's integrity or availability.	2024-11-12	4.3	CVE-2024-47593
SAP_SE--SAP NetWeaver Application Server for ABAP and ABAP Platform	SAP NetWeaver Application Server for ABAP and ABAP Platform allows an unauthenticated attacker to send a maliciously crafted http request which could cause a null pointer dereference in the kernel. This dereference will result in the system crashing and rebooting, causing the system to be temporarily unavailable. There is no impact on Confidentiality or Integrity.	2024-11-12	5.3	CVE-2024-47586
SAP_SE--SAP NetWeaver Application Server Java (Logon	SAP NetWeaver AS Java allows an unauthenticated attacker to brute force the login functionality in order to identify the legitimate user IDs. This has an impact on confidentiality but not on integrity or availability.	2024-11-12	5.3	CVE-2024-47592

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Application)				
SAP_SE--SAP NetWeaver AS Java (System Landscape Directory)	Due to missing authorization check in SAP NetWeaver AS Java (System Landscape Directory) an unauthorized user can read and modify some restricted global SLD configurations causing low impact on confidentiality and integrity of the application.	2024-11-12	6.5	CVE-2024-42372
SAP_SE--SAP NetWeaver Java (Software Update Manager)	In SAP NetWeaver Java (Software Update Manager 1.1), under certain conditions when a software upgrade encounters errors, credentials are written in plaintext to a log file. An attacker with local access to the server, authenticated as a non-administrative user, can acquire the credentials from the logs. This leads to a high impact on confidentiality, with no impact on integrity or availability.	2024-11-12	4.7	CVE-2024-47588
Schneider Electric--Modicon M340 CPU (part numbers BMXP34*)	CWE-20: Improper Input Validation vulnerability exists that could lead to loss of confidentiality of controller memory after a successful Man-In-The-Middle attack followed by sending a crafted Modbus function call used to tamper with memory.	2024-11-13	6.5	CVE-2024-8936
Schneider Electric--Modicon M340 CPU (part numbers BMXP34*)	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause a potential arbitrary code execution after a successful Man-In-The Middle attack followed by sending a crafted Modbus function call to tamper with memory area involved in the authentication process.	2024-11-13	6.5	CVE-2024-8937
sharethepractice -- christian_science_bible_lesson_subjects	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Gabriel Serafini Christian Science Bible Lesson Subjects allows DOM-Based XSS.This issue affects Christian Science Bible Lesson Subjects: from n/a through 2.0.	2024-11-11	5.4	CVE-2024-52353
siemens -- ozw672_firmware	A vulnerability has been identified in OZW672 (All versions < V5.2), OZW772 (All versions < V5.2). The user accounts tab of affected devices is vulnerable to stored cross-site scripting (XSS) attacks. This could allow an authenticated remote attacker to inject arbitrary JavaScript code that is later executed by another authenticated victim user with potential higher privileges than the attacker.	2024-11-12	5.4	CVE-2024-36140
siemens -- ruggedcom_rm1224_lte\(4g\)_eu_firmware	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.2), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.2), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V8.2), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.2), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.2), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.2), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.2), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.2), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.2), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.2), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.2), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.2), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.2), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.2), SCALANCE MUM856-1 (B1)	2024-11-12	6.1	CVE-2024-50561

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(6GK5856-2EA10-3BA1) (All versions < V8.2), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.2), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.2), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.2), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.2), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.2). Affected devices do not properly sanitize the filenames before uploading. This could allow an authenticated remote attacker to compromise of integrity of the system.			
siemens -- ruggedcom_rm1224_lte\(4g\)_eu_firmware	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.2), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.2), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V8.2), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.2), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.2), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.2), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.2), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.2), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.2), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.2), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.2), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.2), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.2), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.2), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.2), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.2), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.2), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.2), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.2), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.2). Affected devices improperly manage access control for read-only users. This could allow an attacker to cause a temporary denial of service condition.	2024-11-12	4.3	CVE-2024-50558
siemens -- ruggedcom_rm1224_lte\(4g\)_eu_firmware	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.2), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.2), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V8.2), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.2), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.2), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.2), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.2), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.2), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.2), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.2), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.2), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.2), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.2), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.2), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.2), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.2), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.2), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.2), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-	2024-11-12	4.3	CVE-2024-50559

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2AA2) (All versions < V8.2), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.2). Affected devices do not properly validate the filenames of the certificate. This could allow an authenticated remote attacker to append arbitrary values which will lead to compromise of integrity of the system.			
siemens -- ruggedcom_rm1224_lte\(4g\)_eu_firmware	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.2), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.2), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1AA00-2AA2) (All versions < V8.2), SCALANCE M812-1 ADSL-Router (6GK5812-1BA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V8.2), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V8.2), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.2), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.2), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.2), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.2), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.2), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.2), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.2), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.2), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.2), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.2), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.2), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.2), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.2), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.2), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.2), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.2), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.2), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.2). Affected devices truncates usernames longer than 15 characters when accessed via SSH or Telnet. This could allow an attacker to compromise system integrity.	2024-11-12	4.3	CVE-2024-50560
siemens -- sinec_ins	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 3). The affected application uses hard-coded cryptographic key material to obfuscate configuration files. This could allow an attacker to learn that cryptographic key material through reverse engineering of the application binary and decrypt arbitrary backup files.	2024-11-12	5.3	CVE-2024-46889
siemens -- sinec_nms	A vulnerability has been identified in SINEC NMS (All versions < V3.0 SP1). The affected application contains a database function, that does not properly restrict the permissions of users to write to the filesystem of the host system. This could allow an authenticated medium-privileged attacker to write arbitrary content to any location in the filesystem of the host system.	2024-11-12	6.5	CVE-2024-47808
Siemens--SINEC INS	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 3). The affected application does not properly validate authorization of a user to query the "/api/sftp/users" endpoint. This could allow an authenticated remote attacker to gain knowledge about the list of configured users of the SFTP service and also modify that configuration.	2024-11-12	6.3	CVE-2024-46894
Siemens--SINEC INS	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 3). The affected application does not properly restrict the size of generated log files. This could allow an unauthenticated remote attacker to trigger a large amount of logged events to exhaust the system's resources and create a denial of service condition.	2024-11-12	5.3	CVE-2024-46891
Simple Goods--Simple Goods	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Simple Goods allows Stored XSS.This issue affects Simple Goods: from n/a through 0.1.3.	2024-11-11	6.5	CVE-2024-51574

