BULLETIN (SB24-247)

VULNERABILITY SUMMARY FOR THE WEEK OF

26TH AUGUST, 2024

Bulletin (SB24-247)
Vulnerability Summary for the Week of August 26, 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
Adobe--Acrobat Reader	Acrobat Reader versions 127.0.2651.105 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.	2024-08-26	7.8	CVE-2024-41879 psirt@adobe.com
aertherwide -- exiftags	Buffer Overflow vulnerability in open source exiftags v.1.01 allows a local attacker to execute arbitrary code via the paresetag function.	2024-08-27	7.8	CVE-2024-42851 cve@mitre.org
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 staffcatedit.php. The manipulation of the argument title leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-26	9.8	CVE-2024-8171 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
angeljudesuarez -- tailoring_management_system	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file staffedit.php. The manipulation of the argument id/stafftype/address/fullname/phonenumber/salary leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-27	9.8	CVE-2024-8220 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
apollographql--federation	Apollo Federation is an architecture for declaratively composing APIs into a unified graph. Each team can own their slice of the graph independently, empowering them to deliver autonomously and incrementally. Instances of @apollo/query-planner >=2.0.0 and <2.8.5 are impacted by a denial-of-service vulnerability. @apollo/gateway versions >=2.0.0 and < 2.8.5 and Apollo Router <1.52.1 are also impacted through their use of @apollo/query-panner. If @apollo/query-planner is asked to plan a sufficiently complex query, it may loop infinitely and never complete. This results in unbounded memory consumption and either a crash or out-of-memory (OOM) termination. This issue can be triggered if you have at least one non-@key field that can be resolved by multiple subgraphs. To identify these shared fields, the schema for each subgraph must be reviewed. The mechanism to identify shared fields varies based on the version of Federation your subgraphs are using. You can check if your subgraphs are using Federation 1 or Federation 2 by reviewing their schemas. Federation 2 subgraph schemas will contain a @link directive referencing the version of Federation being used while Federation 1 subgraphs will not. For example, in a Federation 2 subgraph, you will find a line like @link(url: "https://specs.apollo.dev/federation/v2.0"). If a similar @link directive is not present in your subgraph schema, it is using Federation 1. Note that a supergraph can contain a mix of Federation 1 and Federation 2 subgraphs. This issue results from the Apollo query planner attempting to use a Number exceeding Javascript's Number.MAX_VALUE in some cases. In Javascript, Number.MAX_VALUE is (2^1024 - 2^971). When the query planner receives an inbound graphql request, it breaks the query into pieces and for each piece, generates a list of potential execution steps to solve the piece. These candidates represent the steps that the query planner will take to satisfy the pieces of the larger query. As part of normal operations, the query planner requires and calculates the number of possible query plans for the total query. That is, it needs the product of the number of query plan candidates for each piece of the query. Under normal circumstances, after generating all query plan candidates and calculating the number of all permutations, the query planner moves on to stack rank candidates and prune less-than-optimal options. In particularly complex queries, especially those where fields can be solved through multiple subgraphs, this can cause the number of all query plan permutations to balloon. In worst-case scenarios, this can end up being a number larger than Number.MAX_VALUE. In Javascript, if Number.MAX_VALUE is exceeded, Javascript represents the value as "infinity". If the count of candidates is evaluated as infinity, the component of the query planner responsible for pruning less-than-optimal query plans does not actually prune candidates, causing the query planner to evaluate many orders of magnitude more query plan candidates than necessary. This issue has been addressed in @apollo/query-planner v2.8.5, @apollo/gateway v2.8.5, and Apollo Router v1.52.1. Users are advised to upgrade. This issue can be avoided by ensuring there are no fields resolvable from multiple subgraphs. If all subgraphs are using Federation 2, you can confirm that you are not impacted by ensuring that none of your subgraph schemas use the @shareable directive. If you are using	2024-08-27	7.5	CVE-2024-43414 security-advisories@github.com security-advisories@github.com security-advisories@github.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Federation 1 subgraphs, you will need to validate that there are no fields resolvable by multiple subgraphs.			
apollographql--router	The Apollo Router Core is a configurable, high-performance graph router written in Rust to run a federated supergraph that uses Apollo Federation 2. Instances of the Apollo Router running versions >=1.21.0 and < 1.52.1 are impacted by a denial of service vulnerability if _all_ of the following are true: 1. The Apollo Router has been configured to support [External Coprocessing](https://www.apollographql.com/docs/router/customizations/coprocessor). 2. The Apollo Router has been configured to send request bodies to coprocessors. This is a non-default configuration and must be configured intentionally by administrators. Instances of the Apollo Router running versions >=1.7.0 and <1.52.1 are impacted by a denial-of-service vulnerability if all of the following are true: 1. Router has been configured to use a custom-developed Native Rust Plugin. 2. The plugin accesses Request.router_request in the RouterService layer. 3. You are accumulating the body from Request.router_request into memory. If using an impacted configuration, the Router will load entire HTTP request bodies into memory without respect to other HTTP request size-limiting configurations like limits.http_max_request_bytes. This can cause the Router to be out-of-memory (OOM) terminated if a sufficiently large request is sent to the Router. By default, the Router sets limits.http_max_request_bytes to 2 MB. If you have an impacted configuration as defined above, please upgrade to at least Apollo Router 1.52.1. If you cannot upgrade, you can mitigate the denial-of-service opportunity impacting External Coprocessors by setting the coprocessor.router.request.body configuration option to false. Please note that changing this configuration option will change the information sent to any coprocessors you have configured and may impact functionality implemented by those coprocessors. If you have developed a Native Rust Plugin and cannot upgrade, you can update your plugin to either not accumulate the request body or enforce a maximum body size limit. You can also mitigate this issue by limiting HTTP body payload sizes prior to the Router (e.g., in a proxy or web application firewall appliance).	2024-08-27	7.5	CVE-2024-43783 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
bdthemes--Ultimate Store Kit Elementor Addons, Woocommerce Builder, EDD Builder, Elementor Store Builder, Product Grid, Product Table, Woocommerce Slider	The Ultimate Store Kit Elementor Addons, Woocommerce Builder, EDD Builder, Elementor Store Builder, Product Grid, Product Table, Woocommerce Slider plugin is vulnerable to PHP Object Injection via deserialization of untrusted input via the _ultimate_store_kit_wishlist cookie in versions up to , and including, 2.0.3. This makes it possible for an unauthenticated attacker to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker or above to delete arbitrary files, retrieve sensitive data, or execute code.	2024-08-28	9.8	CVE-2024-8030 security@wordfence.com security@wordfence.com
Beckhoff--IPC Diagnostics package	The IPC-Diagnostics package included in TwinCAT/BSD is vulnerable to a local authentication bypass by a low privileged attacker.	2024-08-27	7.8	CVE-2024-41173 info@cert.vde.com
Beckhoff--IPC Diagnostics package	The IPC-Diagnostics package in TwinCAT/BSD is susceptible to improper input neutralization by a low-privileged local attacker.	2024-08-27	7.3	CVE-2024-41174 info@cert.vde.com
brainlowcode -- brain_low-code	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), CWE - 564 - SQL Injection: Hibernate vulnerability in Brain Information Technologies Inc. Brain Low-Code allows SQL Injection.This issue affects Brain Low-Code: before 2.1.0.	2024-08-27	9.8	CVE-2024-7071 iletisim@usom.gov.tr
chartist -- chartist	Chartist 1.x through 1.3.0 allows Prototype Pollution via the extend function.	2024-08-29	9.8	CVE-2024-45435 cve@mitre.org cve@mitre.org
CIGES--CIGESv2	SQL injection vulnerability in ATISolutions CIGES affecting versions lower than 2.15.5. This vulnerability allows a remote attacker to send a specially crafted SQL query to the /modules/ajaxServiciosCentro.php point in the idCentro parameter and retrieve all the information stored in the database.	2024-08-26	9.8	CVE-2024-8161 cve-coordination@incibe.es

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cisco--Cisco NX-OS Software	A vulnerability in the DHCPv6 relay agent of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of specific fields in a DHCPv6 RELAY-REPLY message. An attacker could exploit this vulnerability by sending a crafted DHCPv6 packet to any IPv6 address that is configured on an affected device. A successful exploit could allow the attacker to cause the dhcp_snoop process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition.	2024-08-28	8.6	CVE-2024-20446 ykramarz@cisco.com
code-projects--Blood Bank System	A vulnerability, which was classified as critical, was found in code-projects Blood Bank System 1.0. Affected is an unknown function of the file /login.php of the component Login Page. The manipulation of the argument user leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-26	7.3	CVE-2024-8173 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
code-projects--Hospital Management System	A vulnerability was found in code-projects Hospital Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file index.php of the component Login. 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.	2024-09-01	7.3	CVE-2024-8368 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
cridio -- listingpro	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CridioStudio ListingPro allows SQL Injection.This issue affects ListingPro: from n/a through 2.9.4.	2024-08-29	9.8	CVE-2024-38795 audit@patchstack.com
cridio -- listingpro	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CridioStudio ListingPro.This issue affects ListingPro: from n/a through 2.9.4.	2024-08-29	9.8	CVE-2024-39622 audit@patchstack.com
cridio -- listingpro	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CridioStudio ListingPro allows SQL Injection.This issue affects ListingPro: from n/a through 2.9.4.	2024-08-29	8.8	CVE-2024-39620 audit@patchstack.com
Dell--Dell Client Platform BIOS	Dell Client Platform BIOS contains a Use of Default Cryptographic Key Vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Secure Boot bypass and arbitrary code execution.	2024-08-28	8.2	CVE-2024-39584 security_alert@emc.com
Dinesh Karki--WP Armour Extended	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Dinesh Karki WP Armour Extended.This issue affects WP Armour Extended: from n/a through 1.26.	2024-08-29	7.1	CVE-2024-43948 audit@patchstack.com
dlink -- dir-846w_firmware	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via the tomography_ping_address parameter in /HNAP1/ interface.	2024-08-27	9.8	CVE-2024-41622 cve@mitre.org cve@mitre.org cve@mitre.org
dlink -- dir-846w_firmware	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via the lan(0)_dhcps_staticlist parameter. This vulnerability is exploited via a crafted POST request.	2024-08-27	9.8	CVE-2024-44341 cve@mitre.org cve@mitre.org cve@mitre.org
dlink -- dir-846w_firmware	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via the wl(0).(0)_ssid parameter. This vulnerability is exploited via a crafted POST request.	2024-08-27	9.8	CVE-2024-44342 cve@mitre.org cve@mitre.org cve@mitre.org
dlink -- dir-846w_firmware	D-Link DIR-846W A1 FW100A43 was discovered to contain a remote command execution (RCE) vulnerability via keys smartqos_express_devices and smartqos_normal_devices in SetSmartQoSSettings.	2024-08-27	8.8	CVE-2024-44340 cve@mitre.org cve@mitre.org cve@mitre.org
dlink -- dns-315l_firmware	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and	2024-08-27	9.8	CVE-2024-8210 cna@vuldb.com cna@vuldb.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.			cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
dlink -- dns-315l_firmware	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-27	9.8	CVE-2024-8211 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
dlink -- dns-315l_firmware	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-27	9.8	CVE-2024-8212 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
dlink -- dns-315l_firmware	A vulnerability classified as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-27	9.8	CVE-2024-8213 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
dlink -- dns-315l_firmware	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-27	9.8	CVE-2024-8214 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
donbermoy -- e-commerce_website	A vulnerability has been found in SourceCodester E-Commerce Website 1.0 and classified as critical. This vulnerability affects unknown code of the file /Admin/registration.php. The manipulation of the argument fname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-27	9.8	CVE-2024-8217 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
E4J s.r.l.--VikRentCar	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in E4J s.R.L. VikRentCar allows SQL Injection.This issue affects VikRentCar: from n/a through 1.4.0.	2024-08-29	9.3	CVE-2024-39653 audit@patchstack.com
Easy Digital Downloads--Easy Digital Downloads	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Easy Digital Downloads allows SQL Injection.This issue affects Easy Digital Downloads: from n/a through 3.2.12.	2024-08-29	9.3	CVE-2024-5057 audit@patchstack.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ELECOM CO.,LTD.--WAB-I1750-PS	Missing authentication vulnerability exists in Telnet function of WAB-I1750-PS v1.5.10 and earlier. When Telnet function of the product is enabled, a remote attacker may login to the product without authentication and alter the product's settings.	2024-08-30	8.1	CVE-2024-39300 vultures@jpcert.or.jp vultures@jpcert.or.jp
etoilewebdesign -- front_end_users	The Front End Users plugin for WordPress is vulnerable to time-based SQL Injection via the 'order' parameter in all versions up to, and including, 3.2.28 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-08-29	8.8	CVE-2024-7607 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
eyecix--JobSearch	Deserialization of Untrusted Data vulnerability in eyecix JobSearch allows Object Injection.This issue affects JobSearch: from n/a through 2.5.3.	2024-08-29	9.8	CVE-2024-43931 audit@patchstack.com
fabianros -- job_portal	A vulnerability was found in code-projects Job Portal 1.0. It has been classified as critical. Affected is an unknown function of the file /forget.php. The manipulation of the argument email/mobile leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-26	9.8	CVE-2024-8167 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
fabianros -- online_bus_reservation_site	A vulnerability was found in code-projects Online Bus Reservation Site 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation of the argument Username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-26	9.8	CVE-2024-8168 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
fabianros -- online_quiz_site	A vulnerability was found in code-projects Online Quiz Site 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file signupuser.php. The manipulation of the argument lid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-26	9.8	CVE-2024-8169 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
fabianros -- online_quiz_site	A vulnerability was found in code-projects Online Quiz Site 1.0 and classified as critical. This issue affects some unknown processing of the file index.php. The manipulation of the argument loginid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-27	9.8	CVE-2024-8218 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
fabianros -- responsive_hotel_site	A vulnerability was found in code-projects Responsive Hotel Site 1.0. It has been classified as critical. Affected is an unknown function of the file index.php. The manipulation of the argument name/phone/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.	2024-08-27	9.8	CVE-2024-8219 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
fastcom -- fw300r_firmware	A stack overflow in FAST FW300R v1.3.13 Build 141023 Rel.61347n allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via a crafted file path.	2024-08-26	9.8	CVE-2024-41285 cve@mitre.org cve@mitre.org cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
feehi -- feehicms	A vulnerability, which was classified as critical, was found in FeehiCMS up to 2.1.1. This affects the function update of the file /admin/index.php?r=friendly-link%2Fupdate. The manipulation of the argument FriendlyLink[image] leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-29	9.8	CVE-2024-8294 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
feehi -- feehicms	A vulnerability has been found in FeehiCMS up to 2.1.1 and classified as critical. This vulnerability affects the function createBanner of the file /admin/index.php?r=banner%2Fbanner-create. The manipulation of the argument BannerForm[img] leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-29	9.8	CVE-2024-8295 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
feehi -- feehicms	A vulnerability was found in FeehiCMS up to 2.1.1 and classified as critical. This issue affects the function insert of the file /admin/index.php?r=user%2Fcreate. The manipulation of the argument User[avatar] leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-29	9.8	CVE-2024-8296 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
flowiseai -- flowise	An Authentication Bypass vulnerability exists in Flowise version 1.8.2. This could allow a remote, unauthenticated attacker to access API endpoints as an administrator and allow them to access restricted functionality.	2024-08-27	8.1	CVE-2024-8181 vulnreport@tenable.com
flowiseai -- flowise	An Unauthenticated Denial of Service (DoS) vulnerability exists in Flowise version 1.8.2 leading to a complete crash of the instance running a vulnerable version due to improper handling of user supplied input to the "/api/v1/get-upload-file" api endpoint.	2024-08-27	7.5	CVE-2024-8182 vulnreport@tenable.com
Fonts Plugin--Fonts	Cross-Site Request Forgery (CSRF) vulnerability in Fonts Plugin Fonts allows Stored XSS.This issue affects Fonts: from n/a through 3.7.7.	2024-08-26	7.1	CVE-2024-43301 audit@patchstack.com
fortra -- filecatalyst_workflow	The default credentials for the setup HSQL database (HSQLDB) for FileCatalyst Workflow are published in a vendor knowledgebase article. Misuse of these credentials could lead to a compromise of confidentiality, integrity, or availability of the software. The HSQLDB is only included to facilitate installation, has been deprecated, and is not intended for production use per vendor guides. However, users who have not configured FileCatalyst Workflow to use an alternative database per recommendations are vulnerable to attack from any source that can reach the HSQLDB.	2024-08-27	9.8	CVE-2024-6633 df4dee71-de3a-4139-9588-11b62fe6c0ff
fortra -- filecatalyst_workflow	A vulnerability exists in FileCatalyst Workflow whereby a field accessible to the super admin can be used to perform an SQL injection attack which can lead to a loss of confidentiality, integrity, and availability.	2024-08-27	7.2	CVE-2024-6632 df4dee71-de3a-4139-9588-11b62fe6c0ff
funnelforms--Interactive Contact Form and Multi Step Form Builder with Drag & Drop Editor Funnelforms Free	The Funnelforms Free plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'af2_add_font' function in all versions up to, and including, 3.7.3.2. This makes it possible for authenticated attackers, with administrator-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-08-28	7.2	CVE-2024-6311 security@wordfence.com security@wordfence.com security@wordfence.com
Gether Technology--6SHR System	6SHR system from Gether Technology does not properly validate the specific page parameter, allowing remote attackers with regular privilege to inject SQL command to read, modify, and delete database contents.	2024-08-30	8.8	CVE-2024-8329 twcert@cert.org.tw twcert@cert.org.tw
Gether Technology--6SHR System	6SHR system from Gether Technology does not properly validate uploaded file types, allowing remote attackers with regular privileges to upload web shell scripts and use them to execute arbitrary system commands on the server.	2024-08-30	8.8	CVE-2024-8330 twcert@cert.org.tw twcert@cert.org.tw
getkirby--kirby	Kirby is a CMS targeting designers and editors. Kirby allows to restrict the permissions of specific user roles. Users of that role can only perform permitted	2024-08-29	8.1	CVE-2024-41964 security-

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	actions. Permissions for creating and deleting languages have already existed and could be configured, but were not enforced by Kirby's frontend or backend code. A permission for updating existing languages has not existed before the patched versions. So disabling the languages.* wildcard permission for a role could not have prohibited updates to existing language definitions. The missing permission checks allowed attackers with Panel access to manipulate the language definitions. The problem has been patched in Kirby 3.6.6.6, Kirby 3.7.5.5, Kirby 3.8.4.4, Kirby 3.9.8.2, Kirby 3.10.1.1, and Kirby 4.3.1. Please update to one of these or a later version to fix the vulnerability. There are no known workarounds for this vulnerability.			advisories@github.com security-advisories@github.com
gitapp -- dingfanzu	A vulnerability was found in dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /ajax/checkin.php. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-29	9.8	CVE-2024-8301 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
google -- chrome	Heap buffer overflow in Skia in Google Chrome prior to 128.0.6613.113 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-08-28	8.8	CVE-2024-8193 chrome-cve-admin@google.com chrome-cve-admin@google.com
google -- chrome	Type Confusion in V8 in Google Chrome prior to 128.0.6613.113 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-08-28	8.8	CVE-2024-8194 chrome-cve-admin@google.com chrome-cve-admin@google.com
google -- chrome	Heap buffer overflow in Skia in Google Chrome prior to 128.0.6613.113 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-08-28	8.8	CVE-2024-8198 chrome-cve-admin@google.com chrome-cve-admin@google.com
gVectors Team--wpForo Forum	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in gVectors Team wpForo Forum.This issue affects wpForo Forum: from n/a through 2.3.4.	2024-08-26	7.5	CVE-2024-43289 audit@patchstack.com
gzequan -- eq_enterprise_management_system	An issue in EQ Enterprise Management System before v2.0.0 allows attackers to execute a directory traversal via crafted requests.	2024-08-28	9.8	CVE-2024-44761 cve@mitre.org
Hillstone Networks--Hillstone Networks Web Application Firewall	Improper Input Validation vulnerability in Hillstone Networks Hillstone Networks Web Application Firewall on 5.5R6 allows Command Injection.This issue affects Hillstone Networks Web Application Firewall: fromÂ 5.5R6-2.6.7 through 5.5R6-2.8.13.	2024-08-26	9.8	CVE-2024-8073 sec@hillstonenet.com
Hitachi--Hitachi Ops Center Common Services	Authentication Bypass vulnerability in Hitachi Ops Center Common Services.This issue affects Hitachi Ops Center Common Services: from 10.9.3-00 before 11.0.2-01.	2024-08-27	7.8	CVE-2024-7125 hirt@hitachi.co.jp
hitachienergy -- microscada_x_sys600	The product does not validate any query towards persistent data, resulting in a risk of injection attacks.	2024-08-27	9.8	CVE-2024-4872 cybersecurity@hitachienergy.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hitachienergy -- microscada_x_sys600	The product exposes a service that is intended for local only to all network interfaces without any authentication.	2024-08-27	9.8	CVE-2024-7940 cybersecurity@hitachienergy.com
hitachienergy -- microscada_x_sys600	The product allows user input to control or influence paths or file names that are used in filesystem operations, allowing the attacker to access or modify system files or other files that are critical to the application.	2024-08-27	8.8	CVE-2024-3980 cybersecurity@hitachienergy.com
hitachienergy -- microscada_x_sys600	An attacker with local access to machine where MicroSCADA X SYS600 is installed, could enable the session logging supporting the product and try to exploit a session hijacking of an already established session. By default, the session logging level is not enabled and only users with administrator rights can enable it.	2024-08-27	8.2	CVE-2024-3982 cybersecurity@hitachienergy.com
hornero--Clean Login	The Clean Login plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.14.5 via the 'template' attribute of the clean-login-register shortcode. 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.	2024-08-30	8.8	CVE-2024-8252 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
HP Inc.--HP Security Manager	HP Security Manager is potentially vulnerable to Remote Code Execution as a result of code vulnerability within the product's solution open-source libraries.	2024-08-27	9.8	CVE-2024-7720 hp-security-alert@hp.com
HWA JIUH DIGITAL TECHNOLOGY--Easy test Online Learning and Testing Platform	Easy test Online Learning and Testing Platform fromÂ HWA JIUH DIGITAL TECHNOLOGY does not properly validate a specific page parameter, allowing remote attackers with regular privilege to inject arbitrary SQL commands to read, modify, and delete database contents.	2024-08-30	8.8	CVE-2024-8327 twcert@cert.org.tw twcert@cert.org.tw
IBM--Sterling Connect:Direct Web Services	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 uses default credentials for potentially critical functionality.	2024-08-31	8.1	CVE-2024-39747 psirt@us.ibm.com psirt@us.ibm.com
in2code -- powermail	An issue was discovered in powermail extension through 12.3.5 for TYPO3. Several actions in the OutputController can directly be called, due to missing or insufficiently implemented access checks, resulting in Broken Access Control. Depending on the configuration of the Powermail Frontend plugins, an unauthenticated attacker can exploit this to edit, update, delete, or export data of persisted forms. This can only be exploited when the Powermail Frontend plugins are used. The fixed versions are 7.5.0, 8.5.0, 10.9.0, and 12.4.0.	2024-08-29	9.8	CVE-2024-45233 cve@mitre.org
jpillora--chisel	Chisel is a fast TCP/UDP tunnel, transported over HTTP, secured via SSH. The Chisel server doesn't ever read the documented `AUTH` environment variable used to set credentials, which allows any unauthenticated user to connect, even if credentials were set. Anyone running the Chisel server that is using the `AUTH` environment variable to specify credentials to authenticate against is affected by this vulnerability. Chisel is often used to provide an entrypoint to a private network, which means services that are gated by Chisel may be affected. Additionally, Chisel is often used for exposing services to the internet. An attacker could MITM requests by connecting to a Chisel server and requesting to forward traffic from a remote port. This issue has been addressed in release version 1.10.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-08-26	8.6	CVE-2024-43798 security-advisories@github.com
kitsada8621 -- digital_library_management_system	A vulnerability was found in kitsada8621 Digital Library Management System 1.0. It has been classified as problematic. Affected is the function JwtRefreshAuth of the file middleware/jwt_refresh_token_middleware.go. The manipulation of the argument Authorization leads to improper output neutralization for logs. It is possible to launch the attack remotely. The name of the patch is 81b3336b4c9240f0bf50c13cb8375cf860d945f1. It is recommended to apply a patch to fix this issue.	2024-08-29	7.5	CVE-2024-8297 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: mm: list_lru: fix UAF for memory cgroup The mem_cgroup_from_slab_obj() is supposed to be called under rcu lock or cgroup_mutex or others which could prevent returned memcg from being freed. Fix it by adding missing rcu read lock. Found by code	2024-08-26	7.8	CVE-2024-43888 416baaa9-dc9f-4396-8d5f-8c081fb06d67

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	inspection. [songmuchun@bytedance.com: only grab rcu lock when necessary, per Vlastimil] Link: https://lkml.kernel.org/r/20240801024603.1865-1-songmuchun@bytedance.com			416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: media: xc2028: avoid use-after-free in load_firmware_cb() syzkaller reported use-after-free in load_firmware_cb() [1]. The reason is because the module allocated a struct tuner in tuner_probe(), and then the module initialization failed, the struct tuner was released. A worker which created during module initialization accesses this struct tuner later, it caused use-after-free. The process is as follows: task-6504 worker_thread tuner_probe <= alloc dvb_frontend [2] ... request_firmware_nowait <= create a worker ... tuner_remove <= free dvb_frontend ... request_firmware_work_func <= the firmware is ready load_firmware_cb <= but now the dvb_frontend has been freed To fix the issue, check the dvd_frontend in load_firmware_cb(), if it is null, report a warning and just return. [1]: == BUG: KASAN: use-after-free in load_firmware_cb+0x1310/0x17a0 Read of size 8 at addr ffff8000d7ca2308 by task kworker/2:3/6504 Call trace: load_firmware_cb+0x1310/0x17a0 request_firmware_work_func+0x128/0x220 process_one_work+0x770/0x1824 worker_thread+0x488/0xea0 kthread+0x300/0x430 ret_from_fork+0x10/0x20 Allocated by task 6504: kzalloc tuner_probe+0xb0/0x1430 i2c_device_probe+0x92c/0xaf0 really_probe+0x678/0xcd0 driver_probe_device+0x280/0x370 __device_attach_driver+0x220/0x330 bus_for_each_drv+0x134/0x1c0 __device_attach+0x1f4/0x410 device_initial_probe+0x20/0x30 bus_probe_device+0x184/0x200 device_add+0x924/0x12c0 device_register+0x24/0x30 i2c_new_device+0x4e0/0xc44 v4l2_i2c_new_subdev_board+0xbc/0x290 v4l2_i2c_new_subdev+0xc8/0x104 em28xx_v4l2_init+0x1dd0/0x3770 Freed by task 6504: kfree+0x238/0x4e4 tuner_remove+0x144/0x1c0 i2c_device_remove+0xc8/0x290 __device_release_driver+0x314/0x5fc device_release_driver+0x30/0x44 bus_remove_device+0x244/0x490 device_del+0x350/0x900 device_unregister+0x28/0xd0 i2c_unregister_device+0x174/0x1d0 v4l2_device_unregister+0x224/0x380 em28xx_v4l2_init+0x1d90/0x3770 The buggy address belongs to the object at ffff8000d7ca2000 which belongs to the cache kmalloc-2k of size 2048 The buggy address is located 776 bytes inside of 2048-byte region [ffff8000d7ca2000, ffff8000d7ca2800) The buggy address belongs to the page: page:ffff7fe00035f280 count:1 mapcount:0 mapping:ffff8000c001f000 index:0x0 flags: 0x7ff800000000100(slab) raw: 07ff800000000100 ffff7fe00049d880 0000000300000003 ffff8000c001f000 raw: 0000000000000000 0000000080100010 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff8000d7ca2200: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8000d7ca2280: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb >ffff8000d7ca2300: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ^ ffff8000d7ca2380: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ffff8000d7ca2400: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb == [2] Actually, it is allocated for struct tuner, and dvb_frontend is inside.	2024-08-26	7.8	CVE-2024-43900 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: idpf: fix UAFs when destroying the queues The second tagged commit started sometimes (very rarely, but possible) throwing WARNs from net/core/page_pool.c:page_pool_disable_direct_recycling(). Turned out idpf frees interrupt vectors with embedded NAPIs *before* freeing the queues making page_pools' NAPI pointers lead to freed memory before these pools are destroyed by libeth. It's not clear whether there are other accesses to the freed vectors when destroying the queues, but anyway, we usually free queue/interrupt vectors only when the queues are destroyed and the NAPIs are guaranteed to not be referenced anywhere. Invert the allocation and freeing logic making queue/interrupt vectors be allocated first and freed last. Vectors don't require queues to be present, so this is safe. Additionally, this change allows to remove that useless queue->q_vector pointer cleanup, as vectors are still valid when freeing the queues (+ both are freed within one function, so it's not clear why nullify the pointers at all).	2024-08-26	7.8	CVE-2024-44932 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net: bridge: mcast: wait for previous gc cycles when removing port syzbot hit a use-after-free[1] which is caused because the bridge doesn't make sure that all previous	2024-08-26	7.8	CVE-2024-44934 416baaa9-dc9f-4396-8d5f-

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	garbage has been collected when removing a port. What happens is: CPU 1 CPU 2 start gc cycle remove port acquire gc lock first wait for lock call br_multicasg_gc() directly acquire lock now but free port the port can be freed while grp timers still running Make sure all previous gc cycles have finished by using flush_work before freeing the port. [1] BUG: KASAN: slab-use-after-free in br_multicast_port_group_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 Read of size 8 at addr ffff888071d6d000 by task syz.5.1232/9699 CPU: 1 PID: 9699 Comm: syz.5.1232 Not tainted 6.10.0-rc5-syzkaller-00021-g24ca36a562d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/07/2024 Call Trace: <IRQ> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:114 print_address_description mm/kasan/report.c:377 [inline] print_report+0xc3/0x620 mm/kasan/report.c:488 kasan_report+0xd9/0x110 mm/kasan/report.c:601 br_multicast_port_group_expired+0x4c0/0x550 net/bridge/br_multicast.c:861 call_timer_fn+0x1a3/0x610 kernel/time/timer.c:1792 expire_timers kernel/time/timer.c:1843 [inline] __run_timers+0x74b/0xaf0 kernel/time/timer.c:2417 __run_timer_base kernel/time/timer.c:2428 [inline] __run_timer_base kernel/time/timer.c:2421 [inline] run_timer_base+0x111/0x190 kernel/time/timer.c:2437			8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to do sanity check on F2FS_INLINE_DATA flag in inode during GC syzbot reports a f2fs bug as below: ------------[cut here]------------ kernel BUG at fs/f2fs/inline.c:258! CPU: 1 PID: 34 Comm: kworker/u8:2 Not tainted 6.9.0-rc6-syzkaller-00012-g9e4bc4bcae01 #0 RIP: 0010:f2fs_write_inline_data+0x781/0x790 fs/f2fs/inline.c:258 Call Trace: f2fs_write_single_data_page+0xb65/0x1d60 fs/f2fs/data.c:2834 f2fs_write_cache_pages fs/f2fs/data.c:3133 [inline] __f2fs_write_data_pages fs/f2fs/data.c:3288 [inline] f2fs_write_data_pages+0x1efe/0x3a90 fs/f2fs/data.c:3315 do_writepages+0x35b/0x870 mm/page-writeback.c:2612 __writeback_single_inode+0x165/0x10b0 fs/fs-writeback.c:1650 writeback_sb_inodes+0x905/0x1260 fs/fs-writeback.c:1941 wb_writeback+0x457/0xce0 fs/fs-writeback.c:2117 wb_do_writeback fs/fs-writeback.c:2264 [inline] wb_workfn+0x410/0x1090 fs/fs-writeback.c:2304 process_one_work kernel/workqueue.c:3254 [inline] process_scheduled_works+0xa12/0x17c0 kernel/workqueue.c:3335 worker_thread+0x86d/0xd70 kernel/workqueue.c:3416 kthread+0x2f2/0x390 kernel/kthread.c:388 ret_from_fork+0x4d/0x80 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:244 The root cause is: inline_data inode can be fuzzed, so that there may be valid blkaddr in its direct node, once f2fs triggers background GC to migrate the block, it will hit f2fs_bug_on() during dirty page writeback. Let's add sanity check on F2FS_INLINE_DATA flag in inode during GC, so that, it can forbid migrating inline_data inode's data block for fixing.	2024-08-26	7.8	CVE-2024-44942 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
lopalopa -- music_management_system	A Cross-Site Request Forgery (CSRF) vulnerability was found in Kashipara Music Management System v1.0 via a crafted request to the /music/ajax.php?action=save_user page.	2024-08-28	8	CVE-2024-42793 cve@mitre.org cve@mitre.org
lopalopa -- responsive_school_management_system	A SQL injection vulnerability in /smsa/admin_login.php in Kashipara Responsive School Management System v3.2.0 allows an attacker to execute arbitrary SQL commands via the "username" parameter of the Admin Login Page	2024-08-28	7.2	CVE-2024-41236 cve@mitre.org cve@mitre.org
Magic Post Thumbnail--Magic Post Thumbnail	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Magic Post Thumbnail allows Reflected XSS.This issue affects Magic Post Thumbnail: from n/a through 5.2.9.	2024-08-29	7.1	CVE-2024-43921 audit@patchstack.com
ManageEngine--Endpoint Central	Zohocorp ManageEngine Endpoint Central affected byÂ Incorrect authorization vulnerability while isolating the devices.This issue affects Endpoint Central: before 11.3.2406.08 and before 11.3.2400.15	2024-08-30	7.6	CVE-2024-38868 0fc0942c-577d-436f-ae8e-945763c79b02
ManageEngine--Exchange Reporter Plus	Zohocorp ManageEngine Exchange Reporter Plus versions beforeÂ 5715 are vulnerable toÂ SQL Injection in the reports module.	2024-08-30	8.3	CVE-2024-6204 0fc0942c-577d-436f-ae8e-945763c79b02