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
simpleform--SimpleForm Contact form made simple	The SimpleForm - Contact form made simple 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, 2.2.0. 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.	2024-11-16	6.1	CVE-2024-10883
simpleform--SimpleForm Contact Form Submissions	The SimpleForm Contact Form Submissions 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, 2.1.0. 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.	2024-11-16	6.1	CVE-2024-10884
smartwpress--Music Player for Elementor Audio Player & Podcast Player	The Music Player for Elementor - Audio Player & Podcast Player plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the import_mpfe_template() function in all versions up to, and including, 2.4.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to import templates.	2024-11-15	4.3	CVE-2024-10582
smub--WPForms Easy Form Builder for WordPress Contact Forms, Payment Forms, Surveys, & More	The WPForms - Easy Form Builder for WordPress - Contact Forms, Payment Forms, Surveys, & More plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.9.1.6. This is due to missing or incorrect nonce validation on the process_admin_ui function. This makes it possible for unauthenticated attackers to delete WPForm logs via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-11-13	4.3	CVE-2024-10593
SoftBank Corp.--Mesh Wi-Fi router RP562B	Active debug code vulnerability exists in Mesh Wi-Fi router RP562B firmware version v1.0.2 and earlier. If this vulnerability is exploited, a network-adjacent authenticated attacker may obtain or alter the settings of the device .	2024-11-12	4.6	CVE-2024-29075
Sonatype--Nexus Repository	A Remote Code Execution vulnerability has been discovered in Sonatype Nexus Repository 2.Â This issue affects Nexus Repository 2 OSS/Pro versions up to and including 2.15.1.	2024-11-14	4.3	CVE-2024-5082
Sonatype--Nexus Repository	A storedÂ Cross-site Scripting vulnerability has been discovered in Sonatype Nexus Repository 2 This issue affects Nexus Repository 2 OSS/Pro versions up to and including 2.15.1.	2024-11-14	4.6	CVE-2024-5083
Sound Research--SECOMN64 Driver	Potential vulnerabilities have been identified in the audio package for certain HP PC products using the Sound Research SECOMN64 driver, which might allow escalation of privilege. Sound Research has released driver updates to mitigate the potential vulnerabilities.	2024-11-12	6	CVE-2024-2207
SourceCodester--Best Employee Management System	A vulnerability, which was classified as critical, has been found in SourceCodester Best Employee Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/fetch_product_details.php. The manipulation of the argument barcode leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-14	6.3	CVE-2024-11212
SourceCodester--Best Employee Management System	A vulnerability, which was classified as critical, was found in SourceCodester Best Employee Management System 1.0. This affects an unknown part of the file /admin/edit_role.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-14	4.7	CVE-2024-11213
SourceCodester--Best Employee	A vulnerability has been found in SourceCodester Best Employee Management System 1.0 and classified as critical. This vulnerability affects unknown code of the	2024-11-14	4.7	CVE-2024-11214

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	file /admin/profile.php. The manipulation of the argument website_image leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher disclosure contains confusing vulnerability classes.			
SourceCodester--Hospital Management System	A vulnerability classified as problematic has been found in SourceCodester Hospital Management System 1.0. This affects an unknown part of the file /vm/patient/delete-account.php. The manipulation of the argument id leads to improper authorization. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-11	4.3	CVE-2024-11073
SourceCodester--Student Record Management System	A vulnerability, which was classified as critical, was found in SourceCodester Student Record Management System 1.0. Affected is an unknown function of the file StudentRecordManagementSystem.cpp of the component Number of Students Menu. The manipulation leads to memory corruption. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used.	2024-11-15	5.3	CVE-2024-11261
SourceCodester--Student Record Management System	A vulnerability has been found in SourceCodester Student Record Management System 1.0 and classified as critical. Affected by this vulnerability is the function main of the component View All Student Marks. The manipulation leads to stack-based buffer overflow. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used.	2024-11-15	5.3	CVE-2024-11262
starverte--Steel	The Steel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's btn shortcode in all versions up to, and including, 1.3.0 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.	2024-11-16	6.4	CVE-2024-10147
staxwp--BuddyPress Builder for Elementor BuddyBuilder	The BuddyPress Builder for Elementor - BuddyBuilder plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.7.4 via the 'elementor-template' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts crated by Elementor that they should not have access to.	2024-11-13	4.3	CVE-2024-10778
stevehenty--Drop Shadow Boxes	The The Drop Shadow Boxes plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.7.14. 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.	2024-11-16	6.3	CVE-2024-10262
themes4wp--Popularis Extra	The Popularis Extra plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.2.7 via the 'elementor-template' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created via Elementor that they should not have access to.	2024-11-16	4.3	CVE-2024-10795
themeum--Tutor LMS Elementor Addons	The Tutor LMS Elementor Addons plugin for WordPress is vulnerable to unauthorized plugin installation due to a missing capability check on the install_etlms_dependency_plugin() function in all versions up to, and including, 2.1.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install Elementor or Tutor LMS. Please note the impact of this issue is incredibly limited due to the fact that these two plugins will likely already be installed as a dependency of the plugin.	2024-11-15	4.3	CVE-2024-10897
thimpress--LearnPress Export Import WordPress extension for	The LearnPress Export Import - WordPress extension for LearnPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'learnpress_import_form_server' parameter in all versions up to, and including, 4.0.4 due to insufficient input sanitization and output escaping. This makes it	2024-11-15	6.1	CVE-2024-9609

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
LearnPress	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.			
thinkaquamarine--Aqua SVG Sprite	The Aqua SVG Sprite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 3.0.14 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.	2024-11-13	6.4	CVE-2024-9426
TIBCO Software Inc--TIBCO Hawk	XSS Attack in mar.jar, Monitoring Archive Utility (MAR Utility),Â monitoringconsolecommon.jarÂ in TIBCO Software IncÂ TIBCO Hawk andÂ TIBCO Operational Intelligence	2024-11-12	5.2	CVE-2024-10217
TIBCO Software Inc--TIBCO Hawk	XSS Attack in mar.jar, Monitoring Archive Utility (MAR Utility),Â monitoringconsolecommon.jarÂ in TIBCO Software IncÂ TIBCO Hawk andÂ TIBCO Operational Intelligence	2024-11-12	5.2	CVE-2024-10218
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 & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.8.0. 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.	2024-11-13	6.1	CVE-2024-10882
Unknown--Jobs for WordPress	The Jobs for WordPress plugin before 2.7.8 does not sanitise and escape some of its Job settings, which could allow high privilege users such as contributor to perform Stored Cross-Site Scripting attacks	2024-11-15	5.9	CVE-2024-10104
Unknown--RSS Feed Widget	The RSS Feed Widget WordPress plugin before 3.0.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	2024-11-12	5.9	CVE-2024-9836
Unknown--RSS Feed Widget	The RSS Feed Widget WordPress plugin before 3.0.1 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could lead to Reflected Cross-Site Scripting in old web browsers	2024-11-12	4.8	CVE-2024-9835
Unknown--Secure Custom Fields	The Secure Custom Fields WordPress plugin before 6.3.9, Secure Custom Fields WordPress plugin before 6.3.6.3, Advanced Custom Fields Pro WordPress plugin before 6.3.9 does not prevent users from running arbitrary functions through its setting import functionalities, which could allow high privilege users such as admin to run arbitrary PHP functions.	2024-11-15	6.6	CVE-2024-9529
Unknown--Simple File List	The Simple File List WordPress plugin before 6.1.13 does not sanitise and escape a generated URL before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against admins.	2024-11-14	5.4	CVE-2024-10146
unopim--unopim	UnoPim is an open-source Product Information Management (PIM) system built on the Laravel framework. A vulnerability exists in the Create User process, allowing the creation of a new admin account with an option to upload a profile image. An attacker can upload a malicious SVG file containing an embedded script. When the profile image is accessed, the embedded script executes, leading to the potential theft of session cookies. This vulnerability is fixed in 0.1.5.	2024-11-13	6.5	CVE-2024-52305
VaeMendis--VaeMendis Ubooquity version 2.1.2	VaeMendis - CWE-352: Cross-Site Request Forgery (CSRF)	2024-11-14	4.5	CVE-2024-47914

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
VIWIS--LMS	A vulnerability was found in VIWIS LMS 9.11. It has been classified as critical. Affected is an unknown function of the component Print Handler. The manipulation leads to missing authorization. It is possible to launch the attack remotely. A user with the role learner can use the administrative print function with an active session before and after an exam slot to access the entire exam including solutions in the web application. It is recommended to apply a patch to fix this issue.	2024-11-13	5.3	CVE-2024-8001
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 2.1.0.	2024-11-11	5.4	CVE-2024-52356
westi--PJW Mime Config	The PJW Mime Config 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.	2024-11-16	6.4	CVE-2024-10017
wpdevteam--Essential Addons for Elementor Best Elementor Addon, Templates, Widgets, Kits & WooCommerce Builders	The Essential Addons for Elementor - Best Elementor Addon, Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'nomore_items_text' parameter in all versions up to, and including, 6.0.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-15	6.4	CVE-2024-8961
wpdevteam--Essential Addons for Elementor Best Elementor Addon, Templates, Widgets, Kits & WooCommerce Builders	The Essential Addons for Elementor - Best Elementor Addon, Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 6.0.9 via the 'init_content_register_user_email_controls' function. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive data including usernames and passwords of any users who register via the Login | Register Form widget, as long as that user opens the email notification for successful registration.	2024-11-15	5.7	CVE-2024-8978
wpeka-club--WP AdCenter Ad Manager & Adsense Ads	The WP AdCenter - Ad Manager & Adsense Ads plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpadcenter_ad shortcode in all versions up to, and including, 2.5.7 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.	2024-11-15	6.4	CVE-2024-10113
wpmariocom--Exclusive Divi Divi Preloader, Modules for Divi & Extra Theme	The Exclusive Divi - Divi Preloader, Modules for Divi & Extra Theme plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.4 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.	2024-11-16	6.4	CVE-2024-9386
wpmonks--Styler for Ninja Forms	The Styler for Ninja Forms plugin for WordPress is vulnerable to unauthorized modification of data that can lead to a denial of service due to a missing capability check on the deactivate_license function in all versions up to, and including, 3.3.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary option values on the WordPress site. This can be leveraged to delete an option that would create an error on the site and deny service to legitimate users. Note: This issue can also be used to add arbitrary options with an empty value.	2024-11-13	6.5	CVE-2024-10717