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ManageEngine--Password Manager Pro	ZohocorpÂ ManageEngine Password Manager Pro versions before 12431 andÂ ManageEngine PAM360 versionsÂ before 7001 are affected byÂ authenticated SQL Injection vulnerability via a global search option.	2024-08-28	8.3	CVE-2024-5546 0fc0942c-577d-436f-ae8e-945763c79b02
maxfoundry--Media Library Folders	The Media Library Folders plugin for WordPress is vulnerable to second order SQL Injection via the 'sort_type' parameter of the 'mlf_change_sort_type' AJAX action in all versions up to, and including, 8.2.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with 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.	2024-08-29	9.8	CVE-2024-7857 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
menulux -- managment_portal	Improper Privilege Management vulnerability in Menulux Information Technologies Managment Portal allows Collect Data as Provided by Users.This issue affects Managment Portal: through 21.05.2024.	2024-08-29	9.8	CVE-2024-4428 iletisim@usom.gov.tr
meshtastic--firmware	Meshtastic device firmware is a firmware for meshtastic devices to run an open source, off-grid, decentralized, mesh network built to run on affordable, low-power devices. Meshtastic device firmware is subject to a denial of serivce vulnerability in MQTT handling, fixed in version 2.4.1 of the Meshtastic firmware and on the Meshtastic public MQTT Broker. It's strongly suggested that all users of Meshtastic, particularly those that connect to a privately hosted MQTT server, update to this or a more recent stable version right away. There are no known workarounds for this vulnerability.	2024-08-27	7.5	CVE-2024-45038 security-advisories@github.com
mndpsingh287--Theme Editor	The Theme Editor plugin for WordPress is vulnerable to deserialization of untrusted input via the 'images_array' parameter in versions up to, and including 2.8. This makes it possible for authenticated attackers with administrative privileges to call files using a PHAR wrapper that will deserialize and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.	2024-08-29	7.2	CVE-2022-2440 security@wordfence.com security@wordfence.com security@wordfence.com
MuffinGroup--Betheme	The Betheme theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 27.5.6 via deserialization of untrusted input of the 'mfn-page-items' post meta value. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-08-30	8.8	CVE-2024-2694 security@wordfence.com security@wordfence.com
n/a--n/a	An SEH-based buffer overflow in the BPQ32 HTTP Server in BPQ32 6.0.24.1 allows remote attackers with access to the Web Terminal to achieve remote code execution via an HTTP POST /TermInput request.	2024-08-26	9.8	CVE-2024-34087 cve@mitre.org cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	TOTOLINK AC1200 Wireless Router A3002RU V2.1.1-B20230720.1011 is vulnerable to Buffer Overflow. The formWlEncrypt CGI handler in the boa program fails to limit the length of the wlan_ssid field from user input. This allows attackers to craft malicious HTTP requests by supplying an excessively long value for the wlan_ssid field, leading to a stack overflow. This can be further exploited to execute arbitrary commands or launch denial-of-service attacks.	2024-08-28	9.8	CVE-2024-34198 cve@mitre.org
n/a--n/a	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\manageFilesFolders.php	2024-08-29	9.8	CVE-2024-41361 cve@mitre.org
n/a--n/a	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\trackEdit.php	2024-08-29	9.8	CVE-2024-41364 cve@mitre.org
n/a--n/a	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\userScripts.php	2024-08-29	9.8	CVE-2024-41366 cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\api\playlist\appendFileToPlaylist.php	2024-08-29	9.8	CVE-2024-41367 cve@mitre.org
n/a--n/a	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\inc.setWlanIpMail.php	2024-08-29	9.8	CVE-2024-41368 cve@mitre.org
n/a--n/a	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\inc.setWifi.php	2024-08-29	9.8	CVE-2024-41369 cve@mitre.org
n/a--n/a	Organizr v1.90 was discovered to contain a SQL injection vulnerability via chat/setlike.php.	2024-08-29	9.8	CVE-2024-41370 cve@mitre.org cve@mitre.org
n/a--n/a	Organizr v1.90 was discovered to contain a SQL injection vulnerability via chat/settyping.php.	2024-08-29	9.8	CVE-2024-41372 cve@mitre.org cve@mitre.org
n/a--n/a	SeaCMS v12.9 has a SQL injection vulnerability in the key parameter of /js/player/dmplayer/dmku/index.php?ac=so.	2024-08-26	9.8	CVE-2024-41444 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	Beijing Digital China Cloud Technology Co., Ltd. DCME-320 v.7.4.12.60 has a command execution vulnerability, which can be exploited to obtain device administrator privileges via the getVar function in the code/function/system/tool/ping.php file.	2024-08-28	9.8	CVE-2024-42905 cve@mitre.org cve@mitre.org
n/a--n/a	An arbitrary file write issue in the exfiltration endpoint in BYOB (Build Your Own Botnet) 2.0 allows attackers to overwrite SQLite databases and bypass authentication via an unauthenticated HTTP request with a crafted parameter. This occurs in file_add in api/files/routes.py.	2024-08-26	9.8	CVE-2024-45256 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	A SQL injection vulnerability in the poll component in SkySystem Arfa-CMS before 5.1.3124 allows remote attackers to execute arbitrary SQL commands via the psid parameter.	2024-08-26	9.8	CVE-2024-45265 cve@mitre.org cve@mitre.org
n/a--n/a	The App::cpanminus package through 1.7047 for Perl downloads code via insecure HTTP, enabling code execution for network attackers.	2024-08-27	9.8	CVE-2024-45321 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	One Identity Safeguard for Privileged Passwords before 7.5.2 allows unauthorized access because of an issue related to cookies. This only affects virtual appliance installations (VMware or HyperV). The fixed versions are 7.0.5.1 LTS, 7.4.2, and 7.5.2.	2024-08-30	9.8	CVE-2024-45488 cve@mitre.org cve@mitre.org
n/a--n/a	An issue was discovered in libexpat before 2.6.3. xmlparse.c does not reject a negative length for XML_ParseBuffer.	2024-08-30	9.8	CVE-2024-45490 cve@mitre.org cve@mitre.org
n/a--n/a	A weak password requirement issue was discovered in Teldats Router RS123, RS123w allows a remote attacker to escalate privileges	2024-08-27	8	CVE-2022-39997 cve@mitre.org cve@mitre.org
n/a--n/a	A Cross-Site Request Forgery (CSRF) vulnerability was found in Kashipara Music Management System v1.0 via /music/ajax.php?action=delete_genre.	2024-08-26	8.8	CVE-2024-42791 cve@mitre.org cve@mitre.org
n/a--n/a	Validating the order of the public keys in the Diffie-Hellman Key Agreement Protocol, when an approved safe prime is used, allows remote attackers (from the client side) to trigger unnecessarily expensive server-side DHE modular-exponentiation calculations. The client may cause asymmetric resource consumption. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE and validate the order of the public key.	2024-08-26	7.5	CVE-2024-41996 cve@mitre.org cve@mitre.org cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	A reflected cross-site scripting (XSS) vulnerability in the tag parameter in the index page of vTiger CRM 7.4.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload.	2024-08-29	7.4	CVE-2024-44777 cve@mitre.org cve@mitre.org
n/a--n/a	A reflected cross-site scripting (XSS) vulnerability in the parent parameter in the index page of vTiger CRM 7.4.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload.	2024-08-29	7.4	CVE-2024-44778 cve@mitre.org cve@mitre.org
n/a--n/a	A reflected cross-site scripting (XSS) vulnerability in the viewname parameter in the index page of vTiger CRM 7.4.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload.	2024-08-29	7.4	CVE-2024-44779 cve@mitre.org cve@mitre.org
n/a--n/a	Vulnerability in admin_ip.php in Seacms v13.1, when action=set, allows attackers to control IP parameters that are written to the data/admin/ip.php file and could result in arbitrary command execution.	2024-08-30	7.2	CVE-2024-44916 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	A traversal vulnerability in GeneralDocs.aspx in CentralSquare CryWolf (False Alarm Management) through 2024-08-09 allows unauthenticated attackers to read files outside of the working web directory via the rpt parameter, leading to the disclosure of sensitive information.	2024-08-26	7.5	CVE-2024-45241 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	An issue was discovered in libexpat before 2.6.3. dtdCopy in xmlparse.c can have an integer overflow for nDefaultAtts on 32-bit platforms (where UINT_MAX equals SIZE_MAX).	2024-08-30	7.3	CVE-2024-45491 cve@mitre.org cve@mitre.org
n/a--n/a	An issue was discovered in libexpat before 2.6.3. nextScaffoldPart in xmlparse.c can have an integer overflow for m_groupSize on 32-bit platforms (where UINT_MAX equals SIZE_MAX).	2024-08-30	7.3	CVE-2024-45492 cve@mitre.org cve@mitre.org
NixOS--hydra	Hydra is a Continuous Integration service for Nix based projects. It is possible to trigger evaluations in Hydra without any authentication. Depending on the size of evaluations, this can impact the availability of systems. The problem can be fixed by applying https://github.com/NixOS/hydra/commit/f73043378907c2c7e44f633ad764c8bdd1c947d5 to any Hydra package. Users are advised to upgrade. Users unable to upgrade should deny the `/api/push` route in a reverse proxy. This also breaks the "Evaluate jobset" button in the frontend.	2024-08-27	7.5	CVE-2024-45049 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
ollama -- ollama	extractFromZipFile in model.go in Ollama before 0.1.47 can extract members of a ZIP archive outside of the parent directory.	2024-08-29	7.5	CVE-2024-45436 cve@mitre.org cve@mitre.org
OpenText--NetIQ Access Manager	Improper Input Validation vulnerability in OpenText NetIQ Access Manager leads to Cross-Site Scripting (XSS) attack.Â This issue affects NetIQ Access Manager before 5.0.4.1 and 5.1.	2024-08-28	7.3	CVE-2024-4554 security@opentext.com security@opentext.com
OpenText--NetIQ Access Manager	Improper Privilege Management vulnerability in OpenText NetIQ Access Manager allows user account impersonation in specific scenario.Â This issue affects NetIQ Access Manager before 5.0.4.1 and before 5.1	2024-08-28	7.7	CVE-2024-4555 security@opentext.com security@opentext.com
OpenText--NetIQ Advance Authentication	A vulnerability identified in storing and reusing information in Advance Authentication. This issue can lead to leakage of sensitive data to unauthorized user. The issue affects NetIQ Advance Authentication before 6.3.5.1	2024-08-28	8.1	CVE-2021-22509 security@opentext.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
OpenText--NetIQ Advance Authentication	A vulnerability identified in NetIQ Advance Authentication that doesn't enforce account lockout when brute force attack is performed on API based login. This issue may lead to user account compromise if successful or may impact server performance. This issue impacts all NetIQ Advance Authentication before 6.3.5.1	2024-08-28	8.2	CVE-2021-22530 security@opentext.com
OpenText--NetIQ Advance Authentication	Insufficient or weak TLS protocol version identified in Advance authentication client server communication when specific service is accessed between devices.Â This issue affects NetIQ Advance Authentication versions before 6.3.5.1	2024-08-28	8.3	CVE-2021-38121 security@opentext.com
oretnom23 -- music_gallery_site	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/categories/manage_category.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-27	9.8	CVE-2024-8221 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- music_gallery_site	A vulnerability classified as critical has been found in SourceCodester Music Gallery Site 1.0. This affects an unknown part of the file /admin/?page=musics/manage_music. 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.	2024-08-27	9.8	CVE-2024-8222 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- music_gallery_site	A vulnerability classified as critical was found in SourceCodester Music Gallery Site 1.0. This vulnerability affects unknown code of the file /classes/Master.php?f=delete_category. 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.	2024-08-27	9.8	CVE-2024-8223 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
OTRS AG--OTRS	Passwords of agents and customers are displayed in plain text in the OTRS admin log module if certain configurations regarding the authentication sources match and debugging for the authentication backend has been enabled. This issue affects: * OTRS from 7.0.X through 7.0.50 * OTRS 8.0.X * OTRS 2023.X * OTRS from 2024.X through 2024.5.X * ((OTRS)) Community Edition: 6.0.x Products based on the ((OTRS)) Community Edition also very likely to be affected	2024-08-26	8.2	CVE-2024-43444 security@otrs.com
Philip Hazel--xfpt	xfpt versions prior to 1.01 fails to handle appropriately some parameters inside the input data, resulting in a stack-based buffer overflow vulnerability. When a user of the affected product is tricked to process a specially crafted file, arbitrary code may be executed on the user's environment.	2024-08-29	7	CVE-2024-43700 vultures@jpcert.or.jp vultures@jpcert.or.jp vultures@jpcert.or.jp
PHPOffice--PhpSpreadsheet	PHPSpreadsheet is a pure PHP library for reading and writing spreadsheet files. Affected versions are subject to a bypassing of a filter which allows for an XXE-attack. This in turn allows attacker to obtain contents of local files, even if error reporting is muted. This vulnerability has been addressed in release version 2.2.1. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-08-28	8.8	CVE-2024-45048 security-advisories@github.com security-advisories@github.com
PriceListo--Best Restaurant Menu by PriceListo	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in PriceListo Best Restaurant Menu by PriceListo allows SQL Injection.This issue affects Best Restaurant Menu by PriceListo: from n/a through 1.4.1.	2024-08-29	8.5	CVE-2024-38793 audit@patchstack.com
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2024.0.0,Â a SQL Injection vulnerability allows an unauthenticated attacker to retrieve the users encrypted password.	2024-08-29	9.8	CVE-2024-6670 security@progress.com security@progress.com
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2024.0.0, if the application is configured with only a single user, a SQL Injection vulnerability allows an unauthenticated attacker to retrieve the users encrypted password.	2024-08-29	9.8	CVE-2024-6671 security@progress.com security@progress.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				com
Progress Software Corporation--WhatsUp Gold	In WhatsUp Gold versions released before 2024.0.0, a SQL Injection vulnerability allows an authenticated low-privileged attacker to achieve privilege escalation by modifying a privileged user's password.	2024-08-29	8.8	CVE-2024-6672 security@progress.com security@progress.com
Propovoice--Propovoice Pro	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Propovoice Propovoice Pro allows SQL Injection.This issue affects Propovoice Pro: from n/a through 1.7.0.3.	2024-08-29	9.3	CVE-2024-43941 audit@patchstack.com
Red Hat--streams for Apache Kafka	A flaw was found in Kroxylicious. When establishing the connection with the upstream Kafka server using a TLS secured connection, Kroxylicious fails to properly verify the server's hostname, resulting in an insecure connection. For a successful attack to be performed, the attacker needs to perform a Man-in-the-Middle attack or compromise any external systems, such as DNS or network routing configuration. This issue is considered a high complexity attack, with additional high privileges required, as the attack would need access to the Kroxylicious configuration or a peer system. The result of a successful attack impacts both data integrity and confidentiality.	2024-08-30	7.3	CVE-2024-8285 secalert@redhat.com secalert@redhat.com
rems --zipped_folder_manager_app	A vulnerability classified as problematic has been found in SourceCodester Zipped Folder Manager App 1.0. This affects an unknown part of the file /endpoint/add-folder.php. The manipulation of the argument folder leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-26	9.8	CVE-2024-8170 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Rockwell Automation--ThinManager ThinServer	A remote code execution vulnerability exists in the Rockwell Automation ThinManagerÂ® ThinServerâ„¢ that allows a threat actor to execute arbitrary code with System privileges. This vulnerability exists due to the lack of proper data input validation, which allows files to be overwritten.	2024-08-26	9.8	CVE-2024-7988 PSIRT@rockwellautomation.com
Roundup WP--Registrations for the Events Calendar	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Roundup WP Registrations for the Events Calendar allows SQL Injection.This issue affects Registrations for the Events Calendar: from n/a through 2.12.2.	2024-08-29	8.5	CVE-2024-39638 audit@patchstack.com
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. An OS Command Injection vulnerability allows any authenticated user on the application to execute arbitrary code on the web application server via port scanning functionality. User-supplied input is used without validation when constructing and executing an OS command. User supplied JSON POST data is parsed and if "id" JSON key does not exist, JSON value supplied via "ip" JSON key is assigned to the "ip" variable. Later on, "ip" variable which can be controlled by the attacker is used when constructing the cmd and cmd1 strings without any extra validation. Then, server_mod.subprocess_execute function is called on both cmd1 and cmd2. When the definition of the server_mod.subprocess_execute() function is analyzed, it can be seen that subprocess.Popen() is called on the input parameter with shell=True which results in OS Command Injection. This issue has not yet been patched. Users are advised to contact the Roxy-WI to coordinate a fix.	2024-08-29	8.8	CVE-2024-43804 security-advisories@github.com
rubrik --cloud_data_management	An incorrect access control vulnerability in Rubrik CDM versions prior to 9.1.2-p1, 9.0.3-p6 and 8.1.3-p12, allows an attacker with network access to execute arbitrary code.	2024-08-27	8.8	CVE-2024-36068 cve@mitre.org cve@mitre.org
Salon Booking System--Salon booking system	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Salon Booking System Salon booking system allows SQL Injection.This issue affects Salon booking system: from n/a through 10.7.	2024-08-29	7.6	CVE-2024-39658 audit@patchstack.com
shafayat-alam--Attire	The Attire theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.0.6 via deserialization of untrusted input. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target	2024-08-31	8.8	CVE-2024-7435 security@wordfence.com security@wordfence.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.			
skyss -- arfa-cms	A cross-site request forgery (CSRF) vulnerability in the admin panel in SkySystem Arfa-CMS before 5.1.3124 allows remote attackers to add a new administrator, leading to escalation of privileges.	2024-08-27	8.8	CVE-2024-45264 cve@mitre.org cve@mitre.org
Smackcoders--SendGrid for WordPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Smackcoders SendGrid for WordPress allows SQL Injection.This issue affects SendGrid for WordPress: from n/a through 1.4.	2024-08-29	8.2	CVE-2024-43965 audit@patchstack.com
sonaar--MP3 Audio Player Music Player, Podcast Player & Radio by Sonaar	The MP3 Audio Player - Music Player, Podcast Player & Radio by Sonaar plugin for WordPress is vulnerable to unauthorized arbitrary file deletion due to a missing capability check on the removeTempFiles() function and insufficient path validation on the 'file' parameter in all versions up to, and including, 5.7.0.1. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary files which can make remote code execution possible when wp-config.php is deleted.	2024-08-29	9.1	CVE-2024-7856 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
SourceCodester--Electric Billing Management System	A vulnerability classified as critical has been found in SourceCodester Electric Billing Management System 1.0. This affects an unknown part of the file /Actions.php?a=login. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-30	7.3	CVE-2024-8340 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Sentiment Based Movie Rating System	A vulnerability, which was classified as critical, was found in SourceCodester Sentiment Based Movie Rating System 1.0. Affected is an unknown function of the file /classes/Users.php?f=save_client of the component User Registration Handler. 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.	2024-08-30	7.3	CVE-2024-8343 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
sportsnet -- sportsnet	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/conexiones/ax/openTracExt/, parameter categoria;.	2024-08-29	9.8	CVE-2024-29723 cve-coordination@incibe.es
sportsnet -- sportsnet	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/ax/registerSp/, parameter idDesafio.	2024-08-29	9.8	CVE-2024-29724 cve-coordination@incibe.es
sportsnet -- sportsnet	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/sort_bloques/, parameter list.	2024-08-29	9.8	CVE-2024-29725 cve-coordination@incibe.es
sportsnet -- sportsnet	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/setAsRead/, parameter id.	2024-08-29	9.8	CVE-2024-29726 cve-coordination@incibe.es
sportsnet -- sportsnet	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/sendParticipationRemember/ , parameter send.	2024-08-29	9.8	CVE-2024-29727 cve-coordination@incibe.es
sportsnet -- sportsnet	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/inscribeUsuario/ , parameter idDesafio.	2024-08-29	9.8	CVE-2024-29728 cve-coordination@incibe.es

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sportsnet -- sportsnet	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query: https://XXXXXXX.saludydesafio.com/app/ax/generateShortURL/, parameter url.	2024-08-29	9.8	CVE-2024-29729 cve-coordination@incibe.es
sportsnet -- sportsnet	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query:Â https://XXXXXXX.saludydesafio.com/app/ax/consejoRandom/ , parameter idCat;.	2024-08-29	9.8	CVE-2024-29730 cve-coordination@incibe.es
sportsnet -- sportsnet	SQL injection vulnerabilities in SportsNET affecting version 4.0.1. These vulnerabilities could allow an attacker to retrieve, update and delete all information in the database by sending a specially crafted SQL query:Â https://XXXXXXX.saludydesafio.com/app/ax/checkBlindFields/ , parameters idChallenge and idEmpresa.	2024-08-29	9.8	CVE-2024-29731 cve-coordination@incibe.es
Stark Digital--WP Testimonial Widget	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Stark Digital WP Testimonial Widget.This issue affects WP Testimonial Widget: from n/a through 3.1.	2024-08-26	7.6	CVE-2024-43966 audit@patchstack.com
Stormhill Media--MyBookTable Bookstore	Cross-Site Request Forgery (CSRF) vulnerability in Stormhill Media MyBookTable Bookstore allows Cross-Site Scripting (XSS).This issue affects MyBookTable Bookstore: from n/a through 3.3.9.	2024-08-26	7.1	CVE-2024-43255 audit@patchstack.com
StylemixThemes--Cost Calculator Builder	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in StylemixThemes Cost Calculator Builder allows SQL Injection.This issue affects Cost Calculator Builder: from n/a through 3.2.15.	2024-08-29	9.3	CVE-2024-43144 audit@patchstack.com
sunmochina -- enterprise_management_system	Incorrect access control in the component /servlet/SnoopServlet of Shenzhou News Union Enterprise Management System v5.0 through v18.8 allows attackers to access sensitive information regarding the server.	2024-08-28	7.5	CVE-2024-44760 cve@mitre.org
TemplateInvaders--TI WooCommerce Wishlist	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in TemplateInvaders TI WooCommerce Wishlist allows SQL Injection.This issue affects TI WooCommerce Wishlist: from n/a through 2.8.2.	2024-08-29	9.3	CVE-2024-43917 audit@patchstack.com
tenda -- ax1806_firmware	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function formGetIptv.	2024-08-26	9.8	CVE-2024-44549 cve@mitre.org
tenda -- ax1806_firmware	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function formGetIptv.	2024-08-26	9.8	CVE-2024-44550 cve@mitre.org
tenda -- ax1806_firmware	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function formGetIptv.	2024-08-26	9.8	CVE-2024-44551 cve@mitre.org
tenda -- ax1806_firmware	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function formGetIptv.	2024-08-26	9.8	CVE-2024-44552 cve@mitre.org
tenda -- ax1806_firmware	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function formGetIptv.	2024-08-26	9.8	CVE-2024-44553 cve@mitre.org
tenda -- ax1806_firmware	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.city.vlan parameter in the function setIptvInfo.	2024-08-26	9.8	CVE-2024-44555 cve@mitre.org
tenda -- ax1806_firmware	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stballvlans parameter in the function setIptvInfo.	2024-08-26	9.8	CVE-2024-44556 cve@mitre.org
tenda -- ax1806_firmware	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.mode parameter in the function setIptvInfo.	2024-08-26	9.8	CVE-2024-44557 cve@mitre.org
tenda -- ax1806_firmware	Tenda AX1806 v1.0.0.1 contains a stack overflow via the adv.iptv.stbpvid parameter in the function setIptvInfo.	2024-08-26	9.8	CVE-2024-44558 cve@mitre.org
tenda -- ax1806_firmware	Tenda AX1806 v1.0.0.1 contains a stack overflow via the iptv.stb.port parameter in the function setIptvInfo.	2024-08-26	9.8	CVE-2024-44563 cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenda -- ax1806_firmware	Tenda AX1806 v1.0.0.1 contains a stack overflow via the serverName parameter in the function form_fast_setting_internet_set.	2024-08-26	9.8	CVE-2024-44565 cve@mitre.org
tenda -- g3_firmware	A vulnerability, which was classified as critical, has been found in Tenda G3 15.11.0.20. This issue affects the function formSetDebugCfg of the file /goform/setDebugCfg. The manipulation of the argument enable/level/module leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-27	9.8	CVE-2024-8224 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
tenda -- g3_firmware	A vulnerability, which was classified as critical, was found in Tenda G3 15.11.0.20. Affected is the function formSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument sysTimePolicy leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-27	9.8	CVE-2024-8225 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
tenda -- o1_firmware	A vulnerability has been found in Tenda O1 1.0.0.7(10648) and classified as critical. Affected by this vulnerability is the function formSetCfm of the file /goform/setcfm. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-28	9.8	CVE-2024-8226 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
tenda -- o1_firmware	A vulnerability was found in Tenda O1 1.0.0.7(10648) and classified as critical. Affected by this issue is the function fromDhcpSetSer of the file /goform/DhcpSetSer. The manipulation of the argument dhcpStartIp/dhcpEndIp/dhcpGw/dhcpMask/dhcpLeaseTime/dhcpDns1/dhcpDns2 leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-28	9.8	CVE-2024-8227 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
tenda -- o5_firmware	A vulnerability was found in Tenda O5 1.0.0.8(5017). It has been classified as critical. This affects the function fromSafeSetMacFilter of the file /goform/setMacFilterList. The manipulation of the argument remark/type/time leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-28	9.8	CVE-2024-8228 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
tenda -- o6_firmware	A vulnerability was found in Tenda O6 1.0.0.7(2054). It has been declared as critical. This vulnerability affects the function frommacFilterModify of the file /goform/operateMacFilter. The manipulation of the argument mac leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-28	9.8	CVE-2024-8229 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
tenda -- o6_firmware	A vulnerability was found in Tenda O6 1.0.0.7(2054). It has been rated as critical. This issue affects the function fromSafeSetMacFilter of the file /goform/setMacFilterList. The manipulation of the argument remark/type/time leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-28	9.8	CVE-2024-8230 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Tenda--O6	A vulnerability classified as critical has been found in Tenda O6 1.0.0.7(2054). Affected is the function fromVirtualSet of the file /goform/setPortForward. The manipulation of the argument ip/localPort/publicPort/app leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-28	8.8	CVE-2024-8231 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
The Beaver Builder Team--Beaver Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Beaver Builder Team Beaver Builder allows Reflected XSS.This issue affects Beaver Builder: from n/a through 2.8.3.2.	2024-08-29	7.1	CVE-2024-43926 audit@patchstack.com
theeventscalendar--The Events	The Events Calendar Pro plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 7.0.2 via deserialization of untrusted input from	2024-08-30	9.1	CVE-2024-8016 security@wordfenc

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Calendar Pro	the 'filters' parameter in widgets. This makes it possible for authenticated attackers, with administrator-level access and above, to inject a PHP Object. The additional presence of a POP chain allows attackers to execute code remotely. In certain configurations, this can be exploitable by lower level users. We confirmed that this plugin installed with Elementor makes it possible for users with contributor-level access and above to exploit this issue.			e.com security@wordfence.com security@wordfence.com
themeum -- droip	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Themeum Droip allows File Manipulation.This issue affects Droip: from n/a through 1.1.1.	2024-08-29	7.5	CVE-2024-43955 audit@patchstack.com
themium--Tutor LMS Pro	The Tutor LMS Pro plugin for WordPress is vulnerable to unauthorized administrative actions execution due to a missing capability checks on multiple functions like treport_quiz_atttempt_delete and tutor_gc_class_action in all versions up to, and including, 2.7.2. This makes it possible for authenticated attackers, with the subscriber-level access and above, to preform an administrative actions on the site, like comments, posts or users deletion, viewing notifications, etc.	2024-08-30	7.1	CVE-2024-5784 security@wordfence.com security@wordfence.com
thimpress--WP Events Manager	The WP Events Manager plugin for WordPress is vulnerable to time-based SQL Injection via the 'order' parameter in all versions up to, and including, 2.1.11 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.	2024-08-31	8.8	CVE-2024-7717 security@wordfence.com security@wordfence.com security@wordfence.com
totolink -- a3002r_firmware	TOTOLINK AC1200 Wireless Router A3002R Firmware V1.1.1-B20200824 is vulnerable to Buffer Overflow. In the boa server program's CGI handling function formWlEncrypt, there is a lack of length restriction on the wlan_ssid field. This oversight leads to potential buffer overflow under specific circumstances. For instance, by invoking the formWlanRedirect function with specific parameters to alter wlan_idx's value and subsequently invoking the formWlEncrypt function, an attacker can trigger buffer overflow, enabling arbitrary command execution or denial of service attacks.	2024-08-28	9.8	CVE-2024-34195 cve@mitre.org
totolink -- t10_firmware	A vulnerability classified as critical has been found in TOTOLINK T10 AC1200 4.1.8cu.5207. Affected is an unknown function of the file /squashfs-root/web_cste/cgi-bin/product.ini of the component Telnet Service. The manipulation leads to hard-coded credentials. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-26	9.8	CVE-2024-8162 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Unknown--Web Directory Free	The Web Directory Free WordPress plugin before 1.7.3 does not validate a parameter before using it in an include(), which could lead to Local File Inclusion issues.	2024-08-30	9.1	CVE-2024-3673 contact@wpscan.com
WBW--WBW Product Table PRO	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WBW WBW Product Table PRO allows SQL Injection.This issue affects WBW Product Table PRO: from n/a through 1.9.4.	2024-08-29	10	CVE-2024-43918 audit@patchstack.com
weDevs--WP User Frontend	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in weDevs WP User Frontend allows SQL Injection.This issue affects WP User Frontend: from n/a through 4.0.7.	2024-08-29	7.6	CVE-2024-38693 audit@patchstack.com
Wpsoul--Greenshift Query and Meta Addon	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Wpsoul Greenshift Query and Meta Addon allows SQL Injection.This issue affects Greenshift Query and Meta Addon: from n/a before 3.9.2.	2024-08-29	8.5	CVE-2024-43942 audit@patchstack.com
Wpsoul--Greenshift Woocommerce Addon	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Wpsoul Greenshift Woocommerce Addon allows SQL Injection.This issue affects Greenshift Woocommerce Addon: from n/a before 1.9.8.	2024-08-29	8.5	CVE-2024-43943 audit@patchstack.com
WPWeb Elite--Docket (WooCommerce Collections /	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPWeb Elite Docket (WooCommerce Collections / Wishlist / Watchlist) allows SQL Injection.This issue affects Docket (WooCommerce Collections / Wishlist / Watchlist): from n/a before 1.7.0.	2024-08-29	9.3	CVE-2024-43132 audit@patchstack.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Wishlist / Watchlist)				
Xiaomi--App Market	A code execution vulnerability exists in the Xiaomi App market product. The vulnerability is caused by unsafe configuration and can be exploited by attackers to execute arbitrary code.	2024-08-28	7.6	CVE-2023-26323 security@xiaomi.com
Xiaomi--GetApps application	A code execution vulnerability exists in the XiaomiGetApps application product. This vulnerability is caused by the verification logic being bypassed, and an attacker can exploit this vulnerability to execute malicious code.	2024-08-28	8.8	CVE-2023-26322 security@xiaomi.com
Xiaomi--GetApps application	A code execution vulnerability exists in the XiaomiGetApps application product. This vulnerability is caused by the verification logic being bypassed, and an attacker can exploit this vulnerability to execute malicious code.	2024-08-28	8.8	CVE-2023-26324 security@xiaomi.com
Xiaomi--GetApps application	A code execution vulnerability exists in the XiaomiGetApps application product. This vulnerability is caused by the verification logic being bypassed, and an attacker can exploit this vulnerability to execute malicious code.	2024-08-28	8.8	CVE-2024-45346 security@xiaomi.com
10Web Form Builder Team--Form Maker by 10Web	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in 10Web Form Builder Team Form Maker by 10Web allows Reflected XSS.This issue affects Form Maker by 10Web: from n/a through 1.15.26.	2024-08-12	7.1	CVE-2024-43220 audit@patchstack.com
AddonMaster--Post Grid Master	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AddonMaster Post Grid Master allows Reflected XSS.This issue affects Post Grid Master: from n/a through 3.4.10.	2024-08-12	7.1	CVE-2024-43156 audit@patchstack.com
adobe -- acrobat	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could result in arbitrary code execution in the context of the current user. This issue occurs when the state of a resource changes between its check-time and use-time, allowing an attacker to manipulate the resource. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7	CVE-2024-39420 psirt@adobe.com
adobe -- acrobat	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	7.8	CVE-2024-39422 psirt@adobe.com
adobe -- acrobat	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	7.8	CVE-2024-39423 psirt@adobe.com
adobe -- acrobat	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	7.8	CVE-2024-39424 psirt@adobe.com
adobe -- acrobat	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to privilege escalation. Exploitation of this issue require local low-privilege access to the affected system and attack complexity is high.	2024-08-14	7	CVE-2024-39425 psirt@adobe.com
adobe -- acrobat	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	CVE-2024-39426 psirt@adobe.com
adobe -- acrobat	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	7.8	CVE-2024-41830 psirt@adobe.com
adobe -- acrobat	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Use After Free vulnerability that could result in	2024-08-14	7.8	CVE-2024-41831 psirt@adobe.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue does not require user interaction, but attack complexity is high and scope is changed.	2024-08-14	9	CVE-2024-39397 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability could allow an admin attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link. Confidentiality and integrity impact is high as it affects other admin accounts.	2024-08-14	8.1	CVE-2024-39400 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed.	2024-08-14	8.4	CVE-2024-39401 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed.	2024-08-14	8.4	CVE-2024-39402 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Restriction of Excessive Authentication Attempts vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability to perform brute force attacks and potentially gain unauthorized access to accounts. Exploitation of this issue does not require user interaction, but attack complexity is high.	2024-08-14	7.4	CVE-2024-39398 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. A low-privileged attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed.	2024-08-14	7.7	CVE-2024-39399 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality impact is high due to the attacker being able to exfiltrate sensitive information.	2024-08-14	7.6	CVE-2024-39403 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploitation of this issue does not require user interaction and scope is changed.	2024-08-14	7.7	CVE-2024-39406 psirt@adobe.com
adobe -- illustrator	Illustrator versions 28.5, 27.9.4 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.	2024-08-14	7.8	CVE-2024-34133 psirt@adobe.com
adobe -- indesign	InDesign Desktop versions ID19.4, ID18.5.2 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.	2024-08-14	7.1	CVE-2024-34127 psirt@adobe.com
adobe -- substance_3d_designer	Substance3D - Designer versions 13.1.2 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.	2024-08-14	7.8	CVE-2024-41864 psirt@adobe.com
Adobe--Acrobat Reader	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	7.8	CVE-2024-39383 psirt@adobe.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Bridge	Bridge versions 13.0.8, 14.1.1 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.	2024-08-14	7.8	CVE-2024-39386 psirt@adobe.com
Adobe--Bridge	Bridge versions 13.0.8, 14.1.1 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.	2024-08-14	7.8	CVE-2024-41840 psirt@adobe.com
Adobe--Dimension	Dimension versions 3.4.11 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.	2024-08-14	7.8	CVE-2024-20789 psirt@adobe.com
Adobe--Dimension	Dimension versions 3.4.11 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.	2024-08-14	7.8	CVE-2024-34124 psirt@adobe.com
Adobe--Dimension	Dimension versions 3.4.11 and earlier are affected by an Untrusted Search Path vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by inserting a malicious file into the search path, which the application might execute instead of the legitimate file. This could occur if the application uses a search path to locate executables or libraries. Exploitation of this issue requires user interaction.	2024-08-14	7.8	CVE-2024-41865 psirt@adobe.com
Adobe--Illustrator	Illustrator versions 28.5, 27.9.4 and earlier are affected by an Improper Input Validation 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.	2024-08-14	7.8	CVE-2024-41856 psirt@adobe.com
Adobe--InCopy	InCopy versions 18.5.2, 19.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	CVE-2024-41858 psirt@adobe.com
Adobe--InDesign Desktop	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a Stack-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.	2024-08-14	7.8	CVE-2024-39389 psirt@adobe.com
Adobe--InDesign Desktop	InDesign Desktop versions ID19.4, ID18.5.2 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.	2024-08-14	7.8	CVE-2024-39390 psirt@adobe.com
Adobe--InDesign Desktop	InDesign Desktop versions ID19.4, ID18.5.2 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.	2024-08-14	7.8	CVE-2024-39391 psirt@adobe.com
Adobe--InDesign Desktop	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	CVE-2024-39393 psirt@adobe.com
Adobe--InDesign Desktop	InDesign Desktop versions ID19.4, ID18.5.2 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.	2024-08-14	7.8	CVE-2024-39394 psirt@adobe.com
Adobe--InDesign Desktop	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	CVE-2024-41850 psirt@adobe.com
Adobe--InDesign Desktop	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	CVE-2024-41851 psirt@adobe.com
Adobe--InDesign Desktop	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a Stack-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.	2024-08-14	7.8	CVE-2024-41852 psirt@adobe.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--InDesign Desktop	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	CVE-2024-41853 psirt@adobe.com
Adobe--Photoshop Desktop	Photoshop Desktop versions 24.7.3, 25.9.1 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	CVE-2024-34117 psirt@adobe.com
Adobe--Substance3D - Stager	Substance3D - Stager versions 3.0.2 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	7.8	CVE-2024-39388 psirt@adobe.com
AMD--3rd Gen AMD EPYC Processors	Improper validation in a model specific register (MSR) could allow a malicious program with ring0 access to modify SMM configuration while SMI lock is enabled, potentially leading to arbitrary code execution.	2024-08-12	7.5	CVE-2023-31315 psirt@amd.com
AMD--AMD Athlon 3000 Series Desktop Processors with Radeon Graphics	Improper bounds checking in APCB firmware may allow an attacker to perform an out of bounds write, corrupting the APCB entry, potentially leading to arbitrary code execution.	2024-08-13	7.5	CVE-2022-23815 psirt@amd.com
AMD--AMD EPYC 7001 Processors	A TOCTOU (Time-Of-Check-Time-Of-Use) in SMM may allow an attacker with ring0 privileges and access to the BIOS menu or UEFI shell to modify the communications bufferÂ potentially resulting in arbitrary code execution.	2024-08-13	7.5	CVE-2023-20578 psirt@amd.com
AMD--AMD EPYC 7001 Series Processors	An out of bounds memory write when processing the AMD PSP1 Configuration Block (APCB) could allow an attacker with access the ability to modify the BIOS image, and the ability to sign the resulting image, to potentially modify the APCB block resulting in arbitrary code execution.	2024-08-13	7.2	CVE-2021-26344 psirt@amd.com
AMD--AMD Ryzen 3000 Series Desktop Processors	Insufficient checking of memory buffer in ASP Secure OS may allow an attacker with a malicious TA to read/write to the ASP Secure OS kernel virtual address space, potentially leading to privilege escalation.	2024-08-13	7	CVE-2022-23817 psirt@amd.com
AMD--Prof Tool	Insufficient validation of the Input Output Control (IOCTL) input buffer in AMD ?Prof may allow an authenticated attacker to cause an out-of-bounds write, potentially causing a WindowsÂ® OS crash, resulting in denial of service.	2024-08-13	7.3	CVE-2023-31341 psirt@amd.com
AMD--Prof Tool	A DLL hijacking vulnerability in AMD Î¼Prof could allow an attacker to achieve privilege escalation, potentially resulting in arbitrary code execution.	2024-08-13	7.3	CVE-2023-31348 psirt@amd.com
AMD--Prof Tool	Incorrect default permissions in the AMD ?Prof installation directory could allow an attacker to achieve privilege escalation, potentially resulting in arbitrary code execution.	2024-08-13	7.3	CVE-2023-31349 psirt@amd.com
angeljudesuarez --tailoring_management_system	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been classified as critical. This affects an unknown part of the file /incedit.php?id=4. The manipulation of the argument id/inccat/desc/date/amount leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	9.8	CVE-2024-7680 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
anhvnit--Woocommerce OpenPos	Missing Authorization vulnerability in anhvnit Woocommerce OpenPos allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Woocommerce OpenPos: from n/a through 6.4.4.	2024-08-13	7.5	CVE-2024-37935 audit@patchstack.com
annke --crater_2_firmware	An OS command injection vulnerability in the ccm_debug component of MIPC Camera firmware prior to v5.4.1.240424171021 allows attackers within the same network to execute arbitrary code via a crafted HTML request.	2024-08-12	8.8	CVE-2024-39091 cve@mitre.org
Apache Software Foundation--Apache DolphinScheduler	Improper Input Validation vulnerability in Apache DolphinScheduler. An authenticated user can cause arbitrary, unsandboxed javascript to be executed on the server. If you are using the switch task plugin, please upgrade to version 3.2.2.	2024-08-12	8.8	CVE-2024-29831 security@apache.org
averta--Slider & Popup Builder by Depicter Add Image Slider,	The Slider and Carousel slider by Depicter plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the uploadFile function in all versions up to, and including, 3.1.1. This makes it possible for authenticated	2024-08-14	8.8	CVE-2024-4389 security@wordfence.com security@wordfenc