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wpplugin -- contact_form_7_redirect_\&_thank_you_page	The Contact Form 7 Redirect & Thank You Page plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 1.0.6 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.	2024-11-12	6.1	CVE-2024-10685
wproyal--Royal Elementor Addons and Templates	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Google Maps widget in all versions up to, and including, 1.7.1001 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.	2024-11-13	6.4	CVE-2024-9059
wproyal--Royal Elementor Addons and Templates	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown widget in all versions up to, and including, 1.7.1001 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.	2024-11-13	6.4	CVE-2024-9668
wproyal--Royal Elementor Addons and Templates	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Form Builder widget in all versions up to, and including, 1.7.1001 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.	2024-11-13	6.4	CVE-2024-9682
wpslickstream--Slickstream: Engagement and Conversions	The Slickstream: Engagement and Conversions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's slick-grid shortcode in all versions up to, and including, 1.4.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-11-12	6.4	CVE-2024-10179
yotpo--Yotpo: Product & Photo Reviews for WooCommerce	The Yotpo: Product & Photo Reviews for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'yotpo_user_email' and 'yotpo_user_name' parameters in all versions up to, and including, 1.7.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2024-11-15	6.1	CVE-2024-9356
YugabyteDB--YugabyteDB Anywhere	An information disclosure vulnerability exists in Yugabyte Anywhere, where the LDAP bind password is logged in plaintext within application logs. This flaw results in the unintentional exposure of sensitive information in Yugabyte Anywhere logs, potentially allowing unauthorized users with access to these logs to view the LDAP bind password.Â An attacker with log access could exploit this vulnerability to gain unauthorized access to the LDAP server, leading to potential exposure or compromise of LDAP-managed resources This issue affects YugabyteDB Anywhere: from 2.20.0.0 before 2.20.7.0, from 2.23.0.0 before 2.23.1.0, from 2024.1.0.0 before 2024.1.3.0.	2024-11-13	6.5	CVE-2024-11193
zyxel -- gs1900-8_firmware	A post-authentication command injection vulnerability in the CGI program in the Zyxel GS1900-48 switch firmware version V2.80(AAHN.1)C0 and earlier could allow an authenticated, LAN-based attacker with administrator privileges to execute some operating system (OS) commands on an affected device by sending a crafted HTTP request.	2024-11-12	6.8	CVE-2024-8881

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zyxel -- gs1900-8_firmware	A buffer overflow vulnerability in the CGI program in the Zyxel GS1900-48 switch firmware version V2.80(AAHN.1)C0 and earlierÂ could allow an authenticated, LAN-based attacker with administrator privileges to cause denial of service (DoS) conditions via a crafted URL.	2024-11-12	4.5	CVE-2024-8882
zzcms -- zzcms	A vulnerability was found in ZZCMS up to 2023. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/msg.php. The manipulation of the argument keyword leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-12	4.8	CVE-2024-11130

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Axis Communications AB--AXIS OS	Erik de Jong, member of the AXIS OS Bug Bounty Program, has found that the VAPIX API ftptest.cgi did not have a sufficient input validation allowing for a possible command injection leading to being able to transfer files from/to the Axis device. This flaw can only be exploited after authenticating with an administrator-privileged service account. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	2024-11-26	3.8	CVE-2024-8160
code-projects--Blood Bank System	A vulnerability was found in code-projects Blood Bank System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /controllers/updatesettings.php of the component Setting Handler. The manipulation of the argument firstname leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	2024-11-30	3.5	CVE-2024-12000
code-projects--Crud Operation System	A vulnerability, which was classified as problematic, has been found in code-projects Crud Operation System 1.0. This issue affects some unknown processing of the file /add.php. The manipulation of the argument saddress leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	2024-11-27	3.5	CVE-2024-11820
code-projects--Farmacia	A vulnerability was found in code-projects Farmacia 1.0. It has been classified as problematic. This affects an unknown part of the file usuario.php. The manipulation of the argument name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	2024-11-25	3.5	CVE-2024-11660
code-projects--Farmacia	A vulnerability has been found in code-projects Farmacia 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /pagamento.php. The manipulation of the argument total leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-29	3.5	CVE-2024-11995
code-projects--Farmacia	A vulnerability was found in code-projects Farmacia 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /editar-fornecedor.php. The manipulation of the argument cidade leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	2024-11-30	3.5	CVE-2024-11996
code-projects--Farmacia	A vulnerability was found in code-projects Farmacia 1.0. It has been classified as problematic. This affects an unknown part of the file /vendas.php. The manipulation of the argument notaFiscal 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.	2024-11-30	3.5	CVE-2024-11997
code-projects--Wazifa System	A vulnerability classified as problematic has been found in code-projects Wazifa System 1.0. Affected is an unknown function of the file /controllers/updatesettings.php of the component Setting Handler. The manipulation of the argument firstname 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. Other parameters might be affected as well.	2024-11-30	3.5	CVE-2024-12001
CodeAstro--Hospital Management System	A vulnerability has been found in CodeAstro Hospital Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /backend/admin/his_admin_register_patient.php of the component Add Patient Details Page. The manipulation of the argument pat_fname/pat_ailment/pat_lname/pat_age/pat_dob/pat_number/pat_phone/pat_type/pat_addr leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-26	3.5	CVE-2024-11675

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
CodeAstro--Hospital Management System	A vulnerability was found in CodeAstro Hospital Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /backend/admin/his_admin_add_lab_equipment.php of the component Add Laboratory Equipment Page. The manipulation of the argument eqp_code/eqp_name/eqp_vendor/eqp_desc/eqp_dept/eqp_status/eqp_qty leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-26	3.5	CVE-2024-11676
CodeAstro--Hospital Management System	A vulnerability was found in CodeAstro Hospital Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /backend/admin/his_admin_add_vendor.php of the component Add Vendor Details Page. The manipulation of the argument v_name/v_adr/v_number/v_email/v_phone/v_desc 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.	2024-11-26	3.5	CVE-2024-11677
CodeAstro--Hospital Management System	A vulnerability was found in CodeAstro Hospital Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /backend/doc/his_doc_register_patient.php. The manipulation of the argument pat_fname/pat_ailment/pat_lname/pat_age/pat_dob/pat_number/pat_phone/pat_type/pat_addr leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-26	3.5	CVE-2024-11678
Guizhou Xiaoma Technology--jpress	A vulnerability classified as problematic was found in Guizhou Xiaoma Technology jpress 5.1.2. Affected by this vulnerability is an unknown functionality of the file /commons/attachment/upload of the component Avatar Handler. The manipulation of the argument files leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-28	3.5	CVE-2024-11971
nofusscomputing--centurion_erp	Centurion ERP (Enterprise Rescource Planning) is a simple application developed to provide open source IT management with a large emphasis on the IT Service Management (ITSM) modules. A user who is authenticated and has view permissions for a ticket, can view the tickets of another organization they are not apart of. Users with following permissions are applicable: 1. `view_ticket_change` permission can view change tickets from organizations they are not apart of. 2. `view_ticket_incident` permission can view incident tickets from organizations they are not apart of. 3. `view_ticket_request` permission can view request tickets from organizations they are not apart of. 4. `view_ticket_problem` permission can view problem tickets from organizations they are not apart of. The access to view the tickets from different organizations is only applicable when browsing the API endpoints for the tickets in question. The Centurion UI is not affected. Project Tasks, although a "ticket type" are also **Not** affected. This issue has been addressed in release version 1.3.1 and users are advised to upgrade. Users unable to upgrade may remove the ticket view permissions from users which would alleviate this vulnerability, if this is deemed not-viable, Upgrading is recommended.	2024-11-27	1.9	CVE-2024-53855
SourceCodester--Best House Rental Management System	A vulnerability, which was classified as problematic, has been found in SourceCodester Best House Rental Management System 1.0. This issue affects some unknown processing of the file /rental/ajax.php?action=save_tenant. The manipulation of the argument lastname/firstname/middlename leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	2024-11-26	3.5	CVE-2024-11742
SUSE--Container suse/manager/5.0/x86_64/server:5.0.2.7.8.1	A Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in the Setup Wizard, HTTP Proxy credentials pane in spacewalk-web allows attackers to attack users by providing specially crafted URLs to click. This issue affects Container suse/manager/5.0/x86_64/server:5.0.2.7.8.1: before 5.0.15-150600.3.10.2; SUSE Manager Server Module 4.3: before 4.3.42-150400.3.52.1.	2024-11-28	3.5	CVE-2024-49502

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SUSE--Container suse/manager/5.0/x86_64/server:5.0.2.7.8.1	A Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SUSE manager allows attackers to execute Javascript code in the organization credentials sub page. This issue affects Container suse/manager/5.0/x86_64/server:5.0.2.7.8.1: before 5.0.15-150600.3.10.2; SUSE Manager Server Module 4.3: before 4.3.42-150400.3.52.1.	2024-11-28	3.5	CVE-2024-49503
Unknown--YaDisk Files	The YaDisk Files WordPress plugin through 1.2.5 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).	2024-11-25	3.5	CVE-2024-10710
Zabbix--Zabbix	The reported vulnerability is a stack buffer overflow in the zbx_snmp_cache_handle_engineid function within the Zabbix server/proxy code. This issue occurs when copying data from session->securityEngineID to local_record.engineid without proper bounds checking.	2024-11-27	3	CVE-2024-36468
Zabbix--Zabbix	When the webdriver for the Browser object downloads data from a HTTP server, the data pointer is set to NULL and is allocated only in curl_write_cb when receiving data. If the server's response is an empty document, then wd->data in the code below will remain NULL and an attempt to read from it will result in a crash.	2024-11-27	3.3	CVE-2024-42328
Zabbix--Zabbix	The webdriver for the Browser object expects an error object to be initialized when the webdriver_session_query function fails. But this function can fail for various reasons without an error description and then the wd->error will be NULL and trying to read from it will result in a crash.	2024-11-27	3.3	CVE-2024-42329
Zabbix--Zabbix	In the src/libs/zbxembed/browser.c file, the es_browser_ctor method retrieves a heap pointer from the Duktape JavaScript engine. This heap pointer is subsequently utilized by the browser_push_error method in the src/libs/zbxembed/browser_error.c file. A use-after-free bug can occur at this stage if the wd->browser heap pointer is freed by garbage collection.	2024-11-27	3.3	CVE-2024-42331
Zabbix--Zabbix	The researcher is showing that due to the way the SNMP trap log is parsed, an attacker can craft an SNMP trap with additional lines of information and have forged data show in the Zabbix UI. This attack requires SNMP auth to be off and/or the attacker to know the community/auth details. The attack requires an SNMP item to be configured as text on the target host.	2024-11-27	3.7	CVE-2024-42332
Zabbix--Zabbix	When a URL is added to the map element, it is recorded in the database with sequential IDs. Upon adding a new URL, the system retrieves the last sysmapelementurlid value and increments it by one. However, an issue arises when a user manually changes the sysmapelementurlid value by adding sysmapelementurlid + 1. This action prevents others from adding URLs to the map element.	2024-11-26	2.2	CVE-2024-22117
Zabbix--Zabbix	When exporting media types, the password is exported in the YAML in plain text. This appears to be a best practices type issue and may have no actual impact. The user would need to have permissions to access the media types and therefore would be expected to have access to these passwords.	2024-11-27	2.7	CVE-2024-36464
Zabbix--Zabbix	The researcher is showing that it is possible to leak a small amount of Zabbix Server memory using an out of bounds read in src/libs/zbxmedia/email.c	2024-11-27	2.7	CVE-2024-42333
Apereo--CAS	A vulnerability was found in Apereo CAS 6.6 and classified as problematic. Affected by this issue is some unknown functionality of the file /login?service. The manipulation leads to session expiration. 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.	2024-11-14	3.7	CVE-2024-11208