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Carousel Slider, Exit Intent Popup, Popup Modal, Coupon Popup, Post Slider Carousel	attackers, with contributor access or higher, to upload arbitrary files on the affected site's server which may make remote code execution possible.			e.com security@wordfence.com
BannerSky--BSK Forms Blacklist	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BannerSky BSK Forms Blacklist allows Reflected XSS.This issue affects BSK Forms Blacklist: from n/a through 3.8.	2024-08-12	7.1	CVE-2024-43233 audit@patchstack.com
BerqWP--BerqWP	Unrestricted Upload of File with Dangerous Type vulnerability in BerqWP allows Code Injection.This issue affects BerqWP: from n/a through 1.7.6.	2024-08-13	10	CVE-2024-43160 audit@patchstack.com
boa-dev--boa	Boa is an embeddable and experimental Javascript engine written in Rust. Starting in version 0.16 and prior to version 0.19.0, a wrong assumption made when handling ECMAScript's `AsyncGenerator` operations can cause an uncaught exception on certain scripts. Boa's implementation of `AsyncGenerator` makes the assumption that the state of an `AsyncGenerator` object cannot change while resolving a promise created by methods of `AsyncGenerator` such as `%AsyncGeneratorPrototype%.next`, `%AsyncGeneratorPrototype%.return`, or `%AsyncGeneratorPrototype%.throw`. However, a carefully constructed code could trigger a state transition from a getter method for the promise's `then` property, which causes the engine to fail an assertion of this assumption, causing an uncaught exception. This could be used to create a Denial Of Service attack in applications that run arbitrary ECMAScript code provided by an external user. Version 0.19.0 is patched to correctly handle this case. Users unable to upgrade to the patched version would want to use `std::panic::catch_unwind` to ensure any exceptions caused by the engine don't impact the availability of the main application.	2024-08-15	7.5	CVE-2024-43367 security-advisories@github.com security-advisories@github.com security-advisories@github.com
CAYIN Technology--CMS-SE(22.04)	The specific CGI of the CAYIN Technology CMS does not properly validate user input, allowing a remote attacker with administrator privileges to inject OS commands into the specific parameter and execute them on the remote server.	2024-08-14	7.2	CVE-2024-7728 twcert@cert.org.tw twcert@cert.org.tw twcert@cert.org.tw
CAYIN Technology--SMP-2100	The CAYIN Technology CMS lacks proper access control, allowing unauthenticated remote attackers to download arbitrary CGI files.	2024-08-14	7.5	CVE-2024-7729 twcert@cert.org.tw twcert@cert.org.tw twcert@cert.org.tw
clastix -- kamaji	Kamaji is the Hosted Control Plane Manager for Kubernetes. In versions 1.0.0 and earlier, Kamaji uses an "open at the top" range definition in RBAC for etcd roles leading to some TCPs API servers being able to read, write, and delete the data of other control planes. This vulnerability is fixed in edge-24.8.2.	2024-08-12	9.9	CVE-2024-42480 security-advisories@github.com security-advisories@github.com security-advisories@github.com
code-projects -- simple_ticket_booking	A vulnerability was found in code-projects Simple Ticket Booking 1.0. It has been classified as critical. Affected is an unknown function of the file register_insert.php of the component Registration Handler. The manipulation of the argument name/email/dob/password/Gender/phone leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	9.8	CVE-2024-7635 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects -- simple_ticket_booking	A vulnerability was found in code-projects Simple Ticket Booking 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file authenticate.php of the component Login. The manipulation of the argument email/password leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	9.8	CVE-2024-7636 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
code-projects--Job Portal	A vulnerability was found in code-projects Job Portal 1.0. It has been classified as critical. Affected is an unknown function of the file logindbc.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.	2024-08-15	7.3	CVE-2024-7808 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Codection--Import and export users and customers	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Codection Import and export users and customers allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Import and export users and customers: from n/a through 1.26.8.	2024-08-13	7.5	CVE-2024-38787 audit@patchstack.com
college_management_system_project -- college_management_system	A vulnerability was found in code-projects College Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php of the component Login Page. The manipulation of the argument email/password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	9.8	CVE-2024-7681 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Crocoblock--JetElements	The JetElements plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.6.20 via the 'progress_type' parameter. 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.	2024-08-16	8.8	CVE-2024-7145 security@wordfence.com security@wordfence.com
Crocoblock--JetTabs for Elementor	The JetTabs for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.2.3 via the 'switcher_preset' parameter. 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.	2024-08-16	8.8	CVE-2024-7146 security@wordfence.com security@wordfence.com
dglingren--Media Library Assistant	The Media Library Assistant plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation involving the mla-inline-edit-upload-scripts AJAX action in all versions up to, and including, 3.18. 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.	2024-08-13	8.8	CVE-2024-6823 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
dylanjkotze--Zephyr Project Manager	The Zephyr Project Manager plugin for WordPress is vulnerable to limited privilege escalation in all versions up to, and including, 3.3.101. This is due to the plugin not properly checking a users capabilities before allowing them to enable access to the plugin's settings through the update_user_access() function. This makes it possible for authenticated attackers, with subscriber-level access and above, to grant themselves full access to the plugin's settings.	2024-08-15	8.1	CVE-2024-7624 security@wordfence.com security@wordfence.com security@wordfence.com
edimax -- ic-6220dc_firmware	A vulnerability was found in Edimax IC-6220DC and IC-5150W up to 3.06. It has been rated as critical. Affected by this issue is the function cgiFormString of the file ipcam_cgi. The manipulation of the argument host leads to command injection. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-12	9.8	CVE-2024-7616 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Elastic--Kibana	A flaw allowing arbitrary code execution was discovered in Kibana. An attacker with access to ML and Alerting connector features, as well as write access to internal ML indices can trigger a prototype pollution vulnerability, ultimately leading to arbitrary code execution.	2024-08-13	9.1	CVE-2024-37287 bressers@elastic.co

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
F5--BIG-IP Next Central Manager	The Central Manager user session refresh token does not expire when a user logs out.Â Â Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2024-08-14	7.5	CVE-2024-39809 f5sirt@f5.com
F5--BIG-IP	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Â Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	7.5	CVE-2024-39778 f5sirt@f5.com
F5--BIG-IP	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase in memory resource utilization.Â Â Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	7.5	CVE-2024-41727 f5sirt@f5.com
F5--NGINX Plus	When the NGINX Plus is configured to use the MQTT pre-read module, undisclosed requests can cause an increase in memory resource utilization.Â Â Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	7.5	CVE-2024-39792 f5sirt@f5.com
fabianros -- job_portal	A vulnerability was found in code-projects Job Portal 1.0. It has been rated as critical. This issue affects some unknown processing of the file rw_i_nat.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.	2024-08-12	9.8	CVE-2024-7682 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
fabianros -- online_polling	A vulnerability was found in code-projects Online Polling 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file registeracc.php of the component Registration. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	9.8	CVE-2024-7637 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
ffmpeg -- ffmpeg	A vulnerability, which was classified as critical, was found in FFmpeg up to 5.1.5. This affects the function fill_audiodata of the file /libswresample/swresample.c. The manipulation leads to heap-based buffer overflow. It is possible to initiate the attack remotely. This issue was fixed in version 6.0 by 9903ba28c28ab18dc7b7b6fb8571cc8b5caae1a6 but a backport for 5.1 was forgotten. The exploit has been disclosed to the public and may be used. Upgrading to version 5.1.6 and 6.0 9903ba28c28ab18dc7b7b6fb8571cc8b5caae1a6 is able to address this issue. It is recommended to upgrade the affected component.	2024-08-12	8.8	CVE-2024-7272 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Firewalla--Box Software	A weak credential vulnerability exists in Firewalla Box Software versions before 1.979. This vulnerability allows a physically close attacker to use the license UUID for authentication and provision SSH credentials over the Bluetooth Low-Energy (BTLE) interface. Once an attacker gains access to the LAN, they could log into the SSH interface using the provisioned credentials. The license UUID can be acquired through plain-text Bluetooth sniffing, reading the QR code on the bottom of the device, or brute-forcing the UUID (though this is less likely).	2024-08-12	7.1	CVE-2024-40892 disclosure@vulncheck.com
FIWARE--FIWARE Keyrock	The function "generate_app_certificates" in lib/app_certificates.js of FIWARE Keyrock <= 8.4 does notÂ neutralize special elements used in an OS Command properly. This allows an authenticated user with permissions to create applications to execute commands by creating an application with a malicious name.	2024-08-12	9.1	CVE-2024-42166 office@cyberdanube.com
FIWARE--FIWARE Keyrock	The function "generate_app_certificates" in controllers/saml2/saml2.js of FIWARE Keyrock <= 8.4Â does not neutralize special elements used in an OS Command properly. This allows an authenticated user with permissions to create applications to execute commands by creating an application with a malicious organisationname.	2024-08-12	9.1	CVE-2024-42167 office@cyberdanube.com
FIWARE--FIWARE Keyrock	Insufficiently random values for generating password reset token in FIWARE Keyrock <= 8.4 allowÂ attackers to take over the account of any user by predicting the token for the password reset link.	2024-08-12	8.3	CVE-2024-42163 office@cyberdanube.com
flatpak--flatpak	Flatpak is a Linux application sandboxing and distribution framework. Prior to versions 1.14.0 and 1.15.10, a malicious or compromised Flatpak app using persistent directories could access and write files outside of what it would otherwise have access to, which is an attack on integrity and confidentiality. When `persistent=subdir` is used in the application permissions (represented as `--persist=subdir` in the command-line interface), that means that an application which otherwise doesn't have access to the real user home directory will see an empty home directory with a writeable subdirectory `subdir`. Behind the scenes, this directory is actually a bind mount and the data is stored in the per-application directory as `~/.var/app/$APPID/subdir`. This allows existing apps that are not aware of the per-application directory to still work as intended without general home directory access. However, the application does have write access to the	2024-08-15	10	CVE-2024-42472 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	application directory `~/.var/app/$APPID` where this directory is stored. If the source directory for the `persistent`/`--persist` option is replaced by a symlink, then the next time the application is started, the bind mount will follow the symlink and mount whatever it points to into the sandbox. Partial protection against this vulnerability can be provided by patching Flatpak using the patches in commits ceec2ffc and 98f79773. However, this leaves a race condition that could be exploited by two instances of a malicious app running in parallel. Closing the race condition requires updating or patching the version of bubblewrap that is used by Flatpak to add the new `--bind-fd` option using the patch and then patching Flatpak to use it. If Flatpak has been configured at build-time with `-Dsystem_bubblewrap=bwrap` (1.15.x) or `--with-system-bubblewrap=bwrap` (1.14.x or older), or a similar option, then the version of bubblewrap that needs to be patched is a system copy that is distributed separately, typically `/usr/bin/bwrap`. This configuration is the one that is typically used in Linux distributions. If Flatpak has been configured at build-time with `-Dsystem_bubblewrap=` (1.15.x) or with `--without-system-bubblewrap` (1.14.x or older), then it is the bundled version of bubblewrap that is included with Flatpak that must be patched. This is typically installed as `/usr/libexec/flatpak-bwrap`. This configuration is the default when building from source code. For the 1.14.x stable branch, these changes are included in Flatpak 1.14.10. The bundled version of bubblewrap included in this release has been updated to 0.6.3. For the 1.15.x development branch, these changes are included in Flatpak 1.15.10. The bundled version of bubblewrap in this release is a Meson "wrap" subproject, which has been updated to 0.10.0. The 1.12.x and 1.10.x branches will not be updated for this vulnerability. Long-term support OS distributions should backport the individual changes into their versions of Flatpak and bubblewrap, or update to newer versions if their stability policy allows it. As a workaround, avoid using applications using the `persistent` (`--persist`) permission.			com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
freebsd -- freebsd	A signal handler in sshd(8) may call a logging function that is not async-signal-safe. The signal handler is invoked when a client does not authenticate within the LoginGraceTime seconds (120 by default). This signal handler executes in the context of the sshd(8)'s privileged code, which is not sandboxed and runs with full root privileges. This issue is another instance of the problem in CVE-2024-6387 addressed by FreeBSD-SA-24:04.openssh. The faulty code in this case is from the integration of blacklistd in OpenSSH in FreeBSD. As a result of calling functions that are not async-signal-safe in the privileged sshd(8) context, a race condition exists that a determined attacker may be able to exploit to allow an unauthenticated remote code execution as root.	2024-08-12	8.1	CVE-2024-7589 secteam@freebsd.org secteam@freebsd.org secteam@freebsd.org
freebsd -- freebsd	A logic bug in the code which disables kernel tracing for setuid programs meant that tracing was not disabled when it should have, allowing unprivileged users to trace and inspect the behavior of setuid programs. The bug may be used by an unprivileged user to read the contents of files to which they would not otherwise have access, such as the local password database.	2024-08-12	7.5	CVE-2024-6760 secteam@freebsd.org
frogcms_project -- frogcms	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/layout/delete/1	2024-08-12	8.8	CVE-2024-42623 cve@mitre.org
frogcms_project -- frogcms	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/page/delete/10.	2024-08-12	8.8	CVE-2024-42624 cve@mitre.org
frogcms_project -- frogcms	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/layout/add	2024-08-12	8.8	CVE-2024-42625 cve@mitre.org
frogcms_project -- frogcms	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/snippet/add.	2024-08-12	8.8	CVE-2024-42626 cve@mitre.org
frogcms_project -- frogcms	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/snippet/delete/3.	2024-08-12	8.8	CVE-2024-42627 cve@mitre.org
frogcms_project -- frogcms	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/snippet/edit/3.	2024-08-12	8.8	CVE-2024-42628 cve@mitre.org
frogcms_project -- frogcms	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/page/edit/10.	2024-08-12	8.8	CVE-2024-42629 cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
frogcms_project -- frogcms	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/plugin/file_manager/create_file.	2024-08-12	8.8	CVE-2024-42630 cve@mitre.org
frogcms_project -- frogcms	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/layout/edit/1.	2024-08-12	8.8	CVE-2024-42631 cve@mitre.org
frogcms_project -- frogcms	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/page/add.	2024-08-12	8.8	CVE-2024-42632 cve@mitre.org
G5Theme--Ultimate Bootstrap Elements for Elementor	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in G5Theme Ultimate Bootstrap Elements for Elementor allows PHP Local File Inclusion.This issue affects Ultimate Bootstrap Elements for Elementor: from n/a through 1.4.4.	2024-08-13	7.5	CVE-2024-43140 audit@patchstack.com
ggerganov -- llama.cpp	llama.cpp provides LLM inference in C/C++. The unsafe `data` pointer member in the `rpc_tensor` structure can cause arbitrary address reading. This vulnerability is fixed in b3561.	2024-08-12	9.8	CVE-2024-42478 security-advisories@github.com security-advisories@github.com
ggerganov -- llama.cpp	llama.cpp provides LLM inference in C/C++. The unsafe `data` pointer member in the `rpc_tensor` structure can cause arbitrary address writing. This vulnerability is fixed in b3561.	2024-08-12	9.8	CVE-2024-42479 security-advisories@github.com security-advisories@github.com
ggerganov -- llama.cpp	llama.cpp provides LLM inference in C/C++. The unsafe `type` member in the `rpc_tensor` structure can cause `global-buffer-overflow`. This vulnerability may lead to memory data leakage. The vulnerability is fixed in b3561.	2024-08-12	7.5	CVE-2024-42477 security-advisories@github.com security-advisories@github.com
Google--Android	In _MMU_AllocLevel of mmu_common.c, there is a possible arbitrary code execution due to an integer overflow. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-08-15	7.8	CVE-2024-31333 security@android.com
Google--Android	In multiple functions of TranscodingResourcePolicy.cpp, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-08-15	7.7	CVE-2024-34731 security@android.com security@android.com security@android.com security@android.com security@android.com
Google--Android	In onForegroundServiceButtonClicked of FooterActionsViewModel.kt, there is a possible way to disable the active VPN app from the lockscreen due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-08-15	7.7	CVE-2024-34734 security@android.com security@android.com
Google--Android	In ensureSetPipAspectRatioQuotaTracker of ActivityClientController.java, there is a possible way to generate unmovable and undeletable pip windows due to a logic	2024-08-15	7.7	CVE-2024-34737 security@android.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			security@android.com
Google--Android	In multiple functions of AppOpsService.java, there is a possible way for unprivileged apps to read their own restrictRead app-op states 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.	2024-08-15	7.7	CVE-2024-34738 security@android.com security@android.com
Google--Android	In shouldRestrictOverlayActivities of UsbProfileGroupSettingsManager.java, there is a possible escape from SUW 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.	2024-08-15	7.7	CVE-2024-34739 security@android.com security@android.com
Google--Android	In attributeBytesBase64 and attributeBytesHex of BinaryXmlSerializer.java, there is a possible arbitrary XML injection 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.	2024-08-15	7.7	CVE-2024-34740 security@android.com security@android.com security@android.com
Google--Android	In setForceHideNonSystemOverlayWindowIfNeeded of WindowState.java, there is a possible way for message content to be visible on the screensaver while lock screen visibility settings are restricted by the user 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.	2024-08-15	7.8	CVE-2024-34741 security@android.com security@android.com
guillaumepotier--gettext.js	gettext.js is a GNU gettext port for node and the browser. There is a cross-site scripting (XSS) injection if `.po` dictionary definition files are corrupted. This vulnerability has been patched in version 2.0.3. As a workaround, control the origin of the definition catalog to prevent the use of this flaw in the definition of plural forms.	2024-08-16	7.2	CVE-2024-43370 security-advisories@github.com security-advisories@github.com
HitPay Payment Solutions Pte Ltd--HitPay Payment Gateway for WooCommerce	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in HitPay Payment Solutions Pte Ltd HitPay Payment Gateway for WooCommerce allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects HitPay Payment Gateway for WooCommerce: from n/a through 4.1.3.	2024-08-13	7.5	CVE-2024-38747 audit@patchstack.com
ibexa--fieldtype-richtext	Ibexa RichText Field Type is a Field Type for supporting rich formatted text stored in a structured XML format. In versions on the 4.6 branch prior to 4.6.10, the validator for the RichText fieldtype blocklists `javascript:` and `vbscript:` in links to prevent XSS. This can leave other options open, and the check can be circumvented using upper case. Content editing permissions for RichText content is required to exploit this vulnerability, which typically means Editor role or higher. The fix implements an allowlist instead, which allows only approved link protocols. The new check is case insensitive. Version 4.6.10 contains a patch for this issue. No known workarounds are available.	2024-08-16	7.2	CVE-2024-43369 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
IBM--Common Licensing	IBM Common Licensing 9.0 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 297895.	2024-08-13	7.5	CVE-2024-40697 psirt@us.ibm.com psirt@us.ibm.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--OpenBMC	A vulnerability in the combination of the OpenBMC's FW1050.00 through FW1050.10, FW1030.00 through FW1030.50, and FW1020.00 through FW1020.60 default password and session management allow an attacker to gain administrative access to the BMC. IBM X-Force ID: 290674.	2024-08-13	7.5	CVE-2024-35124 psirt@us.ibm.com psirt@us.ibm.com
IBM--Security Directory Integrator	IBM Security Directory Integrator 7.2.0 and Security Verify Directory Integrator 10.0.0 does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources. IBM X-Force ID: 228570.	2024-08-16	7.3	CVE-2022-33162 psirt@us.ibm.com psirt@us.ibm.com
inspirelabs--InPost PL	The InPost for WooCommerce plugin and InPost PL plugin for WordPress are vulnerable to unauthorized access and deletion of data due to a missing capability check on the 'parse_request' function in all versions up to, and including, 1.4.0 (for InPost for WooCommerce) as well as 1.4.4 (for InPost PL). This makes it possible for unauthenticated attackers to read and delete arbitrary files on Windows servers. On Linux servers, only files within the WordPress install will be deleted, but all files can be read.	2024-08-17	10	CVE-2024-6500 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
inspireui--MStore API Create Native Android & iOS Apps On The Cloud	The MStore API - Create Native Android & iOS Apps On The Cloud plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 4.15.2. This is due to the use of loose comparison in the 'verify_id_token' 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 an @flutter.io email address or phone number. This also requires firebase to be configured on the website and the user to have set up firebase for their account.	2024-08-15	8.1	CVE-2024-7628 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
itsourcecode--Billing System	A vulnerability classified as critical has been found in itsourcecode Billing System 1.0. This affects an unknown part of the file addbill.php. The manipulation of the argument owners_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.	2024-08-15	7.3	CVE-2024-7839 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
itsourcecode--Online Food Ordering System	A vulnerability was found in itsourcecode Online Food Ordering System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /addcategory.php. The manipulation of the argument cname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	7.3	CVE-2024-7838 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
ivanti -- avalanche	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion.	2024-08-14	9.1	CVE-2024-38652 support@hackerone.com
ivanti -- avalanche	An off-by-one error in WLInfoRailService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS.	2024-08-14	7.5	CVE-2024-36136 support@hackerone.com
ivanti -- avalanche	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with admin rights to achieve RCE.	2024-08-14	7.2	CVE-2024-37373 support@hackerone.com
ivanti -- avalanche	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS.	2024-08-14	7.5	CVE-2024-37399 support@hackerone.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ivanti -- avalanche	XXE in SmartDeviceServer in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server.	2024-08-14	7.5	CVE-2024-38653 support@hackerone.com
Ivanti--ITSM	An information disclosure vulnerability in Ivanti ITSM on-prem and Neurons for ITSM versions 2023.4 and earlier allows an unauthenticated attacker to obtain the OIDC client secret via debug information.	2024-08-13	9.6	CVE-2024-7569 3c1d8aa1-5a33-4ea4-8992-aadd6440af75
Ivanti--ITSM	Improper certificate validation in Ivanti ITSM on-prem and Neurons for ITSM Versions 2023.4 and earlier allows a remote attacker in a MITM position to craft a token that would allow access to ITSM as any user.	2024-08-13	8.3	CVE-2024-7570 3c1d8aa1-5a33-4ea4-8992-aadd6440af75
Ivanti--vTM	Incorrect implementation of an authentication algorithm in Ivanti vTM other than versions 22.2R1 or 22.7R2 allows a remote unauthenticated attacker to bypass authentication of the admin panel.	2024-08-13	9.8	CVE-2024-7593 3c1d8aa1-5a33-4ea4-8992-aadd6440af75
j4k0xb -- webcrack	webcrack is a tool for reverse engineering javascript. An arbitrary file write vulnerability exists in the webcrack module when processing specifically crafted malicious code on Windows systems. This vulnerability is triggered when using the unpack bundles feature in conjunction with the saving feature. If a module name includes a path traversal sequence with Windows path separators, an attacker can exploit this to overwrite files on the host system. This vulnerability allows an attacker to write arbitrary `.js` files to the host system, which can be leveraged to hijack legitimate Node.js modules to gain arbitrary code execution. This vulnerability has been patched in version 2.14.1.	2024-08-15	7.8	CVE-2024-43373 security-advisories@github.com security-advisories@github.com security-advisories@github.com
jayesh -- online_exam_system	A Broken Access Control vulnerability was found in /admin/update.php and /admin/dashboard.php in Kashipara Online Exam System v1.0, which allows remote unauthenticated attackers to view administrator dashboard and delete valid user accounts via the direct URL access.	2024-08-12	9.8	CVE-2024-40480 cve@mitre.org cve@mitre.org
kingsoft -- wps_office	Improper path validation in promecefpluginhost.exe in Kingsoft WPS Office version ranging from 12.2.0.13110 to 12.2.0.13489 (inclusive) on Windows allows an attacker to load an arbitrary Windows library. The vulnerability was found weaponized as a single-click exploit in the form of a deceptive spreadsheet document	2024-08-15	7.8	CVE-2024-7262 security@eset.com
kingsoft -- wps_office	Improper path validation in promecefpluginhost.exe in Kingsoft WPS Office version ranging from 12.2.0.13110 to 12.2.0.17153 (exclusive) on Windows allows an attacker to load an arbitrary Windows library. The patch released in version 12.2.0.16909 to mitigate CVE-2024-7262 was not restrictive enough. Another parameter was not properly sanitized which leads to the execution of an arbitrary Windows library.	2024-08-15	7.8	CVE-2024-7263 security@eset.com
Kubernetes--ingress-nginx	A security issue was discovered in ingress-nginx where an actor with permission to create Ingress objects (in the `networking.k8s.io` or `extensions` API group) can bypass annotation validation to inject arbitrary commands and obtain the credentials of the ingress-nginx controller. In the default configuration, that credential has access to all secrets in the cluster.	2024-08-16	8.8	CVE-2024-7646 jordan@liggitt.net jordan@liggitt.net jordan@liggitt.net jordan@liggitt.net
Lenovo--Display Control Center	An insecure permissions vulnerability was reported inÂ Lenovo Display Control Center (LDCC) and Lenovo Accessories and Display Manager (LADM) that could allow a local attacker to escalate privileges.	2024-08-16	7.8	CVE-2024-2175 psirt@lenovo.com
Lenovo--Display Control Center	An insecure driver vulnerability was reported inÂ Lenovo Display Control Center (LDCC) and Lenovo Accessories and Display Manager (LADM) that could allow a local attacker to escalate privileges to kernel.	2024-08-16	7.8	CVE-2024-4763 psirt@lenovo.com
libtiff -- libtiff	A null pointer dereference flaw was found in Libtiff via `tif_dirinfo.c`. This issue may allow an attacker to trigger memory allocation failures through certain means, such as restricting the heap space size or injecting faults, causing a segmentation fault. This can cause an application crash, eventually leading to a denial of service.	2024-08-12	7.5	CVE-2024-7006 secalert@redhat.com secalert@redhat.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
litestar-org--litestar	Litestar is an Asynchronous Server Gateway Interface (ASGI) framework. In versions 2.10.0 and prior, Litestar's `docs-preview.yml` workflow is vulnerable to Environment Variable injection which may lead to secret exfiltration and repository manipulation. This issue grants a malicious actor the permission to write issues, read metadata, and write pull requests. In addition, the `DOCS_PREVIEW_DEPLOY_TOKEN` is exposed to the attacker. Commit 84d351e96aaa2a1338006d6e7221eded161f517b contains a fix for this issue.	2024-08-12	8.3	CVE-2024-42370 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
ManageEngine--ADAudit Plus	Zohocorp ManageEngine ADAudit Plus versions belowÂ 8110 are vulnerable to authenticated SQL Injection in attack surface analyzer's dashboard.	2024-08-12	8.3	CVE-2024-365180fc0942c-577d-436f-ae8e-945763c79b02
matter-labs--era-compiler-vyper	zkvyper is a Vyper compiler. Starting in version 1.3.12 and prior to version 1.5.3, since LLL IR has no Turing-incompletness restrictions, it is compiled to a loop with a much more late exit condition. It leads to a loss of funds or other unwanted behavior if the loop body contains it. However, more real-life use cases like iterating over an array are not affected. No contracts were affected by this issue, which was fixed in version 1.5.3. Upgrading and redeploying affected contracts is the only way to avoid the vulnerability.	2024-08-15	7.5	CVE-2024-43366 security-advisories@github.com
mayurik --advocate_office_management_system	A vulnerability classified as critical has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This affects an unknown part of the file delete_client.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.	2024-08-12	9.8	CVE-2024-7638 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
mayurik --advocate_office_management_system	A vulnerability classified as critical was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This vulnerability affects unknown code of the file delete_act.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.	2024-08-12	9.8	CVE-2024-7639 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
mayurik --advocate_office_management_system	A vulnerability, which was classified as critical, has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This issue affects some unknown processing of the file delete_register.php. The manipulation of the argument case_register_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	9.8	CVE-2024-7640 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
mayurik --advocate_office_management_system	A vulnerability, which was classified as critical, was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected is an unknown function of the file deactivate_act.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	9.8	CVE-2024-7641 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
mayurik --advocate_office_management_system	A vulnerability has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file activate_act.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.	2024-08-12	9.8	CVE-2024-7642 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
mayurik --best_house_rental_management	A Cross-Site Request Forgery (CSRF) vulnerability was found in SourceCodester Best House Rental Management System v1.0. This could lead to an attacker tricking the administrator into adding/modifying/deleting valid tenant data via a crafted HTML page, as demonstrated by a Delete Tenant action at the /rental/ajax.php?action=delete_tenant.	2024-08-12	8	CVE-2024-40476 cve@mitre.org cve@mitre.org
mayurik --best_house_rental_management_sys	SourceCodester Best House Rental Management System v1.0 is vulnerable to Incorrect Access Control via /rental/payment_report.php, /rental/balance_report.php, /rental/invoices.php, /rental/tenants.php, and /rental/users.php.	2024-08-12	8.8	CVE-2024-40475 cve@mitre.org cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tem				
MCJack123--craftos2	CraftOS-PC 2 is a rewrite of the desktop port of CraftOS from the popular Minecraft mod ComputerCraft using C++ and a modified version of PUC Lua, as well as SDL for drawing. Prior to version 2.8.3, users of CraftOS-PC 2 on Windows can escape the computer folder and access files anywhere without permission or notice by obfuscating `..`s to bypass the internal check preventing parent directory traversal. Version 2.8.3 contains a patch for this issue.	2024-08-16	8.2	CVE-2024-43395 security-advisories@github.com security-advisories@github.com
MediaTek, Inc.--MT2735, MT2737, MT6833, MT6835, MT6835T, MT6853, MT6855, MT6873, MT6875, MT6875T, MT6877, MT6879, MT6880, MT6883, MT6885, MT6886, MT6889, MT6890, MT6891, MT6893, MT6895, MT6895T, MT6896, MT6897, MT6980, MT6980D, MT6983, MT6985, MT6989, MT6990	In Modem, there is a possible memory corruption due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01182594; Issue ID: MSV-1529.	2024-08-14	9.8	CVE-2024-20082 security@mediatek.com
microsoft -- .net	.NET and Visual Studio Denial of Service Vulnerability	2024-08-13	7.5	CVE-2024-38168 secure@microsoft.com
microsoft -- 365_apps	Microsoft Project Remote Code Execution Vulnerability	2024-08-13	8.8	CVE-2024-38189 secure@microsoft.com
microsoft -- 365_apps	Microsoft Office Visio Remote Code Execution Vulnerability	2024-08-13	7.8	CVE-2024-38169 secure@microsoft.com
microsoft -- 365_apps	Microsoft Excel Remote Code Execution Vulnerability	2024-08-13	7.1	CVE-2024-38170 secure@microsoft.com
microsoft -- 365_apps	Microsoft PowerPoint Remote Code Execution Vulnerability	2024-08-13	7.8	CVE-2024-38171 secure@microsoft.com
microsoft -- 365_apps	Microsoft Excel Remote Code Execution Vulnerability	2024-08-13	7.8	CVE-2024-38172 secure@microsoft.com
microsoft -- app_installer	Windows App Installer Spoofing Vulnerability	2024-08-13	7.8	CVE-2024-38177 secure@microsoft.com
microsoft -- azure_connected_machine_agent	Azure Connected Machine Agent Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38098 secure@microsoft.com
microsoft -- azure_connected_	Azure Connected Machine Agent Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38162 secure@microsoft.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
machine_agent				com
microsoft -- azure_cyclecloud	Azure CycleCloud Remote Code Execution Vulnerability	2024-08-13	7.8	CVE-2024-38195 secure@microsoft.com
microsoft -- azure_health_bot	An authenticated attacker can exploit an Server-Side Request Forgery (SSRF) vulnerability in Microsoft Azure Health Bot to elevate privileges over a network.	2024-08-13	8.8	CVE-2024-38109 secure@microsoft.com
microsoft -- azure_iot_hub_device_client_sdk	Azure IoT SDK Remote Code Execution Vulnerability	2024-08-13	7	CVE-2024-38157 secure@microsoft.com
microsoft -- azure_iot_hub_device_client_sdk	Azure IoT SDK Remote Code Execution Vulnerability	2024-08-13	7	CVE-2024-38158 secure@microsoft.com
microsoft -- azure_stack_hub	Azure Stack Hub Spoofing Vulnerability	2024-08-13	9.3	CVE-2024-38108 secure@microsoft.com
microsoft -- azure_stack_hub	Azure Stack Hub Elevation of Privilege Vulnerability	2024-08-13	7	CVE-2024-38201 secure@microsoft.com
microsoft -- dynamics_365	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2024-08-13	8.2	CVE-2024-38211 secure@microsoft.com
microsoft -- officeplus	Microsoft OfficePlus Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38084 secure@microsoft.com
microsoft -- remote_desktop	Clipboard Virtual Channel Extension Remote Code Execution Vulnerability	2024-08-13	8.8	CVE-2024-38131 secure@microsoft.com
microsoft -- windows_10_1507	Windows TCP/IP Remote Code Execution Vulnerability	2024-08-13	9.8	CVE-2024-38063 secure@microsoft.com
microsoft -- windows_10_1507	Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability	2024-08-13	9.8	CVE-2024-38140 secure@microsoft.com
microsoft -- windows_10_1507	Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability	2024-08-13	9.8	CVE-2024-38199 secure@microsoft.com
microsoft -- windows_10_1507	Windows Kerberos Elevation of Privilege Vulnerability	2024-08-13	8.1	CVE-2024-29995 secure@microsoft.com
microsoft -- windows_10_1507	Windows IP Routing Management Snapin Remote Code Execution Vulnerability	2024-08-13	8.8	CVE-2024-38114 secure@microsoft.com
microsoft -- windows_10_1507	Windows IP Routing Management Snapin Remote Code Execution Vulnerability	2024-08-13	8.8	CVE-2024-38115 secure@microsoft.com
microsoft -- windows_10_1507	Windows IP Routing Management Snapin Remote Code Execution Vulnerability	2024-08-13	8.8	CVE-2024-38116 secure@microsoft.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				com
microsoft -- windows_10_1507	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-08-13	8.8	CVE-2024-38130 secure@microsoft.com
microsoft -- windows_10_1507	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	2024-08-13	8.8	CVE-2024-38144 secure@microsoft.com
microsoft -- windows_10_1507	Windows SmartScreen Security Feature Bypass Vulnerability	2024-08-13	8.8	CVE-2024-38180 secure@microsoft.com
microsoft -- windows_10_1507	Windows Kernel Elevation of Privilege Vulnerability	2024-08-13	7	CVE-2024-38106 secure@microsoft.com
microsoft -- windows_10_1507	Windows Power Dependency Coordinator Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38107 secure@microsoft.com
microsoft -- windows_10_1507	NTFS Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38117 secure@microsoft.com
microsoft -- windows_10_1507	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38125 secure@microsoft.com
microsoft -- windows_10_1507	Windows Network Address Translation (NAT) Denial of Service Vulnerability	2024-08-13	7.5	CVE-2024-38126 secure@microsoft.com
microsoft -- windows_10_1507	Windows Hyper-V Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38127 secure@microsoft.com
microsoft -- windows_10_1507	Windows Network Address Translation (NAT) Denial of Service Vulnerability	2024-08-13	7.5	CVE-2024-38132 secure@microsoft.com
microsoft -- windows_10_1507	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38134 secure@microsoft.com
microsoft -- windows_10_1507	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38141 secure@microsoft.com
microsoft -- windows_10_1507	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38142 secure@microsoft.com
microsoft -- windows_10_1507	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	2024-08-13	7.5	CVE-2024-38145 secure@microsoft.com
microsoft -- windows_10_1507	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	2024-08-13	7.5	CVE-2024-38146 secure@microsoft.com
microsoft -- windows_10_1507	Windows OLE Remote Code Execution Vulnerability	2024-08-13	7.8	CVE-2024-38152 secure@microsoft.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				com
microsoft -- windows_10_1507	Windows Kernel Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38153 secure@microsoft.com
microsoft -- windows_10_1507	Scripting Engine Memory Corruption Vulnerability	2024-08-13	7.5	CVE-2024-38178 secure@microsoft.com
microsoft -- windows_10_1507	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38193 secure@microsoft.com
microsoft -- windows_10_1507	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38196 secure@microsoft.com
microsoft -- windows_10_1507	Windows Print Spooler Elevation of Privilege Vulnerability	2024-08-13	7.5	CVE-2024-38198 secure@microsoft.com
microsoft -- windows_10_1607	Windows Network Virtualization Remote Code Execution Vulnerability	2024-08-13	9.1	CVE-2024-38159 secure@microsoft.com
microsoft -- windows_10_1607	Windows Network Virtualization Remote Code Execution Vulnerability	2024-08-13	9.1	CVE-2024-38160 secure@microsoft.com
microsoft -- windows_10_1607	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38184 secure@microsoft.com
microsoft -- windows_10_1607	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38185 secure@microsoft.com
microsoft -- windows_10_1607	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38186 secure@microsoft.com
microsoft -- windows_10_1607	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38187 secure@microsoft.com
microsoft -- windows_10_1607	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38191 secure@microsoft.com
microsoft -- windows_10_1809	Windows Kernel Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38133 secure@microsoft.com
microsoft -- windows_10_1809	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability	2024-08-13	7	CVE-2024-38136 secure@microsoft.com
microsoft -- windows_10_1809	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38215 secure@microsoft.com
microsoft -- windows_10_21h2	Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability	2024-08-13	7	CVE-2024-38137 secure@microsoft.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				com
microsoft -- windows_10_21h2	Microsoft DWM Core Library Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38147 secure@microsoft.com
microsoft -- windows_10_21h2	Windows DWM Core Library Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38150 secure@microsoft.com
microsoft -- windows_11_21h2	Windows Secure Channel Denial of Service Vulnerability	2024-08-13	7.5	CVE-2024-38148 secure@microsoft.com
microsoft -- windows_11_22h2	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability	2024-08-13	7.8	CVE-2024-38135 secure@microsoft.com
microsoft -- windows_server_2008	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-08-13	8.8	CVE-2024-38120 secure@microsoft.com
microsoft -- windows_server_2008	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-08-13	8.8	CVE-2024-38121 secure@microsoft.com
microsoft -- windows_server_2008	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-08-13	8.8	CVE-2024-38128 secure@microsoft.com
microsoft -- windows_server_2008	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2024-08-13	8.8	CVE-2024-38154 secure@microsoft.com
microsoft -- windows_server_2008	Windows DNS Spoofing Vulnerability	2024-08-13	7.5	CVE-2024-37968 secure@microsoft.com
microsoft -- windows_server_2016	Windows Deployment Services Remote Code Execution Vulnerability	2024-08-13	7.5	CVE-2024-38138 secure@microsoft.com
Microsoft-- Microsoft Edge (Chromium-based)	Microsoft Edge (HTML-based) Memory Corruption Vulnerability	2024-08-12	8.4	CVE-2024-38218 secure@microsoft.com
Microsoft-- Windows Server 2022	Windows Update Stack Elevation of Privilege Vulnerability	2024-08-14	7.8	CVE-2024-38163 secure@microsoft.com
Muhammad Rehman--Contact Form 7 Summary and Print	Cross-Site Request Forgery (CSRF), Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Muhammad Rehman Contact Form 7 Summary and Print allows Stored XSS.This issue affects Contact Form 7 Summary and Print: from n/a through 1.2.5.	2024-08-13	7.1	CVE-2024-38724 audit@patchstack.com
MultiVendorX--WC Marketplace	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MultiVendorX WC Marketplace allows Reflected XSS.This issue affects WC Marketplace: from n/a through 4.1.17.	2024-08-12	7.1	CVE-2024-43213 audit@patchstack.com
n/a--Intel(R) Core(TM) Ultra Processor stream cache mechanism	Improper isolation in the Intel(R) Core(TM) Ultra Processor stream cache mechanism may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	7.8	CVE-2023-42667 secure@intel.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--Intel(R) Ethernet Network Controllers and Adapters	Improper initialization in the Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters before version 28.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	8.8	CVE-2024-21807 secure@intel.com
n/a--Intel(R) Ethernet Network Controllers and Adapters	Improper input validation in the Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters before version 28.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	8.8	CVE-2024-21810 secure@intel.com
n/a--Intel(R) Ethernet Network Controllers and Adapters	Out-of-bounds write in Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters before version 28.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	8.8	CVE-2024-23497 secure@intel.com
n/a--Intel(R) Ethernet Network Controllers and Adapters	Wrap-around error in Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters before version 28.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	8.8	CVE-2024-23981 secure@intel.com
n/a--Intel(R) Ethernet Network Controllers and Adapters	Improper access control in Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters before version 28.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	8.8	CVE-2024-24986 secure@intel.com
n/a--Intel(R) FPGA products	improper access control in firmware for some Intel(R) FPGA products before version 24.1 may allow a privileged user to enable escalation of privilege via local access.	2024-08-14	7.9	CVE-2024-25576 secure@intel.com
n/a--Intel(R) NUC	Improper input validation in firmware for some Intel(R) NUC may allow a privileged user to potentially enableescalation of privilege via local access.	2024-08-14	7.5	CVE-2024-34163 secure@intel.com
n/a--Intel(R) Processor	Incorrect behavior order in transition between executive monitor and SMI transfer monitor (STM) in some Intel(R) Processor may allow a privileged user to potentially enable escalation of privilege via local access.	2024-08-14	7.2	CVE-2024-24853 secure@intel.com
n/a--Intel(R) Processors stream cache mechanism	Improper isolation in some Intel(R) Processors stream cache mechanism may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	7.8	CVE-2023-49141 secure@intel.com
n/a--Intel(R) Server Board S2600ST Family firmware	Improper input validation in kernel mode driver for some Intel(R) Server Board S2600ST Family firmware before version 02.01.0017 may allow a privileged user to potentially enable escalation of privilege via local access.	2024-08-14	8.2	CVE-2024-28947 secure@intel.com
n/a--Intel(R) TDX module software	Insufficient control flow management in some Intel(R) TDX module software before version 1.5.05.46.698 may allow a privileged user to potentially enable denial of service via local access.	2024-08-14	7.1	CVE-2024-21801 secure@intel.com
n/a--Intel(R) UEFI Integrator Tools on Aptio V for Intel(R) NUC	Improper access control in some Intel(R) UEFI Integrator Tools on Aptio V for Intel(R) NUC may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	7.8	CVE-2024-26022 secure@intel.com
n/a--n/a	Vulnerability in Xiexe XSOverlay before build 647 allows non-local websites to send the malicious commands to the WebSocket API, resulting in the arbitrary code execution.	2024-08-15	9.8	CVE-2024-23168 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	Insecure Permissions vulnerability in Friendica v.2023.12 allows a remote attacker to obtain sensitive information and execute arbitrary code via the cid parameter of the calendar event feature.	2024-08-15	9.8	CVE-2024-27730 cve@mitre.org cve@mitre.org
n/a--n/a	izatop bunt v0.29.19 was discovered to contain a prototype pollution via the component /esm/qs.js. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-08-12	9.8	CVE-2024-38989 cve@mitre.org cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	A SQL injection vulnerability in "/oahms/admin/forgot-password.php" in PHPGurukul Old Age Home Management System v1.0 allows an attacker to execute arbitrary SQL commands via the "email" parameter.	2024-08-12	9.8	CVE-2024-40477 cve@mitre.org cve@mitre.org
n/a--n/a	An Unrestricted file upload vulnerability was found in "/Membership/edit_member.php" of Kashipara Live Membership System v1.0, which allows attackers to execute arbitrary code via uploading a crafted PHP file.	2024-08-12	9.8	CVE-2024-40482 cve@mitre.org
n/a--n/a	A SQL injection vulnerability in "/index.php" of Kashipara Live Membership System v1.0 allows remote attackers to execute arbitrary SQL commands and bypass Login via the email or password Login parameters.	2024-08-12	9.8	CVE-2024-40486 cve@mitre.org cve@mitre.org
n/a--n/a	Gnuboard g6 6.0.7 is vulnerable to Session hijacking due to a CORS misconfiguration.	2024-08-12	9.8	CVE-2024-41475 cve@mitre.org
n/a--n/a	AMTT Hotel Broadband Operation System (HiBOS) V3.0.3.151204 and before is vulnerable to SQL Injection via /manager/card/card_detail.php.	2024-08-12	9.8	CVE-2024-41476 cve@mitre.org cve@mitre.org
n/a--n/a	An Unauthenticated Server-Side Request Forgery (SSRF) in demon callback handling in Havoc 2 0.7 allows attackers to send arbitrary network traffic originating from the team server.	2024-08-12	9.8	CVE-2024-41570 cve@mitre.org
n/a--n/a	An issue in Prestashop v.8.1.7 and before allows a remote attacker to execute arbitrary code via the module upgrade functionality.	2024-08-12	9.8	CVE-2024-41651 cve@mitre.org
n/a--n/a	A Command Injection vulnerability exists in formWriteFacMac of the httpd binary in Tenda AC9 v15.03.06.42. As a result, attacker can execute OS commands with root privileges.	2024-08-16	9.8	CVE-2024-42634 cve@mitre.org
n/a--n/a	H3C R3010 v100R002L02 was discovered to contain a hardcoded password vulnerability in /etc/shadow, which allows attackers to log in as root.	2024-08-16	9.8	CVE-2024-42637 cve@mitre.org cve@mitre.org
n/a--n/a	An issue in OWASP DefectDojo before v.1.5.3.1 allows a remote attacker to escalate privileges via the user permissions component.	2024-08-12	8.8	CVE-2023-48171 cve@mitre.org
n/a--n/a	XML External Entity (XXE) vulnerability in Terminalfour 8.0.0001 through 8.3.18 and XML JDBC versions up to 1.0.4 allows authenticated users to submit malicious XML via unspecified features which could lead to various actions such as accessing the underlying server, remote code execution (RCE), or performing Server-Side Request Forgery (SSRF) attacks.	2024-08-15	8.8	CVE-2024-22218 cve@mitre.org cve@mitre.org
n/a--n/a	Micro-Star International Z-series motherboards (Z590, Z490, and Z790) and B-series motherboards (B760, B560, B660, and B460) with firmware 7D25v14, 7D25v17 to 7D25v19, and 7D25v1A to 7D25v1H was discovered to contain a write-what-where condition in the in the SW handler for SMI 0xE3. Motherboard's with the following chipsets are affected: Intel 300, Intel 400, Intel 500, Intel 600, Intel 700, AMD 300, AMD 400, AMD 500, AMD 600 and AMD 700.	2024-08-12	8.2	CVE-2024-36877 cve@mitre.org cve@mitre.org
n/a--n/a	A SQL injection vulnerability in "/admin/quizquestion.php" in Kashipara Online Exam System v1.0 allows remote attackers to execute arbitrary SQL commands via the "eid" parameter.	2024-08-12	8.1	CVE-2024-40479 cve@mitre.org cve@mitre.org
n/a--n/a	A Cross-Site Request Forgery (CSRF) vulnerability was found in the Kashipara Live Membership System v1.0. This could lead to an attacker tricking the administrator into deleting valid member data via a crafted HTML page, as demonstrated by a Delete Member action at the /delete_members.php.	2024-08-12	8.8	CVE-2024-40488 cve@mitre.org cve@mitre.org
n/a--n/a	Cross Site Scripting vulnerability in Martin Kucej i-librarian v.5.11.0 and before allows a local attacker to execute arbitrary code via the search function in the import component.	2024-08-12	8.8	CVE-2024-40500 cve@mitre.org
n/a--n/a	File Upload vulnerability in Huizhi enterprise resource management system v.1.0 and before allows a remote attacker to execute arbitrary code via the /nssys/common/Upload. Aspx? Action=DNPageAjaxPostBack component	2024-08-15	8.8	CVE-2024-42676 cve@mitre.org
n/a--n/a	VTiger CRM <= 8.1.0 does not correctly check user privileges. A low-privileged user can interact directly with the "Migration" administrative module to disable arbitrary modules.	2024-08-16	8.3	CVE-2024-42995 cve@mitre.org
n/a--n/a	In certain Sonos products before S1 Release 11.12 and S2 release 15.9, the mt_7615.ko wireless driver does not properly validate an information element during negotiation of a WPA2 four-way handshake. This lack of validation leads to a	2024-08-12	7.8	CVE-2023-50809 cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	stack buffer overflow. This can result in remote code execution within the kernel. This affects Amp, Arc, Arc SL, Beam, Beam Gen 2, Beam SL, and Five.			
n/a--n/a	An issue was discovered in Ada Web Server 20.0. When configured to use SSL (which is not the default setting), the SSL/TLS used to establish connections to external services is done without proper hostname validation. This is exploitable by man-in-the-middle attackers.	2024-08-13	7.4	CVE-2024-37015 cve@mitre.org cve@mitre.org
n/a--n/a	A NULL pointer dereference in vercot Serva v4.6.0 allows attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	2024-08-12	7.5	CVE-2024-37826 cve@mitre.org
n/a--n/a	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in addBlacklist. Authenticated Attackers can send malicious packet to execute arbitrary commands.	2024-08-13	7.8	CVE-2024-42736 cve@mitre.org
n/a--n/a	VTiger CRM <= 8.1.0 does not properly sanitize user input before using it in a SQL statement, leading to a SQL Injection in the "CompanyDetails" operation of the "MailManager" module.	2024-08-16	7.2	CVE-2024-42994 cve@mitre.org
nickboss--WordPress File Upload	The WordPress File Upload plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 4.24.8 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.	2024-08-16	7.2	CVE-2024-7301 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
NixOS--calamares-nixos-extensions	calamares-nixos-extensions provides Calamares branding and modules for NixOS, a distribution of GNU/Linux. Users who installed NixOS through the graphical installer who used manual disk partitioning to create a setup where the system was booted via legacy BIOS rather than UEFI; some disk partitions are encrypted; but the partitions containing either `/` or `/boot` are unencrypted; have their LUKS disk encryption key file in plain text either in `/crypto_keyfile.bin`, or in a CPIO archive attached to their NixOS initrd. `nixos-install` is not affected, nor are UEFI installations, nor was the default automatic partitioning configuration on legacy BIOS systems. The problem has been fixed in calamares-nixos-extensions 0.3.17, which was included in NixOS. The current installer images for the NixOS 24.05 and unstable (24.11) channels are unaffected. The fix reached 24.05 at 2024-08-13 20:06:59 UTC, and unstable at 2024-08-15 09:00:20 UTC. Installer images downloaded before those times may be vulnerable. The best solution for affected users is probably to back up their data and do a complete reinstallation. However, the mitigation procedure in GHSA-3rvf-24q2-24ww should work solely for the case where `/` is encrypted but `/boot` is not. If `/` is unencrypted, then the `/crypto_keyfile.bin` file will need to be deleted in addition to the remediation steps in the previous advisory. This issue is a partial regression of CVE-2023-36476 / GHSA-3rvf-24q2-24ww, which was more severe as it applied to the default configuration on BIOS systems.	2024-08-16	7.8	CVE-2024-43378 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
NVIDIA--Mellanox OS	NVIDIA Mellanox OS, ONYX, Skyway, and MetroX-3 XCC contain a vulnerability in the web support, where an attacker can cause a CGI path traversal by a specially crafted URI. A successful exploit of this vulnerability might lead to escalation of privileges and information disclosure.	2024-08-12	7.5	CVE-2024-0113 psirt@nvidia.com
openeclass --openeclass	The Open eClass platform (formerly known as GUnet eClass) is a complete Course Management System. An arbitrary file upload vulnerability in the "save" functionality of the H5P module enables unauthenticated users to upload arbitrary files on the server's filesystem. This may lead in unrestricted RCE on the backend server, since the upload location is accessible from the internet. This vulnerability is fixed in 3.16.	2024-08-12	9.8	CVE-2024-38530 security-advisories@github.com security-advisories@github.com
openfga--openfga	OpenFGA is an authorization/permission engine. OpenFGA v1.5.7 and v1.5.8 are vulnerable to authorization bypass when calling Check API with a model that uses `but not` and `from` expressions and a userset. Users should downgrade to v1.5.6 as soon as possible. This downgrade is backward compatible. As of time of publication, a patch is not available but OpenFGA's maintainers are planning a patch for inclusion in a future release.	2024-08-12	7.5	CVE-2024-42473 security-advisories@github.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openhab--openhab-webui	openHAB, a provider of open-source home automation software, has add-ons including the visualization add-on CometVisu. Prior to version 4.2.1, the proxy endpoint of openHAB's CometVisu add-on can be accessed without authentication. This proxy-feature can be exploited as Server-Side Request Forgery (SSRF) to induce GET HTTP requests to internal-only servers, in case openHAB is exposed in a non-private network. Furthermore, this proxy-feature can also be exploited as a Cross-Site Scripting (XSS) vulnerability, as an attacker is able to re-route a request to their server and return a page with malicious JavaScript code. Since the browser receives this data directly from the openHAB CometVisu UI, this JavaScript code will be executed with the origin of the CometVisu UI. This allows an attacker to exploit call endpoints on an openHAB server even if the openHAB server is located in a private network. (e.g. by sending an openHAB admin a link that proxies malicious JavaScript.) This issue may lead up to Remote Code Execution (RCE) when chained with other vulnerabilities. Users should upgrade to version 4.2.1 of the CometVisu add-on of openHAB to receive a patch.	2024-08-12	10	CVE-2024-42467 security-advisories@github.com security-advisories@github.com security-advisories@github.com
openhab--openhab-webui	openHAB, a provider of open-source home automation software, has add-ons including the visualization add-on CometVisu. Prior to version 4.2.1, CometVisu's file system endpoints don't require authentication and additionally the endpoint to update an existing file is susceptible to path traversal. This makes it possible for an attacker to overwrite existing files on the openHAB instance. If the overwritten file is a shell script that is executed at a later time, this vulnerability can allow remote code execution by an attacker. Users should upgrade to version 4.2.1 to receive a patch.	2024-08-12	9.8	CVE-2024-42469 security-advisories@github.com security-advisories@github.com
opentext -- directory_services	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in OpenText OpenText Directory Services allows Path Traversal.This issue affects OpenText Directory Services: from 16.4.2 before 24.1.	2024-08-12	9.8	CVE-2023-7249 security@opentext.com
oretnom23 -- car_driving_school_management_system	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been classified as problematic. This affects the function save_users of the file admin/user/index.php. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	8.8	CVE-2024-7661 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- clinics_patient_management_system	A vulnerability has been found in SourceCodester Clinics Patient Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /medicines.php. The manipulation of the argument medicine_name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-13	7.5	CVE-2024-7750 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- clinics_patient_management_system	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /update_medicine.php. The manipulation of the argument hidden_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-13	7.5	CVE-2024-7751 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- clinics_patient_management_system	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /user_images/. The manipulation leads to direct request. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-14	7.5	CVE-2024-7753 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- clinics_patient_management_system	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /ajax/check_medicine_name.php. The manipulation of the argument user_name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-14	7.5	CVE-2024-7754 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Parcel Panel--ParcelPanel	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Parcel Panel ParcelPanel allows Reflected XSS.This issue affects ParcelPanel: from n/a through 4.3.2.	2024-08-12	7.1	CVE-2024-43163 audit@patchstack.com
Pepperl+Fuchs--ICDM-RX/TCP-DB9/RJ45-DIN	An unauthenticated remote attacker may use stored XSS vulnerability to obtain information from a user or reboot the affected device once.	2024-08-13	7.1	CVE-2024-38502 info@cert.vde.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Pepperl+Fuchs--ICDM-RX/TCP-DB9/RJ45-DIN	An unauthenticated remote attacker may use a reflected XSS vulnerability to obtain information from a user or reboot the affected device once.	2024-08-13	7.1	CVE-2024-5849 info@cert.vde.com
Phoenix Contact--CHARX SEC-3000 (1139022)	An unauthenticated remote attacker can use this vulnerability to change the device configuration due to a file writeable for short time after system startup.	2024-08-13	7.5	CVE-2024-3913 info@cert.vde.com
PHOENIX CONTACT--CHARX SEC-3000	A remote unauthenticated attacker can use the firmware update feature on the LAN interface of the device to reset the password for the predefined, low-privileged user "user-app" to the default password.	2024-08-13	8.6	CVE-2024-6788 info@cert.vde.com
Pierre Lebedel--Kodex Posts likes	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pierre Lebedel Kodex Posts likes allows Reflected XSS.This issue affects Kodex Posts likes: from n/a through 2.5.0.	2024-08-12	7.1	CVE-2024-43217 audit@patchstack.com
projectsend -- projectsend	A vulnerability, which was classified as problematic, was found in projectsend up to r1605. Affected is the function generate_random_string of the file includes/functions.php of the component Password Reset Token Handler. The manipulation leads to insufficiently random values. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. Upgrading to version r1720 is able to address this issue. The name of the patch is aa27eb97edc2ff2b203f97e6675d7b5ba0a22a17. It is recommended to upgrade the affected component.	2024-08-12	7.5	CVE-2024-7659 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
pxlrbt--filament-excel	Filament Excel enables excel export for Filament admin resources. The export download route `/filament-excel/{path}` allowed downloading any file without login when the webserver allows `../` in the URL. Patched with Version v2.3.3.	2024-08-12	7.5	CVE-2024-42485 security-advisories@github.com security-advisories@github.com
rabilal--JS Help Desk The Ultimate Help Desk & Support Plugin	The JS Help Desk - The Ultimate Help Desk & Support Plugin plugin for WordPress is vulnerable to PHP Code Injection leading to Remote Code Execution in all versions up to, and including, 2.8.6 via the 'storeTheme' function. This is due to a lack of sanitization on user-supplied values, which replace values in the style.php file, along with missing capability checks. This makes it possible for unauthenticated attackers to execute code on the server. This issue was partially patched in 2.8.6 when the code injection issue was resolved, and fully patched in 2.8.7 when the missing authorization and cross-site request forgery protection was added.	2024-08-13	9.8	CVE-2024-7094 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
realmag777--HUSKY	Improper Privilege Management vulnerability in realmag777 HUSKY allows Privilege Escalation.This issue affects HUSKY: from n/a through 1.3.6.1.	2024-08-13	9.1	CVE-2024-43121 audit@patchstack.com
Red Hat--Fence Agents Remediation Operator	A flaw was found in fence agents that rely on SSH/Telnet. This vulnerability can allow a Remote Code Execution (RCE) primitive by supplying an arbitrary command to execute in the --ssh-path/--telnet-path arguments. A low-privilege user, for example, a user with developer access, can create a specially crafted FenceAgentsRemediation for a fence agent supportingÂ --ssh-path/--telnet-path arguments to execute arbitrary commands on the operator's pod. This RCE leads to a privilege escalation, first as the service account running the operator, then to another service account with cluster-admin privileges.	2024-08-12	8.8	CVE-2024-5651 secalert@redhat.com secalert@redhat.com
redhat -- openshift_ai	A vulnerability was found in OpenShift AI that allows for authentication bypass and privilege escalation across models within the same namespace. When deploying AI models, the UI provides the option to protect models with authentication. However, credentials from one model can be used to access other models and APIs within the same namespace. The exposed ServiceAccount tokens, visible in the UI, can be utilized with oc --token={token} to exploit the elevated view privileges	2024-08-12	8.8	CVE-2024-7557 secalert@redhat.com secalert@redhat.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	associated with the ServiceAccount, leading to unauthorized access to additional resources.			
rems -- accounts_manager_app	A vulnerability, which was classified as critical, has been found in SourceCodester Accounts Manager App 1.0. This issue affects some unknown processing of the file /endpoint/delete-account.php. The manipulation of the argument account leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-13	9.8	CVE-2024-7748 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
rems -- daily_calories_monitoring_tool	Sourcecodester Daily Calories Monitoring Tool v1.0 is vulnerable to SQL Injection via "delete-calorie.php."	2024-08-12	9.8	CVE-2024-40472 cve@mitre.org cve@mitre.org
rems -- leads_manager_tool	A vulnerability was found in SourceCodester Leads Manager Tool 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /endpoint/delete-leads.php of the component Delete Leads Handler. The manipulation of the argument leads leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	9.8	CVE-2024-7643 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Roland Barker, xnau webdesign--Participants Database	Deserialization of Untrusted Data vulnerability in Roland Barker, xnau webdesign Participants Database allows Object Injection.This issue affects Participants Database: from n/a through 2.5.9.2.	2024-08-13	9.8	CVE-2024-43141 audit@patchstack.com
samsung -- magicinfo_9_server	Improper limitation of a pathname to a restricted directory vulnerability in Samsung MagicINFO 9 Server version before 21.1050 allows attackers to write arbitrary file as system authority.	2024-08-12	7.5	CVE-2024-7399 PSIRT@samsung.com
SAP_SE--SAP BEx Web Java Runtime Export Web Service	BEx Web Java Runtime Export Web Service does not sufficiently validate an XML document accepted from an untrusted source. An attacker can retrieve information from the SAP ADS system and exhaust the number of XMLForm service which makes the SAP ADS rendering (PDF creation) unavailable. This affects the confidentiality and availability of the application.	2024-08-13	8.2	CVE-2024-42374 cna@sap.com cna@sap.com
SAP_SE--SAP BusinessObjects Business Intelligence Platform	In SAP BusinessObjects Business Intelligence Platform, if Single Signed On is enabled on Enterprise authentication, an unauthorized user can get a logon token using a REST endpoint. The attacker can fully compromise the system resulting in High impact on confidentiality, integrity and availability.	2024-08-13	9.8	CVE-2024-41730 cna@sap.com cna@sap.com
SAP_SE--SAP Commerce Cloud	Some OCC API endpoints in SAP Commerce Cloud allows Personally Identifiable Information (PII) data, such as passwords, email addresses, mobile numbers, coupon codes, and voucher codes, to be included in the request URL as query or path parameters. On successful exploitation, this could lead to a High impact on confidentiality and integrity of the application.	2024-08-13	7.4	CVE-2024-33003 cna@sap.com cna@sap.com
Scooter Software--Beyond Compare	A vulnerability has been found in Scooter Software Beyond Compare up to 3.3.5.15075 and classified as critical. Affected by this vulnerability is an unknown functionality in the library 7zxa.dll. The manipulation leads to uncontrolled search path. Attacking locally is a requirement. The real existence of this vulnerability is still doubted at the moment. NOTE: The vendor explains that a system must be breached before exploiting this issue.	2024-08-16	7.8	CVE-2024-7886 cna@vuldb.com cna@vuldb.com cna@vuldb.com
SECOM--Dr.ID Access control system	Dr.ID Access Control System from SECOM does not properly validate a specific page parameter, allowing unauthenticated remote attackers to inject SQL commands to read, modify, and delete database contents.	2024-08-14	9.8	CVE-2024-7731 twcert@cert.org.tw twcert@cert.org.tw
SECOM--Dr.ID Attendance system	Dr.ID Access Control System from SECOM does not properly validate a specific page parameter, allowing unauthenticated remote attackers to inject SQL commands to read, modify, and delete database contents.	2024-08-14	9.8	CVE-2024-7732 twcert@cert.org.tw twcert@cert.org.tw
Sender--Sender Newsletter, SMS and Email Marketing	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Sender Sender - Newsletter, SMS and Email Marketing Automation for WooCommerce allows Reflected XSS.This issue affects Sender -	2024-08-12	7.1	CVE-2024-43126 audit@patchstack.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Automation for WooCommerce	Newsletter, SMS and Email Marketing Automation for WooCommerce: from n/a through 2.6.14.			
siemens -- location_intelligence	A vulnerability has been identified in Location Intelligence family (All versions < V4.4). The web server of affected products is configured to support weak ciphers by default. This could allow an unauthenticated attacker in an on-path position to to read and modify any data passed over the connection between legitimate clients and the affected device.	2024-08-13	7.5	CVE-2024-41681 productcert@siemens.com
siemens -- sinec_nms	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application does not properly validate user input to a privileged command queue. This could allow an authenticated attacker to execute OS commands with elevated privileges.	2024-08-13	9.1	CVE-2024-41940 productcert@siemens.com
siemens -- sinec_nms	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application does not properly enforce authorization checks. This could allow an authenticated attacker to bypass the checks and elevate their privileges on the application.	2024-08-13	8.8	CVE-2024-41939 productcert@siemens.com
siemens -- sinec_nms	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application executes a subset of its services as `NT AUTHORITY\SYSTEM`. This could allow a local attacker to execute operating system commands with elevated privileges.	2024-08-13	7.8	CVE-2024-36398 productcert@siemens.com
siemens -- sinec_traffic_analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application mounts the container's root filesystem with read and write privileges. This could allow an attacker to alter the container's filesystem leading to unauthorized modifications and data corruption.	2024-08-13	7.2	CVE-2024-41903 productcert@siemens.com
siemens -- sinec_traffic_analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application do not properly enforce restriction of excessive authentication attempts. This could allow an unauthenticated attacker to conduct brute force attacks against legitimate user credentials or keys.	2024-08-13	7.5	CVE-2024-41904 productcert@siemens.com
Siemens--JT2Go	The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process.	2024-08-12	7.8	CVE-2023-7066 ics-cert@hq.dhs.gov ics-cert@hq.dhs.gov
Siemens--NX	A vulnerability has been identified in NX (All versions < V2406.3000). The affected applications contains an out of bounds read vulnerability while parsing specially crafted PRT files. This could allow an attacker to crash the application or execute code in the context of the current process.	2024-08-13	7.8	CVE-2024-41908 productcert@siemens.com
Siemens--RUGGEDCOM RM1224 LTE(4G) EU	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.1), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.1), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.1), SCALANCE M812-1 ADSL-Router family (All versions < V8.1), SCALANCE M816-1 ADSL-Router family (All versions < V8.1), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.1), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.1), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.1), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.1), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.1), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.1), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.1), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.1), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.1), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.1), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.1), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.1), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.1), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.1), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.1), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.1), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.1). Affected devices do not properly validate input in specific VPN configuration fields. This could allow an authenticated remote attacker to execute arbitrary code on the device.	2024-08-13	7.2	CVE-2024-41976 productcert@siemens.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Siemens--RUGGEDCOM RM1224 LTE(4G) EU	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.1), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.1), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.1), SCALANCE M812-1 ADSL-Router family (All versions < V8.1), SCALANCE M816-1 ADSL-Router family (All versions < V8.1), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.1), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.1), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.1), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.1), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.1), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.1), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.1), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.1), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.1), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.1), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.1), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.1), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.1), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.1), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.1), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.1), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.1). Affected devices do not properly enforce isolation between user sessions in their web server component. This could allow an authenticated remote attacker to escalate their privileges on the devices.	2024-08-13	7.1	CVE-2024-41977 productcert@siemens.com
skyportlabs--skyportd	Skyport Daemon (skyportd) is the daemon for the Skyport Panel. By making thousands of folders & files (easy due to skyport's lack of rate limiting on createFolder. createFile), skyportd in a lot of cases will cause 100% CPU usage and an OOM, probably crashing the system. This is fixed in 0.2.2.	2024-08-12	7.5	CVE-2024-42481 security-advisories@github.com
solarwinds -- web_help_desk	SolarWinds Web Help Desk was found to be susceptible to a Java Deserialization Remote Code Execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. While it was reported as an unauthenticatedÂ vulnerability, SolarWinds has been unable to reproduce itÂ without authenticationÂ after thorough testing. Â However, out of an abundance of caution, we recommend all Web Help Desk customers apply the patch, which is now available.	2024-08-13	9.8	CVE-2024-28986 psirt@solarwinds.com psirt@solarwinds.com
SourceCodester--Simple Online Bidding System	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been classified as critical. Affected is an unknown function of the file /simple-online-bidding-system/bidding/admin/ajax.php?action=login. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	7.3	CVE-2024-7797 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Simple Online Bidding System	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /simple-online-bidding-system/bidding/admin/ajax.php?action=login2. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	7.3	CVE-2024-7798 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
TagDiv--tagDiv Opt-In Builder	The tagDiv Opt-In Builder plugin is vulnerable to Blind SQL Injection via the 'subscriptionCouponId' parameter via the 'create_stripe_subscription' REST API endpoint in versions up to, and including, 1.4.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with administrator-level privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-08-17	7.2	CVE-2023-3416 security@wordfence.com security@wordfence.com
TagDiv--tagDiv Opt-In Builder	The tagDiv Opt-In Builder plugin is vulnerable to Blind SQL Injection via the 'couponId' parameter of the 'recreate_stripe_subscription' REST API endpoint in versions up to, and including, 1.4.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with administrator-level privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-08-17	7.2	CVE-2023-3419 security@wordfence.com security@wordfence.com
tc39--ecma262	ECMA-262 is the language specification for the scripting language ECMAScript. A problem in the ECMAScript (JavaScript) specification of async generators,	2024-08-15	8.6	CVE-2024-43357 security-