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects--Farmacia	A vulnerability, which was classified as problematic, was found in code-projects Farmacia 1.0. Affected is an unknown function of the file /adicionar-cliente.php. The manipulation of the argument nome/cpf/dataNascimento leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions the parameter "nome" to be affected. But further inspection indicates that other parameters might be affected as well.	2024-11-15	3.5	CVE-2024-11246
code-projects--Farmacia	A vulnerability, which was classified as problematic, has been found in code-projects Farmacia 1.0. This issue affects some unknown processing of the file /fornecedores.php. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-15	3.5	CVE-2024-11259
code-projects--Job Recruitment	A vulnerability has been found in code-projects Job Recruitment 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /register.php. The manipulation of the argument e leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-11-11	3.5	CVE-2024-11078
dell -- smartfabric_os10	Dell SmartFabric OS10 Software, version(s) 10.5.6.x, 10.5.5.x, 10.5.4.x, 10.5.3.x, contain(s) a Files or Directories Accessible to External Parties vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Filesystem access for attacker.	2024-11-12	3.3	CVE-2024-48838
Digistar--AG-30 Plus	A vulnerability was found in Digistar AG-30 Plus 2.6b. It has been classified as problematic. Affected is an unknown function of the component Login Page. The manipulation leads to improper restriction of excessive authentication attempts. The complexity of an attack is rather high. The exploitability is told to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-12	3.1	CVE-2024-11126
Eclipse Foundation--Open J9	In Eclipse OpenJ9 versions up to 0.47, the JNI function GetStringUTFLength may return an incorrect value which has wrapped around. From 0.48 the value is correct but may be truncated to include a smaller number of characters.	2024-11-11	3.7	CVE-2024-10917
element-hq--element-web	Element is a Matrix web client built using the Matrix React SDK. Versions of Element Web and Desktop earlier than 1.11.85 do not check if thumbnails for attachments, stickers and images are coherent. It is possible to add thumbnails to events trigger a file download once clicked. Fixed in element-web 1.11.85.	2024-11-12	3.5	CVE-2024-51749
Fortinet--FortiAnalyzer	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability [CWE-22] in Fortinet FortiAnalyzer versions below 7.4.2, Fortinet FortiManager versions below 7.4.2 and Fortinet FortiAnalyzer-BigData version 7.4.0 and below 7.2.7 allows a privileged attacker with read write administrative privileges to create non-arbitrary files on a chosen directory via crafted CLI requests.	2024-11-12	2.3	CVE-2024-35274
GitLab--GitLab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.3 before 17.3.7, all versions starting from 17.4 before 17.4.4, all versions starting from 17.5 before 17.5.2. This issue allows an attacker to create a group with a name matching an existing unique Pages domain, potentially leading to domain confusion attacks.	2024-11-14	3.1	CVE-2024-9633
HCL Software--Connections	HCL Connections is vulnerable to a broken access control vulnerability that may allow an unauthorized user to update data in certain scenarios.	2024-11-14	3.7	CVE-2024-42188