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	introduced by a May 2021 spec refactor, may lead to mis-implementation in a way that could present as a security vulnerability, such as type confusion and pointer dereference. The internal async generator machinery calls regular promise resolver functions on IteratorResult (`{ done, value }`) objects that it creates, assuming that the IteratorResult objects will not be then-ables. Unfortunately, these IteratorResult objects inherit from `Object.prototype`, so these IteratorResult objects can be made then-able, triggering arbitrary behaviour, including re-entering the async generator machinery in a way that violates some internal invariants. The ECMAScript specification is a living standard and the issue has been addressed at the time of this advisory's public disclosure. JavaScript engine implementors should refer to the latest specification and update their implementations to comply with the `AsyncGenerator` section. ## References - https://github.com/tc39/ecma262/commit/1e24a286d0a327d08e1154926b3ee79820232727 - https://bugzilla.mozilla.org/show_bug.cgi?id=1901411 - https://github.com/boa-dev/boa/security/advisories/GHSA-f67q-wr6w-23jq - https://bugs.webkit.org/show_bug.cgi?id=275407 - https://issues.chromium.org/issues/346692561 - https://www.cve.org/CVERecord?id=CVE-2024-7652			advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
Team Johnlong software--Raiden MAILD Remote Management System	Raiden MAILD Remote Management System from Team Johnlong Software has a Relative Path Traversal vulnerability, allowing unauthenticated remote attackers to read arbitrary file on the remote server.	2024-08-12	7.5	CVE-2024-7693 twcert@cert.org.tw twcert@cert.org.tw
TeamT5--ThreatSonar Anti-Ransomware	ThreatSonar Anti-Ransomware from TeamT5 does not properly validate the content of uploaded files. Remote attackers with administrator privileges on the product platform can upload malicious files, which can be used to execute arbitrary system command on the server.	2024-08-12	7.2	CVE-2024-7694 twcert@cert.org.tw twcert@cert.org.tw
TECNO--com.transsion.carlcare	Logical vulnerability in the mobile application (com.transsion.carlcare) may lead to user information leakage risks.	2024-08-12	7.5	CVE-2024-7697 907edf6c-bf03-423e-ab1a-8da27e1aa1ea 907edf6c-bf03-423e-ab1a-8da27e1aa1ea
tenda --fh1201_firmware	An issue in the handler function in /goform/telnet of Tenda FH1201 v1.2.0.14 (408) allows attackers to execute arbitrary commands via a crafted HTTP request.	2024-08-15	9.8	CVE-2024-42947 cve@mitre.org
tenda --fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromP2pListFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42940 cve@mitre.org
tenda --fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the wanmode parameter in the fromAdvSetWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42941 cve@mitre.org
tenda --fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the PPPOEPassword parameter in the fromAdvSetWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42943 cve@mitre.org
tenda --fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromNatlimit function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42944 cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenda -- fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromVirtualSer function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42946 cve@mitre.org
tenda -- fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the delno parameter in the fromPptpUserSetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42948 cve@mitre.org
tenda -- fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the Go parameter in the fromSafeClientFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42950 cve@mitre.org
tenda -- fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the mit_pptpusrpw parameter in the fromWizardHandle function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42951 cve@mitre.org
tenda -- fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromqossetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42952 cve@mitre.org
tenda -- fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromSafeClientFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42955 cve@mitre.org
tenda -- fh1206_firmware	An issue in the handler function in /goform/telnet of Tenda FH1206 v02.03.01.35 allows attackers to execute arbitrary commands via a crafted HTTP request.	2024-08-15	9.8	CVE-2024-42978 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the Go parameter in the fromSafeUrlFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42968 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromSafeUrlFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42969 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromSetIpBind function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42973 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromwebExcptypemanFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42974 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromSafeClientFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42976 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the qos parameter in the fromqossetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42977 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the frmL7ProtForm function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42979 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the frmL7ImForm function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42980 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the delno parameter in the fromPptpUserSetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42981 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromVirtualSer function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42982 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the pptpPPW parameter in the fromAdvSetWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42983 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromP2pListFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42984 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromNatlimit function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42985 cve@mitre.org
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the PPPOEPassword parameter in the fromAdvSetWan function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42986 cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenda -- fh1206_firmware	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the modino parameter in the fromPptpUserAdd function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42987 cve@mitre.org
Tenda--FH1206	A vulnerability was found in Tenda FH1206 1.2.0.8(8155) and classified as critical. This issue affects the function fromGstDhcpSetSer of the file /goform/GstDhcpSetSer. The manipulation of the argument dips leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-12	8.8	CVE-2024-7613 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Tenda--FH1206	A vulnerability was found in Tenda FH1206 1.2.0.8(8155). It has been classified as critical. Affected is the function fromqossetting of the file /goform/qossetting. The manipulation of the argument page leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-12	8.8	CVE-2024-7614 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Tenda--FH1206	A vulnerability was found in Tenda FH1206 1.2.0.8. It has been declared as critical. Affected by this vulnerability is the function fromSafeClientFilter/fromSafeMacFilter/fromSafeUrlFilter. The manipulation leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-12	8.8	CVE-2024-7615 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Tenda--FH1206	A vulnerability was found in Tenda FH1206 02.03.01.35 and classified as critical. Affected by this issue is the function formSafeEmailFilter of the file /goform/SafeEmailFilter of the component HTTP POST Request Handler. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-13	8.8	CVE-2024-7707 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
tendacn -- fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the frmL7ImForm function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42942 cve@mitre.org
tendacn -- fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromAddressNat function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42945 cve@mitre.org
tendacn -- fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the qos parameter in the fromqossetting function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42949 cve@mitre.org
tendacn -- fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the PPW parameter in the fromWizardHandle function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42953 cve@mitre.org
tendacn -- fh1201_firmware	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromwebExcptypemanFilter function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	2024-08-15	7.5	CVE-2024-42954 cve@mitre.org
Themewinter--WPCafe	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Themewinter WPCafe allows PHP Local File Inclusion.This issue affects WPCafe: from n/a through 2.2.28.	2024-08-13	7.5	CVE-2024-43135 audit@patchstack.com
thiagosf--Skitter Slideshow	The Skitter Slideshow plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.5.2 via the /image.php file. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	2024-08-17	7.2	CVE-2022-1751 security@wordfence.com security@wordfence.com security@wordfence.com
Tosei--Online Store Management System	A vulnerability classified as critical was found in Tosei Online Store Management System ãƒ‍ãƒƒãƒˆå•—è^—ç®¡ç†ã‚·ã‚¹ãƒ†ãƒ 4.02/4.03/4.04. This vulnerability affects unknown code of the component Backend. The manipulation leads to use of default credentials. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-17	7.3	CVE-2024-7898 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
totolink -- a3002r_firmware	TOTOLINK A3002R v4.0.0-B20230531.1404 contains a buffer overflow vulnerability in /bin/boa via formParentControl.	2024-08-12	9.8	CVE-2024-42520 cve@mitre.org

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totolink -- a3100r_firmware	TOTOLINK A3100R V4.1.2cu.5050_B20200504 has a buffer overflow vulnerability in the password parameter in the loginauth function.	2024-08-12	9.8	CVE-2024-42546 cve@mitre.org
totolink -- a3100r_firmware	TOTOLINK A3100R V4.1.2cu.5050_B20200504 has a buffer overflow vulnerability in the http_host parameter in the loginauth function.	2024-08-12	9.8	CVE-2024-42547 cve@mitre.org
totolink -- a3700r_firmware	TOTOLINK A3700R v9.1.2u.5822_B20200513 has a buffer overflow vulnerability in the http_host parameter in the loginauth function.	2024-08-12	9.8	CVE-2024-42543 cve@mitre.org
totolink -- a3700r_firmware	TOTOLINK A3700R v9.1.2u.5822_B20200513 has a buffer overflow vulnerability in the ssid parameter in setWizardCfg function.	2024-08-12	9.8	CVE-2024-42545 cve@mitre.org
totolink -- lr350_firmware	Incorrect access control in TOTOLINK LR350 V9.3.5u.6369_B20220309 allows attackers to obtain the apmib configuration file, which contains the username and the password, via a crafted request to /cgi-bin/ExportSettings.sh.	2024-08-15	9.8	CVE-2024-42967 cve@mitre.org
totolink -- n350rt_firmware	Incorrect access control in TOTOLINK N350RT V9.3.5u.6139_B20201216 allows attackers to obtain the apmib configuration file, which contains the username and the password, via a crafted request to /cgi-bin/ExportSettings.sh.	2024-08-15	9.8	CVE-2024-42966 cve@mitre.org
totolink -- x5000r_firmware	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in delBlacklist. Authenticated Attackers can send malicious packet to execute arbitrary commands.	2024-08-13	8.8	CVE-2024-42737 cve@mitre.org
totolink -- x5000r_firmware	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setDmzCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	2024-08-13	8.8	CVE-2024-42738 cve@mitre.org
totolink -- x5000r_firmware	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setAccessDeviceCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	2024-08-13	8.8	CVE-2024-42739 cve@mitre.org
totolink -- x5000r_firmware	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setL2tpServerCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	2024-08-12	8.8	CVE-2024-42741 cve@mitre.org
totolink -- x5000r_firmware	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setUrlFilterRules. Authenticated Attackers can send malicious packet to execute arbitrary commands.	2024-08-12	8.8	CVE-2024-42742 cve@mitre.org
totolink -- x5000r_firmware	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setSyslogCfg . Authenticated Attackers can send malicious packet to execute arbitrary commands.	2024-08-12	8.8	CVE-2024-42743 cve@mitre.org
totolink -- x5000r_firmware	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setModifyVpnUser. Authenticated Attackers can send malicious packet to execute arbitrary commands.	2024-08-12	8.8	CVE-2024-42744 cve@mitre.org
totolink -- x5000r_firmware	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setUPnPCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	2024-08-12	8.8	CVE-2024-42745 cve@mitre.org
totolink -- x5000r_firmware	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setWanIeCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	2024-08-12	8.8	CVE-2024-42747 cve@mitre.org
totolink -- x5000r_firmware	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setWiFiWpsCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	2024-08-12	8.8	CVE-2024-42748 cve@mitre.org
veribase -- order_management	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Veribilim Software Veribase Order Management allows OS Command Injection.This issue affects Veribase Order Management: before v4.010.2.	2024-08-12	9.8	CVE-2024-6917 iletisim@usom.gov.tr
Vonets--VAR1200-H	Stack-based buffer overflow vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to execute arbitrary code.	2024-08-12	10	CVE-2024-39791 ics-cert@hq.dhs.gov
Vonets--VAR1200-H	Multiple OS command injection vulnerabilities affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an authenticated remote attacker to execute arbitrary OS commands via various endpoint parameters.	2024-08-12	9.1	CVE-2024-37023 ics-cert@hq.dhs.gov
Vonets--VAR1200-H	Improper check or handling of exceptional conditions vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enable an unauthenticated remote attacker to cause a denial of service.	2024-08-12	9.1	CVE-2024-39815 ics-

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	A specially-crafted HTTP request to pre-authentication resources can crash the service.			cert@hq.dhs.gov
Vonets--VAR1200-H	Improper access control vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to bypass authentication and factory reset the device via unprotected goform endpoints.	2024-08-12	8.6	CVE-2024-29082 ics-cert@hq.dhs.gov
Vonets--VAR1200-H	An improper authentication vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior enables an unauthenticated remote attacker to bypass authentication via a specially crafted direct request when another user has an active session.	2024-08-12	8.6	CVE-2024-42001 ics-cert@hq.dhs.gov
Vonets--VAR1200-H	A directory traversal vulnerability affecting Vonets industrial wifi bridge relays and wifi bridge repeaters, software versions 3.3.23.6.9 and prior, enables an unauthenticated remote attacker to read arbitrary files and bypass authentication.	2024-08-12	7.5	CVE-2024-41936 ics-cert@hq.dhs.gov
wanglongcn--ltcms	A vulnerability has been found in wanglongcn ltcms 1.0.20 and classified as critical. This vulnerability affects the function download of the file /api/test/download of the component API Endpoint. The manipulation of the argument url leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-13	7.3	CVE-2024-7740 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
wanglongcn--ltcms	A vulnerability was found in wanglongcn ltcms 1.0.20. It has been classified as critical. Affected is the function multiDownload of the file /api/file/multiDownload of the component API Endpoint. The manipulation of the argument file leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-13	7.3	CVE-2024-7742 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
wanglongcn--ltcms	A vulnerability was found in wanglongcn ltcms 1.0.20. It has been declared as critical. Affected by this vulnerability is the function downloadUrl of the file /api/file/downloadUrl of the component API Endpoint. The manipulation of the argument file leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-13	7.3	CVE-2024-7743 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
WofficeIO--Woffice	Improper Privilege Management vulnerability in WofficeIO Woffice allows Privilege Escalation.This issue affects Woffice: from n/a through 5.4.10.	2024-08-13	9.8	CVE-2024-43153 audit@patchstack.com
WP Swings--Wallet System for WooCommerce	Missing Authorization vulnerability in WP Swings Wallet System for WooCommerce allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Wallet System for WooCommerce: from n/a through 2.5.13.	2024-08-13	7.5	CVE-2024-38699 audit@patchstack.com
WPFactory--Products, Order & Customers Export for WooCommerce	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPFactory Products, Order & Customers Export for WooCommerce allows Reflected XSS.This issue affects Products, Order & Customers Export for WooCommerce: from n/a through 2.0.11.	2024-08-12	7.1	CVE-2024-43127 audit@patchstack.com
WPWeb--Docket (WooCommerce Collections / Wishlist / Watchlist)	Incorrect Authorization vulnerability in WPWeb Docket (WooCommerce Collections / Wishlist / Watchlist) allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Docket (WooCommerce Collections / Wishlist / Watchlist): from n/a before 1.7.0.	2024-08-13	7.5	CVE-2024-43131 audit@patchstack.com
WPWeb--WooCommerce - Social Login	The WooCommerce - Social Login plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.7.5. This is due to the use of loose comparison of the activation code in the 'woo_slg_confirm_email_user' 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 userID. This requires the email module to be enabled.	2024-08-12	9.8	CVE-2024-7503 security@wordfence.com security@wordfence.com
WPWeb--WooCommerce PDF Vouchers	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WPWeb WooCommerce PDF Vouchers allows File Manipulation.This issue affects WooCommerce PDF Vouchers: from n/a before 4.9.5.	2024-08-13	8.6	CVE-2024-39651 audit@patchstack.com
wurmlab -- sequenceserver	SequenceServer lets you rapidly set up a BLAST+ server with an intuitive user interface for personal or group use. Several HTTP endpoints did not properly sanitize user input and/or query parameters. This could be exploited to inject and run unwanted shell commands. This vulnerability has been fixed in 3.1.2.	2024-08-14	9.8	CVE-2024-42360 security-advisories@github.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				security-advisories@github.com
xpeedstudio--MetForm Contact Form, Survey, Quiz, & Custom Form Builder for Elementor	The Metform Elementor Contact Form Builder for WordPress is vulnerable to Arbitrary File Upload due to insufficient file type validation in versions up to, and including, 3.2.4. This allows unauthenticated visitors to perform a "double extension" attack and upload files containing a malicious extension but ending with a benign extension, which may make remote code execution possible in some configurations.	2024-08-17	8.1	CVE-2023-0714 security@wordfence.com security@wordfence.com security@wordfence.com
xwikisas--xwiki-pro-macros	Pro Macros provides XWiki rendering macros. Missing escaping in the Viewpdf macro allows any user with view right on the `CKEditor.HTMLConverter` page or edit or comment right on any page to perform remote code execution. Other macros like Viewppt are vulnerable to the same kind of attack. This vulnerability is fixed in 1.10.1.	2024-08-12	10	CVE-2024-42489 security-advisories@github.com security-advisories@github.com security-advisories@github.com
Zabbix--Zabbix	An administrator with restricted permissions can exploit the script execution functionality within the Monitoring Hosts section. The lack of default escaping for script parameters enabled this user ability to execute arbitrary code via the Ping script, thereby compromising infrastructure.	2024-08-12	9.9	CVE-2024-22116 security@zabbix.com
Zabbix--Zabbix	Within Zabbix, users have the ability to directly modify memory pointers in the JavaScript engine.	2024-08-12	9.1	CVE-2024-36461 security@zabbix.com
Zabbix--Zabbix	The front-end audit log allows viewing of unprotected plaintext passwords, where the passwords are displayed in plain text.	2024-08-12	8.1	CVE-2024-36460 security@zabbix.com
Zabbix--Zabbix	Uncontrolled resource consumption refers to a software vulnerability where a attacker or system uses excessive resources, such as CPU, memory, or network bandwidth, without proper limitations or controls. This can cause a denial-of-service (DoS) attack or degrade the performance of the affected system.	2024-08-12	7.5	CVE-2024-36462 security@zabbix.com
zimbra -- collaboration	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. The zmmailboxdmgr binary, a component of ZCS, is intended to be executed by the zimbra user with root privileges for specific mailbox operations. However, an attacker can escalate privileges from the zimbra user to root, because of improper handling of input arguments. An attacker can execute arbitrary commands with elevated privileges, leading to local privilege escalation.	2024-08-12	7.8	CVE-2024-27442 cve@mitre.org cve@mitre.org
zimbra -- collaboration	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. The vulnerability involves unauthenticated local file inclusion (LFI) in a web application, specifically impacting the handling of the packages parameter. Attackers can exploit this flaw to include arbitrary local files without authentication, potentially leading to unauthorized access to sensitive information. The vulnerability is limited to files within a specific directory.	2024-08-12	7.5	CVE-2024-33535 cve@mitre.org cve@mitre.org
zohocorp -- manageengine_adaudit_plus	Zohocorp ManageEngine ADAudit Plus versions belowÂ 8003 are vulnerable to authenticated SQL Injection in aggregate reports' search option.	2024-08-12	8.8	CVE-2024-36034 0fc0942c-577d-436f-ae8e-945763c79b02
zohocorp -- manageengine_adaudit_plus	Zohocorp ManageEngine ADAudit Plus versions belowÂ 8003 are vulnerable to authenticated SQL Injection in user session recording.	2024-08-12	8.8	CVE-2024-36035 0fc0942c-577d-436f-ae8e-945763c79b02
zohocorp -- manageengine_adaudit_plus	Zohocorp ManageEngine ADAudit Plus versions belowÂ 8110 are vulnerable to authenticated SQL Injection in attack surface analyzer's export option.	2024-08-12	8.8	CVE-2024-5487 0fc0942c-577d-436f-ae8e-

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				945763c79b02
zohocorp -- manageengine_adaudit_plus	Zohocorp ManageEngine ADAudit Plus versions belowÂ 8110 are vulnerable to authenticated SQL Injection in file auditing configuration.	2024-08-12	8.8	CVE-2024-55270fc0942c-577d-436f-ae8e-945763c79b02
ZoneMinder--zoneminder	ZoneMinder is a free, open source closed-circuit television software application. ZoneMinder is affected by a time-based SQL Injection vulnerability. This vulnerability is fixed in 1.36.34 and 1.37.61.	2024-08-12	9.8	CVE-2024-43360 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
ZoneMinder--zoneminder	ZoneMinder is a free, open source Closed-circuit television software application. In WWW/AJAX/watch.php, Line: 51 takes a few parameter in sql query without sanitizing it which makes it vulnerable to sql injection. This vulnerability is fixed in 1.36.34.	2024-08-12	7.1	CVE-2023-41884 security-advisories@github.com security-advisories@github.com security-advisories@github.com
Zoom Communications Inc.--Zoom Workplace Apps and Rooms Clients	Buffer overflow in some Zoom Workplace Apps and Rooms Clients may allow an authenticated user to conduct an escalation of privilege via network access.	2024-08-14	8.5	CVE-2024-39825 security@zoom.us
Zoom Communications Inc.--Zoom Workplace Apps and SDKs	Protection mechanism failure for some Zoom Workplace Apps and SDKs may allow an authenticated user to conduct information disclosure via network access.	2024-08-14	7.5	CVE-2024-39818 security@zoom.us