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBPhoenix--ibWebAdmin	A vulnerability was found in IBPhoenix ibWebAdmin up to 1.0.2 and classified as problematic. This issue affects some unknown processing of the file /database.php of the component Banco de Dados Tab. The manipulation of the argument db_login_role leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-11-15	3.5	CVE-2024-11240
n/a--DedeCMS	A vulnerability classified as problematic has been found in DedeCMS 5.7.116. This affects an unknown part of the file /dede/uploads/dede/friendlink_add.php. The manipulation of the argument logoimg leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-11-12	2.7	CVE-2024-11138
n/a--Intel(R) PROSet/Wireless Software and Intel(R) Killer(TM) Wi-Fi	Improper initialization in firmware for some Intel(R) PROSet/Wireless Software and Intel(R) Killer(TM) Wi-Fi before version 23.40 may allow a privileged user to potentially enable information disclosure via local access.	2024-11-13	3.4	CVE-2024-25563
n/a--Intel(R) PROSet/Wireless WiFi software for Windows	Improper input validation for some Intel(R) PROSet/Wireless WiFi software for Windows before version 23.60 may allow a privileged user to potentially enable denial of service via local access.	2024-11-13	3.4	CVE-2024-33611
n/a--Intel(R) VPL software	NULL pointer dereference in some Intel(R) VPL software before version 24.1.4 may allow an authenticated user to potentially enable denial of service via local access.	2024-11-13	2.2	CVE-2024-28030
n/a--Intel(R) VPL software	Out-of-bounds read in some Intel(R) VPL software before version 24.1.4 may allow an authenticated user to potentially enable information disclosure via local access.	2024-11-13	2.2	CVE-2024-28051
n/a--Intel(R) VROC software	Improper Input Validation in some Intel(R) VROC software before version 8.6.0.2003 may allow an authenticated user to potentially enable denial of service via local access.	2024-11-13	3.9	CVE-2024-32485
n/a--Intel(R) Xeon(R) processor family (E-Core)	Protection mechanism failure in the SPP for some Intel(R) Xeon(R) processor family (E-Core) may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-11-13	3.8	CVE-2024-38660
n/a--Intel(R) Xeon(R) Processors	Insufficient control flow management in UEFI firmware for some Intel(R) Xeon(R) Processors may allow an authenticated user to enable denial of service via local access.	2024-11-13	3.8	CVE-2024-25565
n/a--n/a	A flaw was found in Keycloak. This issue occurs due to improperly enforcing token types when validating signatures locally. This could allow an authenticated attacker to exchange a logout token for an access token and possibly gain access to data outside of enforced permissions.	2024-11-17	3.4	CVE-2023-0657
n/a--n/a	A flaw was found in moodle. When creating an export of site administration presets, some sensitive secrets and keys are not being excluded from the export, which could result in them unintentionally being leaked if the presets are shared with a third party.	2024-11-11	3.7	CVE-2024-43427
n/a--n/a	A SQL Injection vulnerability was found in /admin/login.php in kashipara E-learning Management System Project 1.0 via the username and password parameters.	2024-11-14	3.5	CVE-2024-50823
n/a--n/a	A SQL Injection vulnerability was found in /admin/class.php in kashipara E-learning Management System Project 1.0 via the class_name parameter.	2024-11-14	3.5	CVE-2024-50824

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	A SQL Injection vulnerability was found in /admin/school_year.php in kashipara E-learning Management System Project 1.0 via the school_year parameter.	2024-11-14	3.5	CVE-2024-50825
n/a--n/a	A SQL Injection vulnerability was found in /admin/add_content.php in kashipara E-learning Management System Project 1.0 via the title and content parameters.	2024-11-14	3.5	CVE-2024-50826
n/a--n/a	A SQL Injection vulnerability was found in /admin/add_subject.php in kashipara E-learning Management System Project 1.0 via the subject_code parameter.	2024-11-14	3.5	CVE-2024-50827
n/a--n/a	A SQL Injection vulnerability was found in /admin/edit_department.php in kashipara E-learning Management System Project 1.0 via the d parameter.	2024-11-14	3.5	CVE-2024-50828
n/a--n/a	A SQL Injection vulnerability was found in /admin/edit_subject.php in kashipara E-learning Management System Project 1.0 via the unit parameter.	2024-11-14	3.5	CVE-2024-50829
n/a--n/a	A SQL Injection vulnerability was found in /admin/calendar_of_events.php in kashipara E-learning Management System Project 1.0 via the date_start, date_end, and title parameters.	2024-11-14	3.5	CVE-2024-50830
n/a--n/a	A SQL Injection was found in /admin/admin_user.php in kashipara E-learning Management System Project 1.0 via the username and password parameters.	2024-11-14	3.5	CVE-2024-50831
n/a--n/a	A SQL Injection vulnerability was found in /admin/edit_class.php in kashipara E-learning Management System Project 1.0 via the class_name parameter.	2024-11-14	3.5	CVE-2024-50832
n/a--n/a	A SQL Injection vulnerability was found in /login.php in KASHIPARA E-learning Management System Project 1.0 via the username and password parameters.	2024-11-14	3.5	CVE-2024-50833
n/a--n/a	A SQL Injection was found in /admin/teachers.php in KASHIPARA E-learning Management System Project 1.0 via the firstname and lastname parameters.	2024-11-14	3.5	CVE-2024-50834
n/a--n/a	A SQL Injection vulnerability was found in /admin/edit_student.php in KASHIPARA E-learning Management System Project 1.0 via the cys, un, ln, fn, and id parameters.	2024-11-14	3.5	CVE-2024-50835
n/a--n/a	Hathway Skyworth Router CM5100-511 v4.1.1.24 was discovered to store sensitive information about USB and Wifi connected devices in plaintext.	2024-11-15	2.4	CVE-2024-46383
n/a--OpenCL(TM) software	Out-of-bounds read for some OpenCL(TM) software may allow an authenticated user to potentially enable denial of service via local access.	2024-11-13	3.9	CVE-2024-32667
n/a--PostgreSQL	Client use of server error message in PostgreSQL allows a server not trusted under current SSL or GSS settings to furnish arbitrary non-NUL bytes to the libpq application. For example, a man-in-the-middle attacker could send a long error message that a human or screen-scraper user of psql mistakes for valid query results. This is probably not a concern for clients where the user interface unambiguously indicates the boundary between one error message and other text. Versions before PostgreSQL 17.1, 16.5, 15.9, 14.14, 13.17, and 12.21 are affected.	2024-11-14	3.1	CVE-2024-10977
nextcloud--security-advisories	Nextcloud Tables allows users to to create tables with individual columns. The information which Table (numeric ID) is shared with which groups and users and the respective permissions was not limited to affected users. It is recommended that the Nextcloud Tables app is upgraded to 0.8.1.	2024-11-15	3.5	CVE-2024-52507
nextcloud--security-advisories	Nextcloud Mail is the mail app for Nextcloud, a self-hosted productivity platform. The Nextcloud mail app incorrectly allowed attaching shared files without download permissions as attachments. This allowed users to send them the files to themselves and then downloading it from their mail clients. It is recommended that the Nextcloud Mail is upgraded to 2.2.10, 3.6.2 or 3.7.2.	2024-11-15	3.5	CVE-2024-52509