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
10up--Simple Local Avatars	Cross-Site Request Forgery (CSRF) vulnerability in 10up Simple Local Avatars.This issue affects Simple Local Avatars: from n/a through 2.7.10.	2024-08-26	4.3	CVE-2024-43116 audit@patchstack.com
advancedforminte gration -- advanced_form_in tegration	Cross-Site Request Forgery (CSRF) vulnerability in Nasirahmed Advanced Form Integration.This issue affects Advanced Form Integration: from n/a through 1.89.4.	2024-08-26	4.3	CVE-2024-43340 audit@patchstack.com
Analytify--Analytify	Cross-Site Request Forgery (CSRF) vulnerability in Analytify.This issue affects Analytify: from n/a through 5.3.1.	2024-08-26	4.3	CVE-2024-43265 audit@patchstack.com
apache -- portable_runtime	Lax permissions set by the Apache Portable Runtime library on Unix platforms would allow local users read access to named shared memory segments, potentially revealing sensitive application data. This issue does not affect non-Unix platforms, or builds withÂ APR_USE_SHMEM_SHMGET=1 (apr.h) Users are recommended to upgrade to APR version 1.7.5, which fixes this issue.	2024-08-26	5.5	CVE-2023-49582 security@apache.org
Automattic-- GHActivity	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Automattic GHActivity allows Stored XSS.This issue affects GHActivity: from n/a through 2.0.0-alpha.	2024-08-29	6.5	CVE-2024-43949 audit@patchstack.com
averta--Premium Portfolio Features for Phlox theme	The Premium Portfolio Features for Phlox theme plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'aux_recent_portfolios_grid' shortcode in all versions up to, and including, 2.3.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-29	6.4	CVE-2024-1384 security@wordfence.com security@wordfence.com
aws--aws-cdk	The AWS Cloud Development Kit (CDK) is an open-source framework for defining cloud infrastructure using code. Customers use it to create their own applications which are converted to AWS CloudFormation templates during deployment to a customer's AWS account. CDK contains pre-built components called "constructs" that are higher-level abstractions providing defaults and best practices. This approach enables developers to use familiar programming languages to define complex cloud infrastructure more efficiently than writing raw CloudFormation templates. We identified an issue in AWS Cloud Development Kit (CDK) which, under certain conditions, can result in granting authenticated Amazon Cognito users broader than intended access. Specifically, if a CDK application uses the "RestApi" construct with "CognitoUserPoolAuthorizer" as the authorizer and uses authorization scopes to limit access. This issue does not affect the availability of the specific API resources. Authenticated Cognito users may gain unintended	2024-08-27	6.4	CVE-2024-45037 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	access to protected API resources or methods, leading to potential data disclosure, and modification issues. Impacted versions: >=2.142.0;<=2.148.0. A patch is included in CDK versions >=2.148.1. Users are advised to upgrade their AWS CDK version to 2.148.1 or newer and re-deploy their application(s) to address this issue.			com
azurecurve--azurecurve Toggle Show/Hide	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in azurecurve azurecurve Toggle Show/Hide allows Stored XSS.This issue affects azurecurve Toggle Show/Hide: from n/a through 2.1.3.	2024-08-29	6.5	CVE-2024-43961 audit@patchstack.com
Beckhoff--IPC Diagnostics package	The IPC-Diagnostics package included in TwinCAT/BSD is vulnerable to a local denial-of-service attack by a low privileged attacker.	2024-08-27	5.5	CVE-2024-41175 info@cert.vde.com info@cert.vde.com
Beckhoff--MDP package	The MPD package included in TwinCAT/BSDÂ allows an authenticated, low-privileged local attacker to induce a Denial-of-Service (DoS) condition on the daemon and execute code in the context of user "root" via a crafted HTTP request.	2024-08-27	6.5	CVE-2024-41176 info@cert.vde.com
Bit Apps--Bit Form Pro	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Bit Apps Bit Form Pro.This issue affects Bit Form Pro: from n/a through 2.6.4.	2024-08-26	6.5	CVE-2024-43251 audit@patchstack.com
blood_bank_system_project --blood_bank_system	A vulnerability has been found in code-projects Blood Bank System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /login.php of the component Login Page. The manipulation of the argument user leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-26	6.1	CVE-2024-8174 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
bobbingwide -- oik	Cross-Site Request Forgery (CSRF) vulnerability in bobbingwide.This issue affects oik: from n/a through 4.12.0.	2024-08-26	4.3	CVE-2024-43356 audit@patchstack.com
bPlugins LLC--Flash & HTML5 Video	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in bPlugins LLC Flash & HTML5 Video.This issue affects Flash & HTML5 Video: from n/a through 2.5.31.	2024-08-26	4.3	CVE-2024-43319 audit@patchstack.com
Brevo--Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue	Cross-Site Request Forgery (CSRF) vulnerability in Brevo Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue.This issue affects Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue: from n/a through 3.1.82.	2024-08-26	4.3	CVE-2024-43287 audit@patchstack.com
bytecodealliance--rustix	Rustix is a set of safe Rust bindings to POSIX-ish APIs. When using `rustix::fs::Dir` using the `linux_raw` backend, it's possible for the iterator to "get stuck" when an IO error is encountered. Combined with a memory over-allocation issue in `rustix::fs::Dir::read_more`, this can cause quick and unbounded memory explosion (gigabytes in a few seconds if used on a hot path) and eventually lead to an OOM crash of the application. The symptoms were initially discovered in https://github.com/imsnif/bandwhich/issues/284. That post has lots of details of our investigation. Full details can be read on the GHSA-c827-hfw6-qwvm repo advisory. If a program tries to access a directory with its file descriptor after the file has been unlinked (or any other action that leaves the `Dir` iterator in the stuck state), and the implementation does not break after seeing an error, it can cause a memory explosion. As an example, Linux's various virtual file systems (e.g. `/proc`, `/sys`) can contain directories that spontaneously pop in and out of existence.	2024-08-26	6.5	CVE-2024-43806 security-advisories@github.com security-advisories@github.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Attempting to iterate over them using `rustix::fs::Dir` directly or indirectly (e.g. with the `procfs` crate) can trigger this fault condition if the implementation decides to continue on errors. An attacker knowledgeable about the implementation details of a vulnerable target can therefore try to trigger this fault condition via any one or a combination of several available APIs. If successful, the application host will quickly run out of memory, after which the application will likely be terminated by an OOM killer, leading to denial of service. This issue has been addressed in release versions 0.35.15, 0.36.16, 0.37.25, and 0.38.19. Users are advised to upgrade. There are no known workarounds for this issue.			
calinvingan--Premium SEO Pack WP SEO Plugin	The Premium SEO Pack - WP SEO Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.6.001. This makes it possible for unauthenticated attackers to view limited information from password protected posts through the social meta data.	2024-08-29	5.3	CVE-2024-3679 security@wordfence.com security@wordfence.com
Campcodes--Supplier Management System	A vulnerability has been found in Campcodes Supplier Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/edit_area.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.	2024-08-30	6.3	CVE-2024-8344 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Checkout Plugins--Stripe Payments For WooCommerce by Checkout	Cross-Site Request Forgery (CSRF) vulnerability in Checkout Plugins Stripe Payments For WooCommerce by Checkout.This issue affects Stripe Payments For WooCommerce by Checkout: from n/a through 1.9.1.	2024-08-26	4.3	CVE-2024-43316 audit@patchstack.com
Chengdu Everbrite Network Technology--BeikeShop	A vulnerability, which was classified as critical, has been found in Chengdu Everbrite Network Technology BeikeShop up to 1.5.5. Affected by this issue is the function rename of the file /Admin/Http/Controllers/FileManagerController.php. The manipulation of the argument new_name leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-26	6.3	CVE-2024-8164 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Chengdu Everbrite Network Technology--BeikeShop	A vulnerability classified as critical was found in Chengdu Everbrite Network Technology BeikeShop up to 1.5.5. Affected by this vulnerability is the function destroyFiles of the file /admin/file_manager/files. The manipulation of the argument files leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-26	5.4	CVE-2024-8163 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Chengdu Everbrite Network Technology--BeikeShop	A vulnerability, which was classified as problematic, was found in Chengdu Everbrite Network Technology BeikeShop up to 1.5.5. This affects the function exportZip of the file /admin/file_manager/export. The manipulation of the argument path leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-26	4.3	CVE-2024-8165 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Cisco--Cisco Application Policy Infrastructure Controller (APIC)	A vulnerability in the software upgrade component of Cisco Application Policy Infrastructure Controller (APIC) and Cisco Cloud Network Controller, formerly Cisco Cloud APIC, could allow an authenticated, remote attacker with Administrator-level privileges to install a modified software image, leading to arbitrary code injection on an affected system. This vulnerability is due to insufficient signature validation of software images. An attacker could exploit this vulnerability by installing a modified software image. A successful exploit could	2024-08-28	6.5	CVE-2024-20478 ykramarz@cisco.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allow the attacker to execute arbitrary code on the affected system and elevate their privileges to root. Note: Administrators should always validate the hash of any upgrade image before uploading it to Cisco APIC and Cisco Cloud Network Controller.			
Cisco--Cisco Application Policy Infrastructure Controller (APIC)	A vulnerability in the restricted security domain implementation of Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated, remote attacker to modify the behavior of default system policies, such as quality of service (QoS) policies, on an affected system. This vulnerability is due to improper access control when restricted security domains are used to implement multi-tenancy. An attacker with a valid user account associated with a restricted security domain could exploit this vulnerability. A successful exploit could allow the attacker to read, modify, or delete child policies created under default system policies, which are implicitly used by all tenants in the fabric, resulting in disruption of network traffic. Exploitation is not possible for policies under tenants that an attacker has no authorization to access.	2024-08-28	4.3	CVE-2024-20279 ykramarz@cisco.com
Cisco--Cisco NX-OS Software	A vulnerability in Cisco NX-OS Software could allow an authenticated, local attacker with privileges to access the Bash shell to execute arbitrary code as root on an affected device. This vulnerability is due to insufficient security restrictions when executing commands from the Bash shell. An attacker with privileges to access the Bash shell could exploit this vulnerability by executing a specific crafted command on the underlying operating system. A successful exploit could allow the attacker to execute arbitrary code with the privileges of root.	2024-08-28	6.7	CVE-2024-20411 ykramarz@cisco.com
Cisco--Cisco NX-OS Software	A vulnerability in Cisco NX-OS Software could allow an authenticated, local attacker with privileges to access the Bash shell to elevate privileges to network-admin on an affected device. This vulnerability is due to insufficient security restrictions when executing application arguments from the Bash shell. An attacker with privileges to access the Bash shell could exploit this vulnerability by executing crafted commands on the underlying operating system. A successful exploit could allow the attacker to create new users with the privileges of network-admin.	2024-08-28	6.7	CVE-2024-20413 ykramarz@cisco.com
Cisco--Cisco NX-OS Software	A vulnerability in the Python interpreter of Cisco NX-OS Software could allow an authenticated, low-privileged, local attacker to escape the Python sandbox and gain unauthorized access to the underlying operating system of the device. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by manipulating specific functions within the Python interpreter. A successful exploit could allow an attacker to escape the Python sandbox and execute arbitrary commands on the underlying operating system with the privileges of the authenticated user. Note: An attacker must be authenticated with Python execution privileges to exploit these vulnerabilities. For more information regarding Python execution privileges, see product-specific documentation, such as the section of the Cisco Nexus 9000 Series NX-OS Programmability Guide.	2024-08-28	5.3	CVE-2024-20284 ykramarz@cisco.com ykramarz@cisco.com
Cisco--Cisco NX-OS Software	A vulnerability in the Python interpreter of Cisco NX-OS Software could allow an authenticated, low-privileged, local attacker to escape the Python sandbox and gain unauthorized access to the underlying operating system of the device. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by manipulating specific functions within the Python interpreter. A successful exploit could allow an attacker to escape the Python sandbox and execute arbitrary commands on the underlying operating system with the privileges of the authenticated user. Note: An attacker must be authenticated with Python execution privileges to exploit these vulnerabilities. For more information regarding Python execution privileges, see product-specific documentation, such as the section of the Cisco Nexus 9000 Series NX-OS Programmability Guide.	2024-08-28	5.3	CVE-2024-20285 ykramarz@cisco.com ykramarz@cisco.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cisco--Cisco NX-OS Software	A vulnerability in the Python interpreter of Cisco NX-OS Software could allow an authenticated, low-privileged, local attacker to escape the Python sandbox and gain unauthorized access to the underlying operating system of the device. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by manipulating specific functions within the Python interpreter. A successful exploit could allow an attacker to escape the Python sandbox and execute arbitrary commands on the underlying operating system with the privileges of the authenticated user. Note: An attacker must be authenticated with Python execution privileges to exploit these vulnerabilities. For more information regarding Python execution privileges, see product-specific documentation, such as the section of the Cisco Nexus 9000 Series NX-OS Programmability Guide.	2024-08-28	5.3	CVE-2024-20286 ykramarz@cisco.com ykramarz@cisco.com
Cisco--Cisco NX-OS Software	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, low-privileged, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments for a specific CLI command. An attacker could exploit this vulnerability by including crafted input as the argument of the affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user.	2024-08-28	4.4	CVE-2024-20289 ykramarz@cisco.com
code-projects--Pharmacy Management System	A vulnerability was found in code-projects Pharmacy Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /index.php?id=userProfileEdit of the component Update My Profile Page. The manipulation of the argument fname/lname/email with the input <script>alert(1)</script> 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.	2024-08-31	4.3	CVE-2024-8366 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
CollaboraOnline--online	Collabora Online is a collaborative online office suite based on LibreOffice technology. In the mobile (Android/iOS) device variants of Collabora Online it was possible to inject JavaScript via url encoded values in links contained in documents. Since the Android JavaScript interface allows access to internal functions, the likelihood that the app could be compromised via this vulnerability is considered high. Non-mobile variants are not affected. Mobile variants should update to the latest version provided by the platform appstore. There are no known workarounds for this vulnerability.	2024-08-29	6.3	CVE-2024-45045 security-advisories@github.com
Contest Gallery--Contest Gallery	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Contest Gallery.This issue affects Contest Gallery: from n/a through 23.1.2.	2024-08-26	5.3	CVE-2024-43283 audit@patchstack.com
cryoutcreations --esotera	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Esotera allows Stored XSS.This issue affects Esotera: from n/a through 1.2.5.1.	2024-08-29	5.4	CVE-2024-43952 audit@patchstack.com
cryoutcreations --tempera	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Tempera allows Stored XSS.This issue affects Tempera: from n/a through 1.8.2.	2024-08-29	5.4	CVE-2024-43951 audit@patchstack.com
cyberlord92--Web Application Firewall website security	The Web Application Firewall plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 2.1.2. This is due to insufficient restrictions on where the IP Address information is being retrieved for request logging and login restrictions. Attackers can supply the X-Forwarded-For header with with a different IP Address that will be logged and can be used to bypass settings that may have blocked out an IP address or country from logging in.	2024-08-31	5.3	CVE-2022-4539 security@wordfence.com security@wordfence.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dell--Dell Client Platform, Dell Dock Firmware	Dell Dock Firmware and Dell Client Platform contain an Improper Link Resolution vulnerability during installation resulting in arbitrary folder deletion, which could lead to Privilege Escalation or Denial of Service.	2024-08-28	6.7	CVE-2023-43078 security_alert@emc.com
Dell--PowerEdge Platform	Dell PowerEdge Platform, 14G Intel BIOS version(s) prior to 2.22.x, contains an Improper Input Validation vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2024-08-29	5.3	CVE-2024-38303 security_alert@emc.com
Dell--PowerScale OneFS	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.1 contains a UNIX symbolic link (symlink) following vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to denial of service, information tampering.	2024-08-31	6.3	CVE-2024-39578 security_alert@emc.com
Dell--PowerScale OneFS	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contains an incorrect privilege assignment vulnerability. A local high privileged attacker could potentially exploit this vulnerability to gain root-level access.	2024-08-31	6.7	CVE-2024-39579 security_alert@emc.com
delower186--WP To Do	The WP To Do plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment in all versions up to, and including, 1.3.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-08-29	4.4	CVE-2024-3944 security@wordfence.com security@wordfence.com
Dinesh Karki--WP Armour Extended	Cross-Site Request Forgery (CSRF) vulnerability in Dinesh Karki WP Armour Extended.This issue affects WP Armour Extended: from n/a through 1.26.	2024-08-29	5.4	CVE-2024-43947 audit@patchstack.com
dingfanzu--CMS	A vulnerability was found in dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. It has been rated as critical. Affected by this issue is some unknown functionality of the file /ajax/chpwd.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. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-29	6.3	CVE-2024-8302 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
dingfanzu--CMS	A vulnerability classified as critical has been found in dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. This affects an unknown part of the file /ajax/getBasicInfo.php. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-29	6.3	CVE-2024-8303 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
discourse--discourse-calendar	discourse-calendar is a discourse plugin which adds the ability to create a dynamic calendar in the first post of a topic. The limit on region value length is too generous. This allows a malicious actor to cause a Discourse instance to use excessive bandwidth and disk space. This issue has been patched in main the main branch. There are no workarounds for this vulnerability. Please upgrade as soon as possible.	2024-08-30	4.3	CVE-2024-21658 security-advisories@github.com
Dylan James--Zephyr Project	Authorization Bypass Through User-Controlled Key vulnerability in Dylan James Zephyr Project Manager.This issue affects Zephyr Project Manager: from n/a through 3.3.102.	2024-08-26	4.3	CVE-2024-43916 audit@patchstack.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Manager				com
etoilewebdesign -- front_end_users	The Front End Users plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'user-search' shortcode in all versions up to, and including, 3.2.28 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.	2024-08-29	5.4	CVE-2024-7606 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
freakingwildchild--Visual Sound	The Visual Sound plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.03. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-08-27	4.3	CVE-2024-8197 security@wordfence.com security@wordfence.com
funnelforms--Interactive Contact Form and Multi Step Form Builder with Drag & Drop Editor Funnelforms Free	The Funnelforms Free plugin for WordPress is vulnerable to arbitrary file deletion in all versions up to, and including, 3.7.3.2 via the 'af2DeleteFontFile' function. This is due to the plugin not properly validating a file or its path prior to deleting it. This makes it possible for unauthenticated attackers to delete arbitrary files, including the wp-config.php file, which can make site takeover and remote code execution possible.	2024-08-28	6.5	CVE-2024-6312 security@wordfence.com security@wordfence.com security@wordfence.com
funnelforms--Interactive Contact Form and Multi Step Form Builder with Drag & Drop Editor Funnelforms Free	The Interactive Contact Form and Multi Step Form Builder with Drag & Drop Editor - Funnelforms Free plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the af2_handel_file_remove AJAX action in all versions up to, and including, 3.7.3.2. This makes it possible for unauthenticated attackers to delete arbitrary media files.	2024-08-29	5.3	CVE-2024-5857 security@wordfence.com security@wordfence.com
funnelforms--Interactive Contact Form and Multi Step Form Builder with Drag & Drop Editor Funnelforms Free	The Interactive Contact Form and Multi Step Form Builder with Drag & Drop Editor - Funnelforms Free plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'fnsf_af2_handel_file_upload' function in all versions up to, and including, 3.7.3.2. This makes it possible for unauthenticated attackers to upload arbitrary media to the site, even if no forms exist.	2024-08-28	5.3	CVE-2024-7447 security@wordfence.com security@wordfence.com security@wordfence.com
FunnelKit--FunnelKit Funnel Builder Pro	The FunnelKit Funnel Builder Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'allow_iframe_tag_in_post' function which uses the 'wp_kses_allowed_html' filter to globally allow script and iframe tags in posts in all versions up to, and including, 3.4.5. This makes it possible for authenticated attackers, with contributor access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-29	6.4	CVE-2024-1056 security@wordfence.com security@wordfence.com
getbrave -- brave	Cross-Site Request Forgery (CSRF) vulnerability in Brave Brave Popup Builder.This issue affects Brave Popup Builder: from n/a through 0.7.0.	2024-08-26	4.3	CVE-2024-43337 audit@patchstack.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gianniporto -- intothedark	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Gianni Porto IntoTheDark allows Reflected XSS.This issue affects IntoTheDark: from n/a through 1.0.5.	2024-08-29	6.1	CVE-2024-43958 audit@patchstack.com
gioni--WP Cerber Security, Anti-spam & Malware Scan	The WP Cerber Security plugin for WordPress is vulnerable to IP Protection bypass in versions up to, and including 9.4 due to the plugin improperly checking for a visitor's IP address. This makes it possible for an attacker whose IP address has been blocked to bypass this control by setting the X-Forwarded-For: HTTP header to an IP Address that hasn't been blocked.	2024-08-31	5.3	CVE-2022-4100 security@wordfence.com security@wordfence.com
HFO4--shudong-share	A vulnerability was found in HFO4 shudong-share 2.4.7. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /includes/fileReceive.php of the component File Extension Handler. The manipulation of the argument file leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2024-08-30	6.3	CVE-2024-8338 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
hitachienergy -- microscada_x_sys600	An HTTP parameter may contain a URL value and could cause the web application to redirect the request to the specified URL. By modifying the URL value to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials.	2024-08-27	6.1	CVE-2024-7941 cybersecurity@hitachienergy.com
hubspotdev--HubSpot CRM, Email Marketing, Live Chat, Forms & Analytics	The HubSpot - CRM, Email Marketing, Live Chat, Forms & Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' attribute of the HubSpot Meeting Widget in all versions up to, and including, 11.1.22 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.	2024-08-30	6.4	CVE-2024-5879 security@wordfence.com security@wordfence.com security@wordfence.com
HWA JIUH DIGITAL TECHNOLOGY--Easy test Online Learning and Testing Platform	Easy test Online Learning and Testing Platform from HWA JIUH DIGITAL TECHNOLOGY does not properly validate a specific page parameter, allowing remote attackers with regular privilege to inject arbitrary JavaScript code and perform Reflected Cross-site scripting attacks.	2024-08-30	5.4	CVE-2024-8328 twcert@cert.org.tw twcert@cert.org.tw
IBM--MaaS360	IBM MaaS360 for Android 6.31 through 8.60 is using hard coded credentials that can be obtained by a user with physical access to the device.	2024-08-29	4.6	CVE-2024-35118 psirt@us.ibm.com psirt@us.ibm.com
IBM--Security Verify Access	IBM Security Verify Access 10.0.0 through 10.0.8 OIDC Provider could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim.	2024-08-29	6.8	CVE-2024-35133 psirt@us.ibm.com psirt@us.ibm.com
in2code -- powermail	An issue was discovered in powermail extension through 12.3.5 for TYPO3. It fails to validate the mail parameter of the confirmationAction, resulting in Insecure Direct Object Reference (IDOR). An unauthenticated attacker can use this to display the user-submitted data of all forms persisted by the extension. This can only be exploited when the extension is configured to save submitted form data to the database (plugin.tx_powermail.settings.db.enable=1), which however is the default setting of the extension. The fixed versions are 7.5.0, 8.5.0, 10.9.0, and 12.4.0	2024-08-29	5.3	CVE-2024-45232 cve@mitre.org

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
insurance_management_system_project -- insurance_management_system	A vulnerability has been found in nafisulbari/itsourcecode Insurance Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file editClient.php. The manipulation of the argument AGENT ID leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-27	6.1	CVE-2024-8208 cna@vuldb.com cna@vuldb.com cna@vuldb.com
insurance_management_system_project -- insurance_management_system	A vulnerability was found in nafisulbari/itsourcecode Insurance Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file addClient.php. The manipulation of the argument CLIENT ID leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-27	6.1	CVE-2024-8209 cna@vuldb.com cna@vuldb.com cna@vuldb.com
insurance_management_system_project -- insurance_management_system	A vulnerability, which was classified as critical, has been found in nafisulbari/itsourcecode Insurance Management System 1.0. Affected by this issue is some unknown functionality of the file editPayment.php of the component Payment Handler. The manipulation of the argument recipt_no leads to improper access controls. The attack may be launched remotely. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-27	5.4	CVE-2024-8216 cna@vuldb.com cna@vuldb.com cna@vuldb.com
irfanview -- irfanview	An issue in the component EXR!ReadEXR+0x40ef1 of Irfanview v4.67.1.0 allows attackers to cause an access violation via a crafted EXR file. This vulnerability can lead to a Denial of Service (DoS).	2024-08-28	5.5	CVE-2024-44913 cve@mitre.org
irfanview -- irfanview	An issue in the component EXR!ReadEXR+0x3df50 of Irfanview v4.67.1.0 allows attackers to cause an access violation via a crafted EXR file. This vulnerability can lead to a Denial of Service (DoS).	2024-08-28	5.5	CVE-2024-44914 cve@mitre.org
irfanview -- irfanview	An issue in the component EXR!ReadEXR+0x4eef0 of Irfanview v4.67.1.0 allows attackers to cause an access violation via a crafted EXR file. This vulnerability can lead to a Denial of Service (DoS).	2024-08-28	5.5	CVE-2024-44915 cve@mitre.org
Jegstudio--Gutenverse	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jegstudio Gutenverse allows Stored XSS.This issue affects Gutenverse: from n/a through 1.9.4.	2024-08-29	6.5	CVE-2024-43920 audit@patchstack.com
jegtheme--Jeg Elementor Kit	The Jeg Elementor Kit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.6.7 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.	2024-08-27	6.4	CVE-2024-6804 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
JEM Plugins--Order Export for WooCommerce	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in JEM Plugins Order Export for WooCommerce.This issue affects Order Export for WooCommerce: from n/a through 3.23.	2024-08-26	5.3	CVE-2024-43259 audit@patchstack.com
jupyter -- jupyterlab	jupyterlab is an extensible environment for interactive and reproducible computing, based on the Jupyter Notebook Architecture. This vulnerability depends on user interaction by opening a malicious notebook with Markdown cells, or Markdown file using JupyterLab preview feature. A malicious user can access any data that the attacked user has access to as well as perform arbitrary requests acting as the attacked user. JupyterLab v3.6.8, v4.2.5 and Jupyter Notebook v7.2.2 have been patched to resolve this issue. Users are advised to upgrade. There is no workaround for the underlying DOM Clobbering susceptibility.	2024-08-28	6.1	CVE-2024-43805 security-advisories@github.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	However, select plugins can be disabled on deployments which cannot update in a timely fashion to minimise the risk. These are: 1. `@jupyterlab/mathjax-extension:plugin` - users will loose ability to preview mathematical equations. 2. `@jupyterlab/markdownviewer-extension:plugin` - users will loose ability to open Markdown previews. 3. `@jupyterlab/mathjax2-extension:plugin` (if installed with optional `jupyterlab-mathjax2` package) - an older version of the mathjax plugin for JupyterLab 4.x. To disable these extensions run: ```jupyter labextension disable @jupyterlab/markdownviewer-extension:plugin && jupyter labextension disable @jupyterlab/mathjax-extension:plugin && jupyter labextension disable @jupyterlab/mathjax2-extension:plugin ``` in bash.			
justinbusa--Beaver Builder WordPress Page Builder	The Beaver Builder - WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'type' parameter in all versions up to, and including, 2.8.3.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-29	6.4	CVE-2024-7895 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
Kriesi--Enfold - Responsive Multi-Purpose Theme	The Enfold - Responsive Multi-Purpose Theme theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wrapper_class' and 'class' parameters in all versions up to, and including, 6.0.3 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.	2024-08-30	6.4	CVE-2024-5061 security@wordfence.com security@wordfence.com
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: Add error handling to pair_device() hci_conn_params_add() never checks for a NULL value and could lead to a NULL pointer dereference causing a crash. Fixed by adding error handling in the function.	2024-08-26	5.5	CVE-2024-43884 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix double inode unlock for direct IO sync writes If we do a direct IO sync write, at btrfs_sync_file(), and we need to skip inode logging or we get an error starting a transaction or an error when flushing delalloc, we end up unlocking the inode when we shouldn't under the 'out_release_extents' label, and then unlock it again at btrfs_direct_write(). Fix that by checking if we have to skip inode unlocking under that label.	2024-08-26	5.5	CVE-2024-43885 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null check in resource_log_pipe_topology_update [WHY] When switching from "Extend" to "Second Display Only" we sometimes call resource_get_otg_master_for_stream on a stream for the eDP, which is disconnected. This leads to a null pointer dereference. [HOW] Added a null check in dc_resource.c/resource_log_pipe_topology_update.	2024-08-26	5.5	CVE-2024-43886 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: padata: Fix possible divide-by-0 panic in padata_mt_helper() We are hit with a not easily reproducible divide-by-0 panic in padata.c at bootup time. [10.017908] Oops: divide error: 0000 1 PREEMPT SMP NOPTI [10.017908] CPU: 26 PID: 2627 Comm: kworker/u1666:1 Not tainted 6.10.0-15.el10.x86_64 #1 [10.017908] Hardware name: Lenovo ThinkSystem SR950 [7X12CTO1WW]/[7X12CTO1WW], BIOS [PSE140J-2.30] 07/20/2021 [10.017908] Workqueue: events_unbound padata_mt_helper [10.017908] RIP: 0010:padata_mt_helper+0x39/0xb0 : [10.017963] Call Trace: [10.017968] <TASK> [10.018004] ? padata_mt_helper+0x39/0xb0 [10.018084] process_one_work+0x174/0x330 [10.018093] worker_thread+0x266/0x3a0 [10.018111] kthread+0xcf/0x100 [10.018124] ret_from_fork+0x31/0x50 [10.018138] ret_from_fork_asm+0x1a/0x30 [10.018147] </TASK> Looking at the padata_mt_helper() function, the only way a divide-by-0 panic can happen is when ps->chunk_size is 0. The way that chunk_size is initialized in padata_do_multithreaded(), chunk_size can be 0 when the min_chunk in the passed-in padata_mt_job structure is 0. Fix this divide-by-0 panic by making sure that chunk_size will be at least 1 no matter what the input parameters are.	2024-08-26	5.5	CVE-2024-43889 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix null pointer deref in dcn20_resource.c Fixes a hang thats triggered when MPV is run on a DCN401 dGPU: mpv --hwdec=vaapi --vo=gpu --hwdec-codecs=all and then enabling fullscreen playback (double click on the video) The following calltrace will be seen: [181.843989] BUG: kernel NULL pointer dereference, address: 0000000000000000 [181.843997] #PF: supervisor instruction fetch in kernel mode [181.844003] #PF: error_code(0x0010) - not-present page [181.844009] PGD 0 P4D 0 [181.844020] Oops: 0010 [#1] PREEMPT SMP NOPTI [181.844028] CPU: 6 PID: 1892 Comm: gnome-shell Tainted: G W OE 6.5.0-41-generic #41~22.04.2-Ubuntu [181.844038] Hardware name: System manufacturer System Product Name/CROSSHAIR VI HERO, BIOS 6302 10/23/2018 [181.844044] RIP: 0010:0x0 [181.844079] Code: Unable to access opcode bytes at 0xffffffffffffffd6. [181.844084] RSP: 0018:ffffb593c2b8f7b0 EFLAGS: 00010246 [181.844093] RAX: 0000000000000000 RBX: 0000000000000000 RCX: 0000000000000004 [181.844099] RDX: ffffb593c2b8f804 RSI: ffffb593c2b8f7e0 RDI: ffff9e3c8e758400 [181.844105] RBP: ffffb593c2b8f7b8 R08: ffffb593c2b8f9c8 R09: ffffb593c2b8f96c [181.844110] R10: 0000000000000000 R11: 0000000000000000 R12: ffffb593c2b8f9c8 [181.844115] R13: 0000000000000001 R14: ffff9e3c88000000 R15: 0000000000000005 [181.844121] FS: 00007c6e323bb5c0(0000) GS:ffff9e3f85f80000(0000) knlGS:0000000000000000 [181.844128] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [181.844134] CR2: ffffffffffffffd6 CR3: 0000000140fbe000 CR4: 00000000003506e0 [181.844141] Call Trace: [181.844146] <TASK> [181.844153] ? show_regs+0x6d/0x80 [181.844167] ? __die+0x24/0x80 [181.844179] ? page_fault_oops+0x99/0x1b0 [	2024-08-26	5.5	CVE-2024-43899 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	181.844192] ? do_user_addr_fault+0x31d/0x6b0 [181.844204] ? exc_page_fault+0x83/0x1b0 [181.844216] ? asm_exc_page_fault+0x27/0x30 [181.844237] dcn20_get_dcc_compression_cap+0x23/0x30 [amdgpu] [181.845115] amdgpu_dm_plane_validate_dcc.constprop.0+0xe5/0x180 [amdgpu] [181.845985] amdgpu_dm_plane_fill_plane_buffer_attributes+0x300/0x580 [amdgpu] [181.846848] fill_dc_plane_info_and_addr+0x258/0x350 [amdgpu] [181.847734] fill_dc_plane_attributes+0x162/0x350 [amdgpu] [181.848748] dm_update_plane_state.constprop.0+0x4e3/0x6b0 [amdgpu] [181.849791] ? dm_update_plane_state.constprop.0+0x4e3/0x6b0 [amdgpu] [181.850840] amdgpu_dm_atomic_check+0xdfe/0x1760 [amdgpu]			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix NULL pointer dereference for DTN log in DCN401 When users run the command: cat /sys/kernel/debug/dri/0/amdgpu_dm_dtn_log The following NULL pointer dereference happens: [+0.000003] BUG: kernel NULL pointer dereference, address: NULL [+0.000005] #PF: supervisor instruction fetch in kernel mode [+0.000002] #PF: error_code(0x0010) - not-present page [+0.000002] PGD 0 P4D 0 [+0.000004] Oops: 0010 [#1] PREEMPT SMP NOPTI [+0.000003] RIP: 0010:0x0 [+0.000008] Code: Unable to access opcode bytes at 0xffffffffffffffd6. [...] [+0.000002] PKRU: 55555554 [+0.000002] Call Trace: [+0.000002] <TASK> [+0.000003] ? show_regs+0x65/0x70 [+0.000006] ? __die+0x24/0x70 [+0.000004] ? page_fault_oops+0x160/0x470 [+0.000006] ? do_user_addr_fault+0x2b5/0x690 [+0.000003] ? prb_read_valid+0x1c/0x30 [+0.000005] ? exc_page_fault+0x8c/0x1a0 [+0.000005] ? asm_exc_page_fault+0x27/0x30 [+0.000012] dcn10_log_color_state+0xf9/0x510 [amdgpu] [+0.000306] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000003] ? vsnprintf+0x2fb/0x600 [+0.000009] dcn10_log_hw_state+0xfd0/0xfe0 [amdgpu] [+0.000218] ? __mod_memcg_lruvec_state+0xe8/0x170 [+0.000008] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? debug_smp_processor_id+0x17/0x20 [+0.000003] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? set_ptes.isra.0+0x2b/0x90 [+0.000004] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? _raw_spin_unlock+0x19/0x40 [+0.000004] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000002] ? do_anonymous_page+0x337/0x700 [+0.000004] dtn_log_read+0x82/0x120 [amdgpu] [+0.000207] full_proxy_read+0x66/0x90 [+0.000007] vfs_read+0xb0/0x340 [+0.000005] ? __count_memcg_events+0x79/0xe0 [+0.000002] ? srso_alias_return_thunk+0x5/0xfbef5 [+0.000003] ? count_memcg_events.constprop.0+0x1e/0x40 [+0.000003] ? handle_mm_fault+0xb2/0x370 [+0.000003] ksys_read+0x6b/0xf0 [+0.000004] __x64_sys_read+0x19/0x20 [+0.000003] do_syscall_64+0x60/0x130 [+0.000004] entry_SYSCALL_64_after_hwframe+0x6e/0x76 [+0.000003] RIP: 0033:0x7fdf32f147e2 [...] This error happens when the color log tries to read the gamut remap information from DCN401 which is not initialized in the dcn401_dpp_funcs which leads to a null pointer dereference. This commit addresses this issue by adding a proper guard to access the gamut_remap callback in case the specific ASIC did not implement this function.	2024-08-26	5.5	CVE-2024-43901 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null checker before passing variables Checks null pointer before passing variables to functions. This fixes 3 NULL_RETURNS issues reported by Coverity.	2024-08-26	5.5	CVE-2024-43902 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add NULL check for 'afb' before dereferencing in amdgpu_dm_plane_handle_cursor_update This commit adds a null check for the 'afb' variable in the amdgpu_dm_plane_handle_cursor_update function. Previously, 'afb' was assumed to be null, but was used later in the code without a null check. This could potentially lead to a null pointer dereference. Fixes the below: drivers/gpu/drm/amd/amdgpu/../display/amdgpu_dm/amdgpu_dm_plane.c:1298 amdgpu_dm_plane_handle_cursor_update() error: we previously assumed 'afb' could be null (see line 1252)	2024-08-26	5.5	CVE-2024-43903 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null checks for 'stream' and 'plane' before dereferencing This commit adds null checks for the 'stream' and 'plane' variables in the dcn30_apply_idle_power_optimizations function. These variables were previously assumed to be null at line 922, but they were used later in the code without checking if they were null. This could potentially lead to a null pointer dereference, which would cause a crash. The null checks ensure that 'stream' and 'plane' are not null before they are used, preventing potential crashes. Fixes the below static smatch checker: drivers/gpu/drm/amd/amdgpu/../display/dc/hwss/dcn30/dcn30_hwseq.c:938 dcn30_apply_idle_power_optimizations() error: we previously assumed 'stream' could be null (see line 922) drivers/gpu/drm/amd/amdgpu/../display/dc/hwss/dcn30/dcn30_hwseq.c:940 dcn30_apply_idle_power_optimizations() error: we previously assumed 'plane' could be null (see line 922)	2024-08-26	5.5	CVE-2024-43904 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: Fix the null pointer dereference for vega10_hwmgr Check return value and conduct null pointer handling to avoid null pointer dereference.	2024-08-26	5.5	CVE-2024-43905 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/admgpu: fix dereferencing null pointer context When user space sets an invalid ta type, the pointer context will be empty. So it need to check the pointer context before using it	2024-08-26	5.5	CVE-2024-43906 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: Fix the null pointer dereference in apply_state_adjust_rules Check the pointer value to fix potential null pointer dereference	2024-08-26	5.5	CVE-2024-43907 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix the null pointer dereference to ras_manager Check ras_manager before using it	2024-08-26	5.5	CVE-2024-43908 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: Fix the null pointer dereference for smu7 optimize the code to avoid pass a null pointer (hwmgr->backend) to function smu7_update_edc_leakage_table.	2024-08-26	5.5	CVE-2024-43909 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix NULL dereference at band check in starting tx ba session In MLD connection, link_data/link_conf are dynamically allocated. They don't point to vif->bss_conf. So, there will be no chanreq assigned to vif->bss_conf and then the chan will be NULL. Tweak the code to check ht_supported/vht_supported/has_he/has_eht on sta deflink. Crash log (with rtw89 version under MLO development): [9890.526087] BUG: kernel NULL pointer dereference, address: 0000000000000000 [9890.526102] #PF: supervisor read access in kernel mode [9890.526105] #PF: error_code(0x0000) - not-present page [9890.526109] PGD 0 P4D 0 [9890.526114] Oops: 0000 [#1] PREEMPT SMP PTI [9890.526119] CPU: 2 PID: 6367 Comm: kworker/u16:2 Kdump: loaded Tainted: G OE 6.9.0 #1 [9890.526123] Hardware name: LENOVO 2356AD1/2356AD1, BIOS G7ETB3WW (2.73) 11/28/2018 [9890.526126] Workqueue: phy2 rtw89_core_ba_work [rtw89_core] [9890.526203] RIP: 0010:ieee80211_start_tx_ba_session (net/mac80211/agg-tx.c:618 (discriminator 1)) mac80211 [9890.526279] Code: f7 e8 d5 93 3e ea 48 83 c4 28 89 d8 5b 41 5c 41 5d 41 5e 41 5f 5d c3 cc cc cc cc 49 8b 84 24 e0 f1 ff ff 48 8b 80 90 1b 00 00 <83> 38 03 0f 84 37 fe ff ff bb ea ff ff ff eb cc 49 8b 84 24 10 f3 All code ======== 0: f7 e8 imul %eax 2: d5 (bad) 3: 93 xchg %eax,%ebx 4: 3e ea ds (bad) 6: 48 83 c4 28 add $0x28,%rsp a: 89 d8 mov %ebx,%eax c: 5b pop %rbx d: 41 5c pop %r12 f: 41 5d pop %r13 11: 41 5e pop %r14 13: 41 5f pop %r15 15: 5d pop %rbp 16: c3 retq 17: cc int3 18: cc int3 19: cc int3 1a: cc int3 1b: 49 8b 84 24 e0 f1 ff mov -0xe20(%r12),%rax 22: ff 23: 48 8b 80 90 1b 00 00 mov 0x1b90(%rax),%rax 2a:* 83 38 03 cmpl $0x3,(%rax) <-- trapping instruction 2d: 0f 84 37 fe ff ff je 0xffffffffffffe6a 33: bb ea ff ff ff mov $0xffffffea,%ebx 38: eb cc jmp 0x6 3a: 49 rex.WB 3b: 8b .byte 0x8b 3c: 84 24 10 test %ah,(%rax,%rdx,1) 3f: f3 repz Code starting with the faulting instruction ========== 0: 83 38 03 cmpl $0x3,(%rax) 3: 0f 84 37 fe ff ff je 0xfffffffffffffe40 9: bb ea ff ff ff mov $0xffffffea,%ebx e: eb cc jmp 0xffffffffffffffdc 10: 49 rex.WB 11: 8b .byte 0x8b 12: 84 24 10 test %ah,(%rax,%rdx,1) 15: f3 repz [9890.526285] RSP: 0018:ffffb8db09013d68 EFLAGS: 00010246 [9890.526291] RAX: 0000000000000000 RBX: 0000000000000000 RCX: ffff9308e0d656c8 [9890.526295] RDX: 0000000000000000 RSI: ffffffffab99460b RDI: ffffffffab9a7685 [9890.526300] RBP: ffffb8db09013db8 R08: 0000000000000000 R09: 0000000000000873 [9890.526304] R10: ffff9308e0d64800 R11: 0000000000000002 R12: ffff9308e5ff6e70 [9890.526308] R13: ffff930952500e20 R14: ffff9309192a8c00 R15: 0000000000000000 [9890.526313] FS: 0000000000000000(0000) GS:ffff930b4e700000(0000) knlGS:0000000000000000 [9890.526316] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [9890.526318] CR2: 0000000000000000 CR3: 0000000391c58005 CR4: 00000000001706f0 [9890.526321] Call Trace: [9890.526324] <TASK> [9890.526327] ? show_regs (arch/x86/kernel/dumpstack.c:479) [9890.526335] ? __die (arch/x86/kernel/dumpstack.c:421 arch/x86/kernel/dumpstack.c:434) [9890.526340] ? page_fault_oops (arch/x86/mm/fault.c:713) [9890.526347] ? search_module_extables (kernel/module/main.c:3256 (discriminator ---truncated---	2024-08-26	5.5	CVE-2024-43911 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: bnxt_en : Fix memory out-of-bounds in bnxt_fill_hw_rss_tbl() A recent commit has modified the code in __bnxt_reserve_rings() to set the default RSS indirection table to default only when the number of RX rings is changing. While this works for newer firmware that requires RX ring reservations, it causes the regression on older firmware not	2024-08-26	5.5	CVE-2024-44933 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	requiring RX ring resrvations (BNXT_NEW_RM() returns false). With older firmware, RX ring reservations are not required and so hw_resc->resv_rx_rings is not always set to the proper value. The comparison: if (old_rx_rings != bp->hw_resc.resv_rx_rings) in __bnxt_reserve_rings() may be false even when the RX rings are changing. This will cause __bnxt_reserve_rings() to skip setting the default RSS indirection table to default to match the current number of RX rings. This may later cause bnxt_fill_hw_rss_tbl() to use an out-of-range index. We already have bnxt_check_rss_tbl_no_rmgr() to handle exactly this scenario. We just need to move it up in bnxt_need_reserve_rings() to be called unconditionally when using older firmware. Without the fix, if the TX rings are changing, we'll skip the bnxt_check_rss_tbl_no_rmgr() call and __bnxt_reserve_rings() may also skip the bnxt_set_dflt_rss_indir_tbl() call for the reason explained in the last paragraph. Without setting the default RSS indirection table to default, it causes the regression: BUG: KASAN: slab-out-of-bounds in __bnxt_hwrm_vnic_set_rss+0xb79/0xe40 Read of size 2 at addr ffff8881c5809618 by task ethtool/31525 Call Trace: __bnxt_hwrm_vnic_set_rss+0xb79/0xe40 bnxt_hwrm_vnic_rss_cfg_p5+0xf7/0x460 __bnxt_setup_vnic_p5+0x12e/0x270 __bnxt_open_nic+0x2262/0x2f30 bnxt_open_nic+0x5d/0xf0 ethnl_set_channels+0x5d4/0xb30 ethnl_default_set_doit+0x2f1/0x620			4396-8d5f-8c081fb06d67
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: sctp: Fix null-ptr-deref in reuseport_add_sock(). syzbot reported a null-ptr-deref while accessing sk2->sk_reuseport_cb in reuseport_add_sock(). [0] The repro first creates a listener with SO_REUSEPORT. Then, it creates another listener on the same port and concurrently closes the first listener. The second listen() calls reuseport_add_sock() with the first listener as sk2, where sk2->sk_reuseport_cb is not expected to be cleared concurrently, but the close() does clear it by reuseport_detach_sock(). The problem is SCTP does not properly synchronise reuseport_alloc(), reuseport_add_sock(), and reuseport_detach_sock(). The caller of reuseport_alloc() and reuseport_{add,detach}_sock() must provide synchronisation for sockets that are classified into the same reuseport group. Otherwise, such sockets form multiple identical reuseport groups, and all groups except one would be silently dead. 1. Two sockets call listen() concurrently 2. No socket in the same group found in sctp_ep_hashtable[] 3. Two sockets call reuseport_alloc() and form two reuseport groups 4. Only one group hit first in __sctp_rcv_lookup_endpoint() receives incoming packets Also, the reported null-ptr-deref could occur. TCP/UDP guarantees that would not happen by holding the hash bucket lock. Let's apply the locking strategy to __sctp_hash_endpoint() and __sctp_unhash_endpoint(). [0]: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000002: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] CPU: 1 UID: 0 PID: 10230 Comm: syz-executor119 Not tainted 6.10.0-syzkaller-12585-g301927d2d2eb #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 RIP: 0010:reuseport_add_sock+0x27e/0x5e0 net/core/sock_reuseport.c:350 Code: 00 0f b7 5d 00 bf 01 00 00 00 89 de e8 1b a4 ff f7 83 fb 01 0f 85 a3 01 00 00 e8 6d a0 ff f7 49 8d 7e 12 48 89 f8 48 c1 e8 03 <42> 0f b6 04 28 84 c0 0f 85 4b 02 00 00 41 0f b7 5e 12 49 8d 7e 14 RSP: 0018:ffffc9000b947c98 EFLAGS: 00010202 RAX: 0000000000000002 RBX: ffff8880252ddf98 RCX: ffff888079478000 RDX: 0000000000000000 RSI: 0000000000000001 RDI: 0000000000000012 RBP: 0000000000000001 R08: ffffffff8993e18d R09: 1ffffffff1fef385 R10: dffffc0000000000 R11: fffffbfff1fef386 R12: ffff8880252ddac0 R13: dffffc0000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 00007f24e45b96c0(0000) GS:ffff8880b9300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ffcced5f7b8 CR3: 00000000241be000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __sctp_hash_endpoint net/sctp/input.c:762 [inline] sctp_hash_endpoint+0x52a/0x600 net/sctp/input.c:790 sctp_listen_start net/sctp/socket.c:8570 [inline] sctp_inet_listen+0x767/0xa20	2024-08-26	5.5	CVE-2024-44935 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	net/sctp/socket.c:8625 __sys_listen_socket net/socket.c:1883 [inline] __sys_listen+0x1b7/0x230 net/socket.c:1894 __do_sys_listen net/socket.c:1902 [inline] __se_sys_listen net/socket.c:1900 [inline] __x64_sys_listen+0x5a/0x70 net/socket.c:1900 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f24e46039b9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 91 1a 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f24e45b9228 EFLAGS: 00000246 ORIG_RAX: 0000000000000032 RAX: ffffffffffffffda RBX: 00007f24e468e428 RCX: 00007f24e46039b9 RDX: 00007f24e46039b9 RSI: 0000000000000003 RDI: 0000000000000004 RBP: 00007f24e468e420 R08: 00007f24e45b96c0 R09: 00007f24e45b96c0 R10: 00007f24e45b96c0 R11: 0000000000000246 R12: 00007f24e468e42c R13: ---truncated---			
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: platform/x86: intel-vbtn: Protect ACPI notify handler against recursion Since commit e2ffcda16290 ("ACPI: OSL: Allow Notify () handlers to run on all CPUs") ACPI notify handlers like the intel-vbtn notify_handler() may run on multiple CPU cores racing with themselves. This race gets hit on Dell Venue 7140 tablets when undocking from the keyboard, causing the handler to try and register priv->switches_dev twice, as can be seen from the dev_info() message getting logged twice: [83.861800] intel-vbtn INT33D6:00: Registering Intel Virtual Switches input-dev after receiving a switch event [83.861858] input: Intel Virtual Switches as /devices/pci0000:00/0000:00:1f.0/PNP0C09:00/INT33D6:00/input/input17 [83.861865] intel-vbtn INT33D6:00: Registering Intel Virtual Switches input-dev after receiving a switch event After which things go seriously wrong: [83.861872] sysfs: cannot create duplicate filename '/devices/pci0000:00/0000:00:1f.0/PNP0C09:00/INT33D6:00/input/input17' ... [83.861967] kobject: kobject_add_internal failed for input17 with -EEXIST, don't try to register things with the same name in the same directory. [83.877338] BUG: kernel NULL pointer dereference, address: 0000000000000018 ... Protect intel-vbtn notify_handler() from racing with itself with a mutex to fix this.	2024-08-26	5.5	CVE-2024-44937 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
MagePeople Team--Taxi Booking Manager for WooCommerce	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MagePeople Team Taxi Booking Manager for WooCommerce allows Stored XSS.This issue affects Taxi Booking Manager for WooCommerce: through 1.0.9.	2024-08-29	5.9	CVE-2024-43986 audit@patchstack.com
master-nan--Sweet-CMS	A vulnerability was found in master-nan Sweet-CMS up to 5f441e022b8876f07cde709c77b5be6d2f262e3f. It has been declared as critical. This vulnerability affects unknown code of the file /table/index. The manipulation leads to sql injection. The attack can be initiated remotely. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The name of the patch is 146359646a5a90cb09156dbd0013b7df77f2aa6c. It is recommended to apply a patch to fix this issue.	2024-08-30	6.3	CVE-2024-8332 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
master-nan--Sweet-CMS	A vulnerability was found in master-nan Sweet-CMS up to 5f441e022b8876f07cde709c77b5be6d2f262e3f. It has been rated as problematic. This issue affects the function LogHandler of the file middleware/log.go. The manipulation leads to improper output neutralization for logs. The attack may be initiated remotely. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The identifier of the patch is 2024c370e6c78b07b358c9d4257fa5d1be732c38. It is recommended to apply a patch to fix this issue.	2024-08-30	4.3	CVE-2024-8334 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
matter-labs--era-compiler-solidity	zksolc is a Solidity compiler for ZKsync. All LLVM versions since 2015 fold `(xor (shl 1, x), -1)` to `(rotl ~1, x)` if run with optimizations enabled. Here `~1` is generated as an unsigned 64 bits number (`2^64-1`). This number is zero-extended to 256 bits on EraVM target while it should have been sign-extended. Thus instead of producing `roti 2^256 - 1, x` the compiler produces `rotl 2^64 - 1, x`. Analysis has shown that no contracts were affected by the date of publishing this advisory. This issue has been addressed in version 1.5.3. Users are advised to upgrade and redeploy all contracts. There are no known workarounds for this vulnerability.	2024-08-29	5.9	CVE-2024-45056 security-advisories@github.com security-advisories@github.com
maxfoundry--Media Library Folders	The Media Library Folders plugin for WordPress is vulnerable to unauthorized access due to missing capability checks on several AJAX functions in the media-library-plus.php file in all versions up to, and including, 8.2.3. This makes it possible for authenticated attackers, with subscriber-level access and above, to perform several actions related to managing media files and folder along with controlling settings.	2024-08-30	6.3	CVE-2024-7858 security@wordfence.com security@wordfence.com security@wordfence.com
mbis--Permalink Manager Lite	The Permalink Manager Lite plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'debug_data', 'debug_query', and 'debug_redirect' functions in all versions up to, and including, 2.4.4. This makes it possible for unauthenticated attackers to extract sensitive data including password, title, and content of password-protected posts.	2024-08-28	5.3	CVE-2024-8195 security@wordfence.com security@wordfence.com security@wordfence.com
Mediavine--Create by Mediavine	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Mediavine Create by Mediavine.This issue affects Create by Mediavine: from n/a through 1.9.8.	2024-08-26	5.3	CVE-2024-43264 audit@patchstack.com
MemberPress--Memberpress	The Memberpress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'mepr_screenname' and 'mepr_key' parameter in all versions up to, and including, 1.11.29 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.	2024-08-30	6.1	CVE-2024-5024 security@wordfence.com security@wordfence.com
Michael Leithold--DSGVO All in one for WP	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Michael Leithold DSGVO All in one for WP allows Stored XSS.This issue affects DSGVO All in one for WP: from n/a through 4.5.	2024-08-29	6.5	CVE-2024-43964 audit@patchstack.com
mihail-barinov--Share This Image	The Share This Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'alignment' parameter in all versions up to, and including, 2.01 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.	2024-08-31	6.4	CVE-2024-8108 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
mollieintegration--Mollie Payments	The Mollie Payments for WooCommerce plugin for WordPress is vulnerable to information exposure in all versions up to, and including, 7.7.0. This is due to the	2024-08-28	5.3	CVE-2024-6448 security@wordfenc

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
for WooCommerce	error reporting being enabled by default in multiple plugin files. This makes it possible for unauthenticated attackers to obtain the full path to instances, which they may be able to use in combination with other vulnerabilities or to simplify reconnaissance work. On its own, this information is of very limited use.			e.com security@wordfence.com security@wordfence.com
mongodb -- mongodb	In certain highly specific configurations of the host system and MongoDB server binary installation on Linux Operating Systems, it may be possible for a unintended actor with host-level access to cause the MongoDB Server binary to load unintended actor-controlled shared libraries when the server binary is started, potentially resulting in the unintended actor gaining full control over the MongoDB server process. This issue affects MongoDB Server v5.0 versions prior to 5.0.14 and MongoDB Server v6.0 versions prior to 6.0.3. Required Configuration: Only environments with Linux as the underlying operating system is affected by this issue	2024-08-27	6.7	CVE-2024-8207 cna@mongodb.com
msaari--Relevanssi Live Ajax Search	The Relevanssi Live Ajax Search plugin for WordPress is vulnerable to argument injection in all versions up to, and including, 2.4. This is due to insufficient validation of input supplied via POST data in the 'search' function. This makes it possible for unauthenticated attackers to inject arbitrary arguments into a WP_Query query and potentially expose sensitive information such as attachments or private posts.	2024-08-28	5.3	CVE-2024-7573 security@wordfence.com security@wordfence.com
MuffinGroup--Betheme	The Betheme theme for WordPress is vulnerable to Stored Cross-Site Scripting via several of the plugin's shortcodes in all versions up to, and including, 27.5.6 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.	2024-08-30	6.4	CVE-2024-3998 security@wordfence.com security@wordfence.com
myCred--myCred	Missing Authorization vulnerability in myCred.This issue affects myCred: from n/a through 2.7.2.	2024-08-26	5.3	CVE-2024-43214 audit@patchstack.com
n/a--jpress	A vulnerability has been found in jpress up to 5.1.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/template/edit of the component Template Module Handler. The manipulation leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-29	4.7	CVE-2024-8304 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
n/a--n/a	There is an Open Redirect vulnerability in Gnuboard v6.0.4 and below via the `url` parameter in login path.	2024-08-26	6.1	CVE-2024-39097 cve@mitre.org cve@mitre.org
n/a--n/a	openflights commit 5234b5b is vulnerable to Cross-Site Scripting (XSS) via php/trip.php	2024-08-29	6.1	CVE-2024-41345 cve@mitre.org
n/a--n/a	openflights commit 5234b5b is vulnerable to Cross-Site Scripting (XSS) via php/submit.php	2024-08-29	6.1	CVE-2024-41346 cve@mitre.org
n/a--n/a	openflights commit 5234b5b is vulnerable to Cross-Site Scripting (XSS) via php/settings.php	2024-08-29	6.1	CVE-2024-41347 cve@mitre.org

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	openflights commit 5234b5b is vulnerable to Cross-Site Scripting (XSS) via php/alsearch.php	2024-08-29	6.1	CVE-2024-41348 cve@mitre.org
n/a--n/a	bjyadmin commit a560fd5 is vulnerable to Cross Site Scripting (XSS) via Public/statics/umeditor1_2_3/php/imageUp.php	2024-08-29	6.1	CVE-2024-41350 cve@mitre.org cve@mitre.org
n/a--n/a	bjyadmin commit a560fd5 is vulnerable to Cross Site Scripting (XSS) via Public/statics/umeditor1_2_3/php/getContent.php	2024-08-29	6.1	CVE-2024-41351 cve@mitre.org cve@mitre.org
n/a--n/a	Organizr v1.90 is vulnerable to Cross Site Scripting (XSS) via api.php.	2024-08-29	6.1	CVE-2024-41371 cve@mitre.org cve@mitre.org
n/a--n/a	A Stored Cross Site Scripting (XSS) vulnerability was found in "/music/ajax.php?action=save_playlist" in Kashipara Music Management System v1.0. This vulnerability allows remote attackers to execute arbitrary code via "title" & "description" parameter fields.	2024-08-26	6.1	CVE-2024-42787 cve@mitre.org cve@mitre.org
n/a--n/a	A Stored Cross Site Scripting (XSS) vulnerability was found in "/music/ajax.php?action=save_music" in Kashipara Music Management System v1.0. This vulnerability allows remote attackers to execute arbitrary code via "title" & "artist" parameter fields.	2024-08-26	6.1	CVE-2024-42788 cve@mitre.org cve@mitre.org
n/a--n/a	A Reflected Cross Site Scripting (XSS) vulnerability was found in "/music/controller.php?page=test" in Kashipara Music Management System v1.0. This vulnerability allows remote attackers to execute arbitrary code via the "page" parameter.	2024-08-26	6.3	CVE-2024-42789 cve@mitre.org cve@mitre.org
n/a--n/a	A Reflected Cross Site Scripting (XSS) vulnerability was found in "/music/index.php?page=test" in Kashipara Music Management System v1.0. This vulnerability allows remote attackers to execute arbitrary code via the "page" parameter.	2024-08-26	6.1	CVE-2024-42790 cve@mitre.org cve@mitre.org
n/a--n/a	A cross-site scripting (XSS) vulnerability in the Create Product function of fastapi-admin pro v0.1.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Product Name parameter.	2024-08-26	6.1	CVE-2024-42816 cve@mitre.org cve@mitre.org
n/a--n/a	A cross-site scripting (XSS) vulnerability in the Config-Create function of fastapi-admin pro v0.1.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Product Name parameter.	2024-08-26	6.1	CVE-2024-42818 cve@mitre.org cve@mitre.org
n/a--n/a	Ruoyi v4.7.9 and before was discovered to contain a cross-site scripting (XSS) vulnerability via the sql parameter of the createTable() function at /tool/gen/create.	2024-08-28	6.1	CVE-2024-42900 cve@mitre.org cve@mitre.org
n/a--n/a	A cross-site scripting (XSS) vulnerability in the component /managers/multiple_freeleech.php of Gazelle commit 63b3370 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the torrents parameter.	2024-08-26	6.1	CVE-2024-44793 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	A cross-site scripting (XSS) vulnerability in the component /master/auth/OnedriveRedirect.php of PicUploader commit fcf82ea allows	2024-08-26	6.1	CVE-2024-44794 cve@mitre.org cve@mitre.org

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the error_description parameter.			cve@mitre.org
n/a--n/a	A cross-site scripting (XSS) vulnerability in the component /login/disabled.php of Gazelle commit 63b3370 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the username parameter.	2024-08-26	6.1	CVE-2024-44795 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	A cross-site scripting (XSS) vulnerability in the component /managers/enable_requests.php of Gazelle commit 63b3370 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the view parameter.	2024-08-26	5.4	CVE-2024-44797 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	A cross-site scripting (XSS) vulnerability in the component admin_ads.php of SeaCMS v12.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the ad description parameter.	2024-08-29	5.4	CVE-2024-44919 cve@mitre.org cve@mitre.org
n/a--n/a	EMI v.1.1.10 and before, fixed in v.1.1.11, contains an Improper Validation of Specified Index, Position, or Offset in Input vulnerability. The specific issue is a failure to validate slot index and decrement stack count in EMI mod for Minecraft, which allows in-game item duplication.	2024-08-28	4.3	CVE-2024-41564 cve@mitre.org cve@mitre.org
n/a--n/a	JustEnoughItems (JEI) 19.5.0.33 and before contains an Improper Validation of Specified Index, Position, or Offset in Input vulnerability. The specific issue is a failure to validate slot index in JEI for Minecraft, which allows in-game item duplication.	2024-08-28	4.3	CVE-2024-41565 cve@mitre.org cve@mitre.org
n/a--n/a	Roughly Enough Items (REI) v.16.0.729 and before contains an Improper Validation of Specified Index, Position, or Offset in Input vulnerability. The specific issue is a failure to validate slot index and decrement stack count in the Roughly Enough Items (REI) mod for Minecraft, which allows in-game item duplication.	2024-08-28	4.3	CVE-2024-42698 cve@mitre.org cve@mitre.org
n/a--n/a	TestLink before v.1.9.20 is vulnerable to Cross Site Scripting (XSS) via the pop-up on upload file. When uploading a file, the XSS payload can be entered into the file name.	2024-08-26	4.1	CVE-2024-42906 cve@mitre.org cve@mitre.org
Naiche--Dark Mode for WP Dashboard	Cross-Site Request Forgery (CSRF) vulnerability in Naiche Dark Mode for WP Dashboard.This issue affects Dark Mode for WP Dashboard: from n/a through 1.2.3.	2024-08-26	4.3	CVE-2024-43325 audit@patchstack.com
nextbricks -- bricksore	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Nextbricks Brickscore allows Stored XSS.This issue affects Brickscore: from n/a through 1.4.2.5.	2024-08-29	6.1	CVE-2024-43950 audit@patchstack.com
NitroPack Inc.--NitroPack	Improper Control of Generation of Code ('Code Injection') vulnerability in NitroPack Inc. NitroPack allows Code Injection.This issue affects NitroPack: from n/a through 1.16.7.	2024-08-29	4.8	CVE-2024-43922 audit@patchstack.com
Nouthemes--Leopard - WordPress offload media	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Nouthemes Leopard - WordPress offload media.This issue affects Leopard - WordPress offload media: from n/a through 2.0.36.	2024-08-26	6.5	CVE-2024-43257 audit@patchstack.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
NVIDIA--CUDA Toolkit	NVIDIA CUDA Toolkit contains a vulnerability in command `cuobjdump` where a user may cause an out-of-bound write by passing in a malformed ELF file. A successful exploit of this vulnerability may lead to code execution or denial of service.	2024-08-31	4.4	CVE-2024-0110 psirt@nvidia.com
NVIDIA--CUDA Toolkit	NVIDIA CUDA Toolkit contains a vulnerability in command 'cuobjdump' where a user may cause a crash or produce incorrect output by passing a malformed ELF file. A successful exploit of this vulnerability may lead to a limited denial of service or data tampering.	2024-08-31	4.4	CVE-2024-0111 psirt@nvidia.com
open-telemetry--opentelemetry-collector-contrib	The OpenTelemetry Collector module AWS firehose receiver is for ingesting AWS Kinesis Data Firehose delivery stream messages and parsing the records received based on the configured record type. `awsfirehosereceiver` allows unauthenticated remote requests, even when configured to require a key. OpenTelemetry Collector can be configured to receive CloudWatch metrics via an AWS Firehose Stream. Firehose sets the header `X-Amz-Firehose-Access-Key` with an arbitrary configured string. The OpenTelemetry Collector awsfirehosereceiver can optionally be configured to require this key on incoming requests. However, when this is configured it **still accepts incoming requests with no key**. Only OpenTelemetry Collector users configured with the "alpha" `awsfirehosereceiver` module are affected. This module was added in version v0.49.0 of the "Contrib" distribution (or may be included in custom builds). There is a risk of unauthorized users writing metrics. Carefully crafted metrics could hide other malicious activity. There is no risk of exfiltrating data. It's likely these endpoints will be exposed to the public internet, as Firehose does not support private HTTP endpoints. A fix was introduced in PR #34847 and released with v0.108.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-08-28	5.3	CVE-2024-45043 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
OpenRapid--RapidCMS	A vulnerability was found in OpenRapid RapidCMS up to 1.3.1. It has been classified as critical. This affects an unknown part of the file /admin/user/user-move-run.php. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-30	6.3	CVE-2024-8331 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
OpenRapid--RapidCMS	A vulnerability classified as critical has been found in OpenRapid RapidCMS up to 1.3.1. Affected is an unknown function of the file /resource/runlogon.php. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-30	6.3	CVE-2024-8335 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
OpenText--NetIQ Access Manager	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in OpenText NetIQ Access Manager allows access the sensitive information.Â This issue affects NetIQ Access Manager before 5.0.4 and before 5.1.	2024-08-28	5.7	CVE-2024-4556 security@opentext.com security@opentext.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
OpenText--NetIQ Advance Authentication	A vulnerability identified in NetIQ Advance Authentication that leaks sensitive server information. This issue affects NetIQ Advance Authentication version before 6.3.5.1	2024-08-28	6.3	CVE-2021-22529 security@opentext.com
OpenText--NetIQ Advance Authentication	A Cross-Site Scripting vulnerable identified in NetIQ Advance Authentication that impacts the server functionality and disclose sensitive information. This issue affects NetIQ Advance Authentication before 6.3.5.1	2024-08-28	6.2	CVE-2021-38122 security@opentext.com
OpenText--NetIQ Advance Authentication	A vulnerability identified in Advance Authentication that allows bash command Injection in administrative controlled functionality of backup due to improper handling in providedÂ command parameters. This issue affects NetIQ Advance Authentication version before 6.3.5.1.	2024-08-28	5.1	CVE-2021-38120 security@opentext.com
OpenZeppelin--cairo-contracts	Cairo-Contracts are OpenZeppelin Contracts written in Cairo for Starknet, a decentralized ZK Rollup. This vulnerability can lead to unauthorized ownership transfer, contrary to the original owner's intention of leaving the contract without an owner. It introduces a security risk where an unintended party (pending owner) can gain control of the contract after the original owner has renounced ownership. This could also be used by a malicious owner to simulate leaving a contract without an owner, to later regain ownership by previously having proposed himself as a pending owner. This issue has been addressed in release version 0.16.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-08-31	5.3	CVE-2024-45304 security-advisories@github.com security-advisories@github.com security-advisories@github.com
OTRS AG--OTRS	Improper Neutralization of Input done by an attacker with admin privileges ('Cross-site Scripting') inÂ OTRS (System Configuration modules) and ((OTRS)) Community Edition allows Cross-Site Scripting (XSS) within the System Configuration targeting other admins. This issue affects:Â * OTRS from 7.0.X through 7.0.50 * OTRS 8.0.X * OTRS 2023.X * OTRS from 2024.X through 2024.5.X * ((OTRS)) Community Edition: 6.0.x Products based on the ((OTRS)) Community Edition also very likely to be affected	2024-08-26	4.9	CVE-2024-43442 security@otrs.com
OTRS AG--OTRS	Improper Neutralization of Input done by an attacker with admin privileges ('Cross-site Scripting') in Process Management modules of OTRS and ((OTRS)) Community Edition allows Cross-Site Scripting (XSS) within the Process Management targeting other admins. This issue affects: * OTRS from 7.0.X through 7.0.50 * OTRS 8.0.X * OTRS 2023.X * OTRS from 2024.X through 2024.5.X * ((OTRS)) Community Edition: 6.0.x Products based on the ((OTRS)) Community Edition also very likely to be affected	2024-08-26	4.9	CVE-2024-43443 security@otrs.com
Oxygen Builder--Oxygen Builder	The Oxygen Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the oxy_save_css_from_admin AJAX action in all versions up to, and including, 4.8.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update stylesheets.	2024-08-27	4.3	CVE-2024-6688 security@wordfence.com security@wordfence.com
pagebuilderaddons--web_and_woocommerce_addons_for_wpbakery_builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Page Builder Addons Web and WooCommerce Addons for WPBakery Builder allows Stored XSS.This issue affects Web and WooCommerce Addons for WPBakery Builder: from n/a through 1.4.6.	2024-08-29	4.8	CVE-2024-43960 audit@patchstack.com
Passionate Programmers B.V.-	Cross-Site Request Forgery (CSRF) vulnerability in Passionate Programmers B.V. WP Data Access.This issue affects WP Data Access: from n/a through 5.5.7.	2024-08-26	4.3	CVE-2024-43295 audit@patchstack.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
-WP Data Access				com
PHPOffice--PhpSpreadsheet	PHPSpreadsheet is a pure PHP library for reading and writing spreadsheet files. In affected versions `\PhpOffice\PhpSpreadsheet\Writer\Html` doesn't sanitize spreadsheet styling information such as font names, allowing an attacker to inject arbitrary JavaScript on the page. As a result an attacker may used a crafted spreadsheet to fully takeover a session of a user viewing spreadsheet files as HTML. This issue has been addressed in release version 2.1.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-08-28	5.4	CVE-2024-45046 security-advisories@github.com security-advisories@github.com security-advisories@github.com
popupbuilder--Popup Builder Create highly converting, mobile friendly marketing popups.	The Popup Builder plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.3.3 via the Subscribers Import feature. This makes it possible for unauthenticated attackers to extract sensitive data after an administrator has imported subscribers via a CSV file. This data may include the first name, last name, e-mail address, and potentially other personally identifiable information of subscribers.	2024-08-29	5.3	CVE-2024-2541 security@wordfence.com security@wordfence.com
Progress Software Corporation--WS_FTP Server	In WS_FTP Server versions before 8.8.8 (2022.0.8), an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in the Web Transfer Module allows File Discovery, Probe System Files, User-Controlled Filename, Path Traversal. Â An authenticated file download flaw has been identified where a user can craft an API call that allows them to download a file from an arbitrary folder on the drive where that user host's root folder is located (by default this is C:)	2024-08-28	6.5	CVE-2024-7744 security@progress.com security@progress.com
Progress Software Corporation--WS_FTP Server	In WS_FTP Server versions before 8.8.8 (2022.0.8), a Missing Critical Step in Multi-Factor Authentication of the Web Transfer Module allows users to skip the second-factor verification and log in with username and password only.	2024-08-28	6.5	CVE-2024-7745 security@progress.com security@progress.com
ptc -- thingworx	An Insecure Direct Object Reference (IDOR) in PTC ThingWorx v9.5.0 allows attackers to view sensitive information, including PII, regardless of access level.	2024-08-27	6.5	CVE-2024-40395 cve@mitre.org
rakuten -- ichiba	'Rakuten Ichiba App' for Android 12.4.0 and earlier and 'Rakuten Ichiba App' for iOS 11.7.0 and earlier are vulnerable to improper authorization in handler for custom URL scheme. An arbitrary site may be displayed on the WebView of the product via Intent from another application installed on the user's device. As a result, the user may be redirected to an unauthorized site, and the user may become a victim of a phishing attack.	2024-08-29	6.1	CVE-2024-41918 vultures@jpcert.or.jp vultures@jpcert.or.jp vultures@jpcert.or.jp
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in libvirt. A refactor of the code fetching the list of interfaces for multiple APIs introduced a corner case on platforms where allocating 0 bytes of memory results in a NULL pointer. This corner case would lead to a NULL-pointer dereference and subsequent crash of virtinterfaced. This issue could allow clients connecting to the read-only socket to crash the virtinterfaced daemon.	2024-08-30	6.2	CVE-2024-8235 secalert@redhat.com secalert@redhat.com secalert@redhat.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rems -- qr_code_attendance_system	A vulnerability, which was classified as problematic, has been found in SourceCodester QR Code Attendance System 1.0. This issue affects some unknown processing of the file /endpoint/delete-student.php. The manipulation of the argument student/attendance leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-26	6.1	CVE-2024-8172 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
restsharp--RestSharp	RestSharp is a Simple REST and HTTP API Client for .NET. The second argument to `RestRequest.AddHeader` (the header value) is vulnerable to CRLF injection. The same applies to `RestRequest.AddOrUpdateHeader` and `RestClient.AddDefaultHeader`. The way HTTP headers are added to a request is via the `HttpHeaders.TryAddWithoutValidation` method which does not check for CRLF characters in the header value. This means that any headers from a `RestSharp.RequestHeaders` object are added to the request in such a way that they are vulnerable to CRLF-injection. In general, CRLF-injection into a HTTP header (when using HTTP/1.1) means that one can inject additional HTTP headers or smuggle whole HTTP requests. If an application using the RestSharp library passes a user-controllable value through to a header, then that application becomes vulnerable to CRLF-injection. This is not necessarily a security issue for a command line application like the one above, but if such code were present in a web application then it becomes vulnerable to request splitting (as shown in the PoC) and thus Server Side Request Forgery. Strictly speaking this is a potential vulnerability in applications using RestSharp, not in RestSharp itself, but I would argue that at the very least there needs to be a warning about this behaviour in the RestSharp documentation. RestSharp has addressed this issue in version 112.0.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-08-29	6.1	CVE-2024-45302 security-advisories@github.com security-advisories@github.com security-advisories@github.com
Robert Felty--Collapsing Archives	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Robert Felty Collapsing Archives allows Stored XSS.This issue affects Collapsing Archives: from n/a through 3.0.5.	2024-08-29	6.5	CVE-2024-43934 audit@patchstack.com
ruijie -- eg2000k_firmware	A vulnerability has been found in Ruijie EG2000K 11.1(6)B2 and classified as critical. This vulnerability affects unknown code of the file /tool/index.php?c=download&a=save. The manipulation of the argument content leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-26	4.9	CVE-2024-8166 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Saturday Drive--Ninja Forms	Cross-Site Request Forgery (CSRF) vulnerability in Saturday Drive Ninja Forms.This issue affects Ninja Forms: from n/a through 3.8.6.	2024-08-26	5.4	CVE-2024-39628 audit@patchstack.com
Sender--Sender Newsletter, SMS and Email Marketing Automation for WooCommerce	Cross-Site Request Forgery (CSRF) vulnerability in Sender Sender - Newsletter, SMS and Email Marketing Automation for WooCommerce.This issue affects Sender - Newsletter, SMS and Email Marketing Automation for WooCommerce: from n/a through 2.6.18.	2024-08-26	4.3	CVE-2024-39657 audit@patchstack.com
Shared Files File Upload Form--Shared Files	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Shared Files - File Upload Form Shared Files.This issue affects Shared Files: from n/a through 1.7.28.	2024-08-26	5.3	CVE-2024-43230 audit@patchstack.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Sk. Abul Hasan--Animated Number Counters	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Sk. Abul Hasan Animated Number Counters allows PHP Local File Inclusion.This issue affects Animated Number Counters: from n/a through 1.9.	2024-08-29	6.5	CVE-2024-43957 audit@patchstack.com
SKT Themes--SKT Blocks Gutenberg based Page Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SKT Themes SKT Blocks - Gutenberg based Page Builder allows Stored XSS.This issue affects SKT Blocks - Gutenberg based Page Builder: from n/a through 1.5.	2024-08-29	6.5	CVE-2024-43946 audit@patchstack.com
smashballoon -- reviews_feed	The Reviews Feed - Add Testimonials and Customer Reviews From Google Reviews, Yelp, TripAdvisor, and More plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_api_key' function in all versions up to, and including, 1.1.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update API Key options.	2024-08-27	4.3	CVE-2024-8199 security@wordfence.com security@wordfence.com security@wordfence.com
smashballoon -- reviews_feed	The Reviews Feed - Add Testimonials and Customer Reviews From Google Reviews, Yelp, TripAdvisor, and More plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the 'update_api_key' function. This makes it possible for unauthenticated attackers to update an API key via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-08-27	4.3	CVE-2024-8200 security@wordfence.com security@wordfence.com security@wordfence.com
Softaculous Team--SpeedyCache	Cross-Site Request Forgery (CSRF) vulnerability in Softaculous Team SpeedyCache.This issue affects SpeedyCache: from n/a through 1.1.8.	2024-08-26	5.4	CVE-2024-43299 audit@patchstack.com
SourceCodester--Computer Laboratory Management System	A vulnerability classified as critical has been found in SourceCodester Computer Laboratory Management System 1.0. Affected is the function update_settings_info of the file /classes/SystemSettings.php?f=update_settings. The manipulation of the argument name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-30	6.3	CVE-2024-8346 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Computer Laboratory Management System	A vulnerability classified as critical was found in SourceCodester Computer Laboratory Management System 1.0. Affected by this vulnerability is the function delete_record of the file /classes/Master.php?f=delete_record. 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.	2024-08-30	6.3	CVE-2024-8347 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Computer Laboratory Management System	A vulnerability, which was classified as critical, has been found in SourceCodester Computer Laboratory Management System 1.0. Affected by this issue is the function delete_category of the file /classes/Master.php?f=delete_category. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-30	6.3	CVE-2024-8348 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Electric Billing Management	A vulnerability was found in SourceCodester Electric Billing Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /?page=tracks of the component Connection Code Handler.	2024-08-30	6.3	CVE-2024-8339 cna@vuldb.com cna@vuldb.com cna@vuldb.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
System	The manipulation of the argument code leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.			cna@vuldb.com cna@vuldb.com
SourceCodester--Music Gallery Site	A vulnerability classified as critical was found in SourceCodester Music Gallery Site 1.0. Affected by this vulnerability is an unknown functionality of the file /php-music/classes/Master.php?f=delete_music. 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.	2024-08-30	6.3	CVE-2024-8336 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Music Gallery Site	A vulnerability was found in SourceCodester Music Gallery Site 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /classes/Users.php?f=delete. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-30	6.3	CVE-2024-8345 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Petshop Management System	A vulnerability classified as critical was found in SourceCodester Petshop Management System 1.0. This vulnerability affects unknown code of the file /controllers/add_user.php. The manipulation of the argument avatar leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-30	6.3	CVE-2024-8341 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Petshop Management System	A vulnerability, which was classified as critical, has been found in SourceCodester Petshop Management System 1.0. This issue affects some unknown processing of the file /controllers/add_client.php. The manipulation of the argument image_profile leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-30	6.3	CVE-2024-8342 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Stark Digital--WP Testimonial Widget	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Stark Digital WP Testimonial Widget allows Stored XSS.This issue affects WP Testimonial Widget: from n/a through 3.1.	2024-08-26	5.9	CVE-2024-43967 audit@patchstack.com
Store Locator Plus--Store Locator Plus	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Store Locator Plus.This issue affects Store Locator Plus: from n/a through 2311.17.01.	2024-08-26	5.3	CVE-2024-43258 audit@patchstack.com
Styra--OPA	A SMB force-authentication vulnerability exists in all versions of OPA for Windows prior to v0.68.0. The vulnerability exists because of improper input validation, allowing a user to pass an arbitrary SMB share instead of a Rego file as an argument to OPA CLI or to one of the OPA Go library's functions.	2024-08-30	6.1	CVE-2024-8260 vulnreport@tenable.com
sveltejs--svelte	svelte performance oriented web framework. A potential mXSS vulnerability exists in Svelte for versions up to but not including 4.2.19. Svelte improperly escapes HTML on server-side rendering. The assumption is that attributes will always stay as such, but in some situation the final DOM tree rendered on browsers is different from what Svelte expects on server-side rendering. This may be leveraged to perform XSS attacks, and a type of the XSS is known as mXSS (mutation XSS). More specifically, this can occur when injecting malicious content into an attribute within a `noscript` tag. This issue has been addressed in release version 4.2.19. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2024-08-30	5.4	CVE-2024-45047 security-advisories@github.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tagDiv--tagDiv Composer	The tagDiv Composer plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'envato_code[]' parameter in all versions up to, and including, 5.0 due to insufficient input sanitization and output escaping within the on_ajax_check_envato_code function. 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.	2024-08-31	6.1	CVE-2024-3886 security@wordfence.com security@wordfence.com
tagDiv--tagDiv Composer	The tagDiv Composer plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'envato_code[]' parameter in all versions up to, and including, 5.0 due to insufficient input sanitization and output escaping within the on_ajax_register_forum_user function. 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.	2024-08-31	6.1	CVE-2024-5212 security@wordfence.com security@wordfence.com
TeamViewer--Meeting	Improper access control in the clipboard synchronization feature in TeamViewer Full Client prior version 15.57 and TeamViewer Meeting prior version 15.55.3 can lead to unintentional sharing of the clipboard with the current presenter of a meeting.	2024-08-28	4.3	CVE-2024-6053 psirt@teamviewer.com
techjewel--Contact Form Plugin by Fluent Forms for Quiz, Survey, and Drag & Drop WP Form Builder	The Contact Form Plugin by Fluent Forms for Quiz, Survey, and Drag & Drop WP Form Builder plugin for WordPress is vulnerable to unauthorized Malichimp API key update due to an insufficient capability check on the verifyRequest function in all versions up to, and including, 5.1.18. This makes it possible for Form Managers with a Subscriber-level access and above to modify the Mailchimp API key used for integration. At the same time, missing Mailchimp API key validation allows the redirect of the integration requests to the attacker-controlled server.	2024-09-01	4.2	CVE-2024-5053 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
techjewel--Ninja Tables Easiest Data Table Builder	The Ninja Tables - Easiest Data Table Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 5.0.12 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.	2024-08-27	6.4	CVE-2024-7304 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
techlabpro1--The Post Grid Shortcode, Gutenberg Blocks and Elementor Addon for Post Grid	The The Post Grid - Shortcode, Gutenberg Blocks and Elementor Addon for Post Grid plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 7.7.11 via the post_query_guten and post_query functions. This makes it possible for authenticated attackers, with contributor-level access and above, to extract information from posts that are not public (i.e. draft, future, etc..).	2024-08-29	4.3	CVE-2024-7418 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
teldat -- rs123_firmware	Cross Site Scripting vulnerability in Teldats Router RS123, RS123w allows attacker to execute arbitrary code via the cmdcookie parameter to the upgrade/query.php page.	2024-08-27	4.8	CVE-2022-39996 cve@mitre.org cve@mitre.org