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud--security-advisories	user_oidc app is an OpenID Connect user backend for Nextcloud. A malicious user could send a malformed login link that would redirect the user to a provided URL after successfully authenticating. It is recommended that the Nextcloud User OIDC app is upgraded to 6.1.0.	2024-11-15	3.3	CVE-2024-52512
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. When a server is configured to only allow sharing with users that are in ones own groups, after a user was removed from a group, previously shared items were not unshared. It is recommended that the Nextcloud Server is upgraded to 22.2.11 or 23.0.11 or 24.0.6 and Nextcloud Enterprise Server is upgraded to 22.2.11 or 23.0.11 or 24.0.6.	2024-11-15	3	CVE-2024-52516
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. After receiving a "Files drop" or "Password protected" share link a malicious user was able to download attachments that are referenced in Text files without providing the password. It is recommended that the Nextcloud Server is upgraded to 28.0.11, 29.0.8 or 30.0.1 and Nextcloud Enterprise Server is upgraded to 25.0.13.13, 26.0.13.9, 27.1.11.9, 28.0.11, 29.0.8 or 30.0.1.	2024-11-15	2.6	CVE-2024-52513
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. The OAuth2 client secrets were stored in a recoverable way, so that an attacker that got access to a backup of the database and the Nextcloud config file, would be able to decrypt them. It is recommended that the Nextcloud Server is upgraded to 28.0.10 or 29.0.7 and Nextcloud Enterprise Server is upgraded to 27.1.11.8, 28.0.10 or 29.0.7.	2024-11-15	2.7	CVE-2024-52519
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. MD5 hashes were used to check background jobs for their uniqueness. This increased the chances of a background job with arguments falsely being identified as already existing and not be queued for execution. By changing the Hash to SHA256 the probability was heavily decreased. It is recommended that the Nextcloud Server is upgraded to 28.0.10, 29.0.7 or 30.0.0.	2024-11-15	2.6	CVE-2024-52521
nextcloud--security-advisories	Nextcloud Server is a self hosted personal cloud system. Under certain conditions the password of a user was stored unencrypted in the session data. The session data is encrypted before being saved in the session storage (Redis or disk), but it would allow a malicious process that gains access to the memory of the PHP process, to get access to the cleartext password of the user. It is recommended that the Nextcloud Server is upgraded to 28.0.12, 29.0.9 or 30.0.2.	2024-11-15	1.8	CVE-2024-52525
Sanluan--PublicCMS	A vulnerability, which was classified as problematic, has been found in Sanluan PublicCMS 5.202406.d. This issue affects some unknown processing of the file /admin/cmsTagType/save of the component Tag Type Handler. The manipulation of the argument name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-11-11	3.5	CVE-2024-11070
SAP_SE--SAP Cash Management (Cash Operations)	Cash Operations does not perform necessary authorization check for an authenticated user, resulting in escalation of privileges causing low impact to confidentiality to the application.	2024-11-12	3.5	CVE-2024-47587
SoftBank Corp.--Mesh Wi-Fi router RP562B	Exposure of sensitive system information to an unauthorized control sphere issue exists in Mesh Wi-Fi router RP562B firmware version v1.0.2 and earlier. If this vulnerability is exploited, a network-adjacent authenticated attacker may obtain information of the other devices connected through the Wi-Fi.	2024-11-12	3.5	CVE-2024-47799
SourceCodester--Hospital Management System	A vulnerability was found in SourceCodester Hospital Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /vm/doctor/edit-doc.php. The manipulation of the argument name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	2024-11-12	3.5	CVE-2024-11102

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SourceCodester--Online Eyewear Shop	A vulnerability has been found in SourceCodester Online Eyewear Shop 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /oews/classes/Master.php?f=save_product of the component Inventory Page. The manipulation of the argument brand leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	2024-11-15	3.5	CVE-2024-11247
themeisle -- multiple_page_generator	The Multiple Page Generator Plugin - MPG plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the mpg_upsert_project_source_block() function in all versions up to, and including, 4.0.2. This makes it possible for authenticated attackers, with editor-level access and above, to delete limited files on the server.	2024-11-12	2.7	CVE-2024-10672
YugabyteDB--YugabyteDB Anywhere	An information disclosure vulnerability exists in the backup configuration process where the SAS token is not masked in the configuration response. This oversight results in sensitive information leakage within the yb_backup log files, exposing the SAS token in plaintext. The leakage occurs during the backup procedure, leading to potential unauthorized access to resources associated with the SAS token.Â This issue affects YugabyteDB Anywhere: from 2.20.0.0 before 2.20.7.0, from 2.23.0.0 before 2.23.1.0, from 2024.1.0.0 before 2024.1.3.0.	2024-11-13	3.9	CVE-2024-11165