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
The Tcpdump Group--libpcap	In affected libpcap versions during the setup of a remote packet capture the internal function sock_initaddress() calls getaddrinfo() and possibly freeaddrinfo(), but does not clearly indicate to the caller function whether freeaddrinfo() still remains to be called after the function returns. This makes it possible in some scenarios that both the function and its caller call freeaddrinfo() for the same allocated memory block. A similar problem was reported in Apple libpcap, to which Apple assigned CVE-2023-40400.	2024-08-31	4.4	CVE-2023-7256 security@tcpdump.org security@tcpdump.org
The Tcpdump Group--libpcap	Remote packet capture support is disabled by default in libpcap. When a user builds libpcap with remote packet capture support enabled, one of the functions that become available is pcap_findalldevs_ex(). One of the function arguments can be a filesystem path, which normally means a directory with input data files. When the specified path cannot be used as a directory, the function receives NULL from opendir(), but does not check the return value and passes the NULL value to readdir(), which causes a NULL pointer derefence.	2024-08-31	4.4	CVE-2024-8006 security@tcpdump.org security@tcpdump.org
themefic--Tourfic Ultimate Hotel Booking, Travel Booking & Apartment Booking WordPress Plugin | WooCommerce Booking	The Tourfic plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.11.20. This is due to missing or incorrect nonce validation on the tf_order_status_email_resend_function, tf_visitor_details_edit_function, tf_checkinout_details_edit_function, tf_order_status_edit_function, tf_order_bulk_action_edit_function, tf_remove_room_order_ids, and tf_delete_old_review_fields functions. This makes it possible for unauthenticated attackers to resend order status emails, update visitor/order details, edit check-in/out details, edit order status, perform bulk order status updates, remove room order IDs, and delete old review fields, respectively, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-08-30	4.3	CVE-2024-8319 security@wordfence.com security@wordfence.com
themeum -- droip	Incorrect Authorization vulnerability in Themeum Droip allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Droip: from n/a through 1.1.1.	2024-08-29	6.3	CVE-2024-43954 audit@patchstack.com
Themeum--Tutor LMS	Cross-Site Request Forgery (CSRF) vulnerability in Themeum Tutor LMS.This issue affects Tutor LMS: from n/a through 2.7.2.	2024-08-26	5.4	CVE-2024-39645 audit@patchstack.com
ThimPress--LearnPress	Cross-Site Request Forgery (CSRF) vulnerability in ThimPress LearnPress.This issue affects LearnPress: from n/a through 4.2.6.8.2.	2024-08-26	4.3	CVE-2024-39641 audit@patchstack.com
Trellix--Trellix NX, EX, AX, FX, CMS and IVX	An authenticated user can access the restricted files from NX, EX, FX, AX, IVX and CMS using path traversal.	2024-08-27	5.9	CVE-2024-7608 trellixpsirt@trellix.com
Unknown--Gutentor	The Gutentor WordPress plugin before 3.3.6 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	2024-08-29	5.4	CVE-2024-5417 contact@wpscan.com
Unknown--Page Builder Gutenberg Blocks	The Page Builder Gutenberg Blocks WordPress plugin before 3.1.13 does not escape the content of post embed via one of its block, which could allow users with the capability to publish posts (editor and admin by default) to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2024-08-29	4.8	CVE-2024-7132 contact@wpscan.com
Unknown--Quiz and Survey Master	The Quiz and Survey Master (QSM) WordPress plugin before 9.1.1 fails to validate and escape certain Quiz fields before displaying them on a page or post where the	2024-08-26	4.7	CVE-2024-6879 contact@wpscan.c

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
(QSM)	Quiz is embedded, which could allows contributor and above roles to perform Stored Cross-Site Scripting (XSS) attacks.			om
Unknown--Shield Security	The Shield Security WordPress plugin before 20.0.6 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	2024-08-26	6.1	CVE-2024-7313 contact@wpscan.com
Unknown--Viral Signup	The Viral Signup WordPress plugin through 2.1 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)	2024-08-29	4.8	CVE-2024-6927 contact@wpscan.com
vim--vim	Vim is an improved version of the unix vi text editor. When flushing the typeahead buffer, Vim moves the current position in the typeahead buffer but does not check whether there is enough space left in the buffer to handle the next characters. So this may lead to the tb_off position within the typebuf variable to point outside of the valid buffer size, which can then later lead to a heap-buffer overflow in e.g. ins_typebuf(). Therefore, when flushing the typeahead buffer, check if there is enough space left before advancing the off position. If not, fall back to flush current typebuf contents. It's not quite clear yet, what can lead to this situation. It seems to happen when error messages occur (which will cause Vim to flush the typeahead buffer) in comnination with several long mappgins and so it may eventually move the off position out of a valid buffer size. Impact is low since it is not easily reproducible and requires to have several mappings active and run into some error condition. But when this happens, this will cause a crash. The issue has been fixed as of Vim patch v9.1.0697. Users are advised to upgrade. There are no known workarounds for this issue.	2024-08-26	4.5	CVE-2024-43802 security-advisories@github.com security-advisories@github.com
vol4ikman--WP Accessibility Helper (WAH)	The WP Accessibility Helper (WAH) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'save_contrast_variations' and 'save_empty_contrast_variations' functions in all versions up to, and including, 0.6.2.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to edit or delete contrast settings. Please note these issues were patched in 0.6.2.8, though it broke functionality and the vendor has not responded to our follow-ups.	2024-08-29	5.4	CVE-2024-5987 security@wordfence.com security@wordfence.com
waspthemes -- yellowpencil	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WaspThemes YellowPencil Visual CSS Style Editor allows Reflected XSS.This issue affects YellowPencil Visual CSS Style Editor: from n/a through 7.6.1.	2024-08-29	6.1	CVE-2024-43963 audit@patchstack.com
webdevmattcrom--GiveWP Donation Plugin and Fundraising Platform	The GiveWP - Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.15.1. This is due to the plugin utilizing Symfony and leaving display_errors on within test files. This makes it possible for unauthenticated attackers 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.	2024-08-29	5.3	CVE-2024-6551 security@wordfence.com security@wordfence.com
webinarpress -- webinarpress	Cross-Site Request Forgery (CSRF) vulnerability in WebinarPress allows Cross-Site Scripting (XSS).This issue affects WebinarPress: from n/a through 1.33.20.	2024-08-26	6.1	CVE-2024-43339 audit@patchstack.com
webpack.js -- webpack	Webpack is a module bundler. Its main purpose is to bundle JavaScript files for usage in a browser, yet it is also capable of transforming, bundling, or packaging just about any resource or asset. The webpack developers have discovered a DOM Clobbering vulnerability in Webpack's `AutoPublicPathRuntimeModule`. The DOM Clobbering gadget in the module can lead to cross-site scripting (XSS) in web pages where scriptless attacker-controlled HTML elements (e.g., an `img` tag with an	2024-08-27	6.1	CVE-2024-43788 security-advisories@github.com security-advisories@github.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unsanitized `name` attribute) are present. Real-world exploitation of this gadget has been observed in the Canvas LMS which allows a XSS attack to happen through a javascript code compiled by Webpack (the vulnerable part is from Webpack). DOM Clobbering is a type of code-reuse attack where the attacker first embeds a piece of non-script, seemingly benign HTML markups in the webpage (e.g. through a post or comment) and leverages the gadgets (pieces of js code) living in the existing javascript code to transform it into executable code. This vulnerability can lead to cross-site scripting (XSS) on websites that include Webpack-generated files and allow users to inject certain scriptless HTML tags with improperly sanitized name or id attributes. This issue has been addressed in release version 5.94.0. All users are advised to upgrade. There are no known workarounds for this issue.			com security-advisories@github.com security-advisories@github.com
webtechstreet--Elementor Addon Elements	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' and 'eae_slider_animation' parameters in all versions up to, and including, 1.13.5 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.	2024-08-30	6.4	CVE-2024-4401 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
webtechstreet--Elementor Addon Elements	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 1.13.6 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.	2024-08-30	6.4	CVE-2024-7122 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
wireshark -- wireshark	NTLMSSP dissector crash in Wireshark 4.2.0 to 4.0.6 and 4.0.0 to 4.0.16 allows denial of service via packet injection or crafted capture file	2024-08-29	5.5	CVE-2024-8250 cve@gitlab.com cve@gitlab.com
wolfSSL Inc.--wolfSSL	An issue was discovered in wolfSSL before 5.7.0. A safe-error attack via Rowhammer, namely FAULT+PROBE, leads to ECDSA key disclosure. When WOLFSSL_CHECK_SIG_FAULTS is used in signing operations with private ECC keys, such as in server-side TLS connections, the connection is halted if any fault occurs.Â The success rate in a certain amount of connection requests can be processed via an advanced technique for ECDSA key recovery.	2024-08-27	5.1	CVE-2024-5288 facts@wolfssl.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WolfSSL--wolfCrypt	Fault Injection vulnerability inÂ wc_ed25519_sign_msg function in wolfssl/wolfcrypt/src/ed25519.c in WolfSSL wolfssl5.6.6 on Linux/Windows allows remote attackerÂ co-resides in the same system with a victim process toÂ disclose information and escalate privileges via Rowhammer fault injection to the ed25519_key structure.	2024-08-30	6.7	CVE-2024-2881 facts@wolfssl.com
WolfSSL--wolfCrypt	Fault Injection vulnerability in RsaPrivateDecryption function in wolfssl/wolfcrypt/src/rsa.c in WolfSSL wolfssl5.6.6 on Linux/Windows allows remote attackerÂ co-resides in the same system with a victim process toÂ disclose information and escalate privileges via Rowhammer fault injection to the RsaKey structure.	2024-08-29	5.9	CVE-2024-1545 facts@wolfssl.com
wolfSSL--wolfSSL	The side-channel protected T-Table implementation in wolfSSL up to version 5.6.5 protects against a side-channel attacker with cache-line resolution. In a controlled environment such as Intel SGX, an attacker can gain a per instruction sub-cache-line resolution allowing them to break the cache-line-level protection. For details on the attack refer to: https://doi.org/10.46586/tches.v2024.i1.457-500	2024-08-29	4.1	CVE-2024-1543 facts@wolfssl.com
wolfSSL--wolfSSL	Generating the ECDSA nonce k samples a random number r and then truncates this randomness with a modular reduction mod n where n is the order of the elliptic curve. Meaning k = r mod n. The division used during the reduction estimates a factor q_e by dividing the upper two digits (a digit having e.g. a size of 8 byte) of r by the upper digit of n and then decrements q_e in a loop until it has the correct size. Observing the number of times q_e is decremented through a control-flow revealing side-channel reveals a bias in the most significant bits of k. Depending on the curve this is either a negligible bias or a significant bias large enough to reconstruct k with lattice reduction methods. For SECP160R1, e.g., we find a bias of 15 bits.	2024-08-27	4.1	CVE-2024-1544 facts@wolfssl.com
WP Delicious--Delicious Recipes WordPress Recipe Plugin	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Delicious Delicious Recipes - WordPress Recipe Plugin allows Stored XSS.This issue affects Delicious Recipes - WordPress Recipe Plugin: from n/a through 1.6.7.	2024-08-29	6.5	CVE-2024-43935 audit@patchstack.com
WPBackItUp--Backup and Restore WordPress	Cross-Site Request Forgery (CSRF) vulnerability in WPBackItUp Backup and Restore WordPress.This issue affects Backup and Restore WordPress: from n/a through 1.50.	2024-08-26	4.3	CVE-2024-43269 audit@patchstack.com
wpbakery --page_builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Classic Addons Classic Addons - WPBakery Page Builder allows Stored XSS.This issue affects Classic Addons - WPBakery Page Builder: from n/a through 3.0.	2024-08-29	5.4	CVE-2024-43953 audit@patchstack.com
wpdevelop--WP Booking Calendar	The WP Booking Calendar plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via several parameters from 'timeline_obj' in all versions up to, and including, 10.5 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.	2024-08-30	6.1	CVE-2024-8274 security@wordfence.com security@wordfence.com security@wordfence.com
WPDeveloper--EmbedPress	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloper EmbedPress allows Stored XSS.This issue affects EmbedPress: from n/a through 4.0.8.	2024-08-29	6.5	CVE-2024-43936 audit@patchstack.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WPMU DEV--Hummingbird	Cross-Site Request Forgery (CSRF) vulnerability in WPMU DEV Hummingbird.This issue affects Hummingbird: from n/a through 3.9.1.	2024-08-26	4.3	CVE-2024-43117 audit@patchstack.com
wpusermanager--wp_user_manager	Cross-Site Request Forgery (CSRF) vulnerability in WP User Manager.This issue affects WP User Manager: from n/a through 2.9.10.	2024-08-26	4.3	CVE-2024-43336 audit@patchstack.com
wpwax--Logo Showcase Ultimate Logo Carousel, Logo Slider & Logo Grid	The Logo Showcase Ultimate - Logo Carousel, Logo Slider & Logo Grid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-08-27	6.4	CVE-2024-8046 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
wpzoom--WPZOOM Portfolio Lite Filterable Portfolio Plugin	The WPZOOM Portfolio Lite - Filterable Portfolio Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' attribute within the 'wp:wpzoom-blocks' Gutenberg block in all versions up to, and including, 1.4.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-31	6.4	CVE-2024-8276 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
Xiaomi--Router AX9000	The Xiaomi router AX9000 has a post-authentication command injection vulnerability. This vulnerability is caused by the lack of input filtering, allowing an attacker to exploit it to obtain root access to the device.	2024-08-26	6.5	CVE-2023-26315 security@xiaomi.com
Xiaomi--Xiaomi File Manager App International Version	A path traversal vulnerability exists in the Xiaomi File Manager application product(international version). The vulnerability is caused by unfiltered special characters and can be exploited by attackers to overwrite and execute code in the file.	2024-08-28	6.3	CVE-2023-26321 security@xiaomi.com
xpro--140+ Widgets | Xpro Addons For Elementor FREE	The 140+ Widgets | Xpro Addons For Elementor - FREE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'arrow' parameter within the Post Grid widget in all versions up to, and including, 1.4.4.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-27	6.4	CVE-2024-7791 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
youtag--Two-factor authentication	The IP Vault - WP Firewall plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 1.1. This is due to insufficient restrictions on where the IP Address information is being retrieved for request logging and	2024-08-31	5.3	CVE-2022-4536 security@wordfence.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
(formerly IP Vault)	login restrictions. Attackers can supply the X-Forwarded-For header with with a different IP Address that will be logged and can be used to bypass settings that may have blocked out an IP address or country from logging in.			security@wordfence.com
zephyr-one -- zephyr_project_manager	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Dylan James Zephyr Project Manager allows Reflected XSS.This issue affects Zephyr Project Manager: from n/a through .3.102.	2024-08-26	5.4	CVE-2024-43915 audit@patchstack.com
zynith -- zynith	Missing Authorization vulnerability in VIICTORY MEDIA LLC Z Y N I T H allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Z Y N I T H: from n/a through 7.4.9.	2024-08-29	6.5	CVE-2024-43939 audit@patchstack.com
zynith -- zynith	Missing Authorization vulnerability in VIICTORY MEDIA LLC Z Y N I T H allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Z Y N I T H: from n/a through 7.4.9.	2024-08-29	6.5	CVE-2024-43940 audit@patchstack.com
2j-slideshow--Slideshow, Image Slider by 2J	The Slideshow, Image Slider by 2J plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'post' parameter in versions up to, and including, 1.3.54 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.	2024-08-17	6.1	CVE-2023-4604 security@wordfence.com security@wordfence.com
adobe -- acrobat	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	5.5	CVE-2024-41832 psirt@adobe.com
adobe -- acrobat	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	5.5	CVE-2024-41833 psirt@adobe.com
adobe -- acrobat	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	5.5	CVE-2024-41834 psirt@adobe.com
adobe -- acrobat	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 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.	2024-08-14	5.5	CVE-2024-41835 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction.	2024-08-14	6.3	CVE-2024-39408 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into	2024-08-14	6.3	CVE-2024-39409 psirt@adobe.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction.			
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an attacker to bypass security features and perform minor unauthorised actions on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a malicious request. Exploitation of this issue requires user interaction.	2024-08-14	5.5	CVE-2024-39410 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures to view and edit low-sensitivity information. Exploitation of this issue does not require user interaction.	2024-08-14	5.4	CVE-2024-39418 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	CVE-2024-39404 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	CVE-2024-39405 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	CVE-2024-39407 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	CVE-2024-39411 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	CVE-2024-39412 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	CVE-2024-39413 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	CVE-2024-39414 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass	2024-08-14	4.3	CVE-2024-39415 psirt@adobe.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	security measures and disclose minor information. Exploitation of this issue does not require user interaction.			
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	CVE-2024-39416 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	CVE-2024-39417 psirt@adobe.com
adobe -- commerce	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.	2024-08-14	4.3	CVE-2024-39419 psirt@adobe.com
adobe -- illustrator	Illustrator versions 28.5, 27.9.4 and earlier are affected by an Improper Input Validation vulnerability that could lead to an application denial-of-service condition. An attacker could exploit this vulnerability to render the application unresponsive or terminate its execution. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	5.5	CVE-2024-34118 psirt@adobe.com
adobe -- illustrator	Illustrator versions 28.5, 27.9.4 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.	2024-08-14	5.5	CVE-2024-34134 psirt@adobe.com
adobe -- illustrator	Illustrator versions 28.5, 27.9.4 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.	2024-08-14	5.5	CVE-2024-34135 psirt@adobe.com
adobe -- illustrator	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	5.5	CVE-2024-34136 psirt@adobe.com
adobe -- illustrator	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS) condition. An attacker could exploit this vulnerability to crash the application, resulting in a DoS. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	5.5	CVE-2024-34137 psirt@adobe.com
adobe -- illustrator	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	5.5	CVE-2024-34138 psirt@adobe.com
adobe -- substance_3d_sampler	Substance3D - Sampler versions 4.5 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.	2024-08-14	5.5	CVE-2024-41860 psirt@adobe.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- substance_3d_sampler	Substance3D - Sampler versions 4.5 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.	2024-08-14	5.5	CVE-2024-41861 psirt@adobe.com
adobe -- substance_3d_sampler	Substance3D - Sampler versions 4.5 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.	2024-08-14	5.5	CVE-2024-41862 psirt@adobe.com
adobe -- substance_3d_sampler	Substance3D - Sampler versions 4.5 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.	2024-08-14	5.5	CVE-2024-41863 psirt@adobe.com
Adobe--Bridge	Bridge versions 13.0.8, 14.1.1 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.	2024-08-14	5.5	CVE-2024-39387 psirt@adobe.com
Adobe--Dimension	Dimension versions 3.4.11 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.	2024-08-14	5.5	CVE-2024-20790 psirt@adobe.com
Adobe--Dimension	Dimension versions 3.4.11 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.	2024-08-14	5.5	CVE-2024-34125 psirt@adobe.com
Adobe--Dimension	Dimension versions 3.4.11 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.	2024-08-14	5.5	CVE-2024-34126 psirt@adobe.com
Adobe--InDesign Desktop	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a DoS condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	5.5	CVE-2024-39395 psirt@adobe.com
Adobe--InDesign Desktop	InDesign Desktop versions ID19.4, ID18.5.2 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.	2024-08-14	5.5	CVE-2024-41854 psirt@adobe.com
Adobe--InDesign Desktop	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-14	5.5	CVE-2024-41866 psirt@adobe.com
aio-libs--aiohttp	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.10.2, static routes which contain files with compressed variants (`.gz` or `.br` extension) are vulnerable to path traversal outside the root directory if those variants are symbolic links. The server protects static routes from path traversal outside the root directory when `follow_symlinks=False` (default). It does this by resolving the requested URL to an absolute path and then checking that path relative to the root. However, these checks are not performed when looking for compressed variants in the `FileResponse` class, and symbolic links are then	2024-08-12	4.8	CVE-2024-42367 security-advisories@github.com security-advisories@github.com security-advisories@github.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	automatically followed when performing the `Path.stat()` and `Path.open()` to send the file. Version 3.10.2 contains a patch for the issue.			com security-advisories@github.com security-advisories@github.com
airveda -- pm2.5_pm10_monitor_firmware	This vulnerability exists in Airveda Air Quality Monitor PM2.5 PM10 due to transmission of sensitive information in plain text during AP pairing mode. An attacker in close proximity could exploit this vulnerability by capturing Wi-Fi traffic of Airveda-AP. Successful exploitation of this vulnerability could allow the attacker to cause Evil Twin attack on the targeted system.	2024-08-12	6.5	CVE-2024-7408 vdisclose@cert-in.org.in
algoritmika--Download Plugins and Themes in ZIP from Dashboard	The Download Plugins and Themes in ZIP from Dashboard plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.8.7. This is due to missing or incorrect nonce validation on the download_theme() function. This makes it possible for unauthenticated attackers to download arbitrary themes from the website via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. In versions prior to 1.8.6 it was possible to download the entire sites files.	2024-08-16	4.2	CVE-2024-7501 security@wordfence.com security@wordfence.com
AMD--AMD EPYC 7001 Processors	Lack of stack protection exploit mechanisms in ASP Secure OS Trusted Execution Environment (TEE) may allow a privileged attacker with access to AMD signing keys to c006Frrupt the return address, causing a stack-based buffer overrun, potentiallyÂ leading to a denial of service.	2024-08-13	5.2	CVE-2021-46746 psirt@amd.com
AMD--AMD EPYC 7001 Series Processors	Improper key usage control in AMD Secure Processor (ASP) may allow an attacker with local access who has gained arbitrary code execution privilege in ASPÂ to extract ASP cryptographic keys, potentially resulting in loss of confidentiality and integrity.	2024-08-13	5.7	CVE-2024-21981 psirt@amd.com
AMD--AMD EPYC 7003 Processors	IOMMU improperly handles certain special address ranges with invalid device table entries (DTEs), which may allow an attacker with privileges and a compromised Hypervisor to induce DTE faults to bypass RMP checks in SEV-SNP, potentially leading to a loss of guest integrity.	2024-08-13	5.3	CVE-2023-20584 psirt@amd.com
AMD--AMD EPYC 7003 Processors	Incomplete system memory cleanup in SEV firmware could allow a privileged attacker to corrupt guest private memory, potentially resulting in a loss of data integrity.	2024-08-13	4.4	CVE-2023-31356 psirt@amd.com
AMD--AMD EPYC 7003 Series Processors	Improper re-initialization of IOMMU during the DRTM event may permit an untrusted platform configuration to persist, allowing an attacker to read or modify hypervisor memory, potentially resulting in loss of confidentiality, integrity, and availability.	2024-08-13	6.5	CVE-2023-20591 psirt@amd.com
AMD--AMD Radeon RX 6000 Series Graphics Cards	An insufficient DRAM address validation in PMFW may allow a privileged attacker to perform a DMA read from an invalid DRAM address to SRAM, potentially resulting in loss of data integrity.	2024-08-13	5.2	CVE-2023-20509 psirt@amd.com
AMD--AMD Radeon RX 6000 Series Graphics Cards	Improper input validation in Power Management Firmware (PMFW) may allow an attacker with privileges to send a malformed input for the "set temperature input selection" command, potentially resulting in a loss of integrity and/or availability.	2024-08-13	5	CVE-2023-31310 psirt@amd.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
AMD--AMD Radeon RX 6000 Series Graphics Cards	An insufficient DRAM address validation in PMFW may allow a privileged attacker to read from an invalid DRAM address to SRAM, potentially resulting in data corruption or denial of service.	2024-08-13	4.7	CVE-2023-20510 psirt@amd.com
AMD--AMD Ryzen 5000 Series Desktop Processor with Radeon Graphics	A malicious attacker in x86 can misconfigure the Trusted Memory Regions (TMRs), which may allow the attacker to set an arbitrary address range for the TMR, potentially leading to a loss of integrity and availability.	2024-08-13	5.7	CVE-2021-26367 psirt@amd.com psirt@amd.com
AMD--Zynq UltraScale+ MPSoC/RFSoC	Improper input validation in ARMÂ® Trusted Firmware used in AMD's Zynqâ„¢ UltraScale+â„¢) MPSoC/RFSoC may allow a privileged attacker to perform out of bound reads, potentially resulting in data leakage and denial of service.	2024-08-13	4.8	CVE-2023-31339 psirt@amd.com
Antoine Hurkmans--Football Pool	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Antoine Hurkmans Football Pool allows Stored XSS.This issue affects Football Pool: from n/a through 2.11.9.	2024-08-12	6.5	CVE-2024-43139 audit@patchstack.com
Antoine Hurkmans--Football Pool	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Antoine Hurkmans Football Pool allows Stored XSS.This issue affects Football Pool: from n/a through 2.11.10.	2024-08-12	5.9	CVE-2024-43130 audit@patchstack.com
Averta--Depicter Slider	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Averta Depicter Slider allows Stored XSS.This issue affects Depicter Slider: from n/a through 3.1.2.	2024-08-12	5.9	CVE-2024-43161 audit@patchstack.com
AxtonYao--MDx	The MDx theme for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'mdx_list_item' shortcode in all versions up to, and including, 2.0.3 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.	2024-08-12	6.4	CVE-2024-6639 security@wordfence.com security@wordfence.com security@wordfence.com
basecamp--trix	The Trix editor, versions prior to 2.1.4, is vulnerable to XSS when pasting malicious code. This vulnerability is a bypass of the fix put in place for GHSA-qjqp-xr96-cj99. In pull request 1149, sanitation was added for Trix attachments with a `text/html` content type. However, Trix only checks the content type on the paste event's `dataTransfer` object. As long as the `dataTransfer` has a content type of `text/html`, Trix parses its contents and creates an `Attachment` with them, even if the attachment itself doesn't have a `text/html` content type. Trix then uses the attachment content to set the attachment element's `innerHTML`. An attacker could trick a user to copy and paste malicious code that would execute arbitrary JavaScript code within the context of the user's session, potentially leading to unauthorized actions being performed or sensitive information being disclosed. This vulnerability was fixed in version 2.1.4.	2024-08-14	6.5	CVE-2024-43368 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				com
bdthemes--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) plugin for WordPress is vulnerable to arbitrary file reads in all versions up to, and including, 5.7.2 via the SVG widget and a lack of sufficient file validation in the render_svg function. 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.	2024-08-12	6.5	CVE-2024-4359 security@wordfence.com security@wordfence.com
bdthemes--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) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 5.7.2 due to insufficient input sanitization and output escaping on user supplied attributes like 'title_tag'. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-12	6.4	CVE-2024-4360 security@wordfence.com security@wordfence.com
bdthemes--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) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Custom Gallery and Countdown widgets in all versions up to, and including, 5.7.2 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.	2024-08-13	6.4	CVE-2024-7247 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
binhnguyenplus--LadiApp: Landing Page, PopupX, Marketing Automation, Affiliate Marketing	The LadiApp plugn for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the init_endpoint() function hooked via 'init' in versions up to, and including, 4.3. This makes it possible for unauthenticated attackers to modify a variety of settings. An attacker can directly modify the 'ladipage_key' which enables them to create new posts on the website and inject malicious web scripts.	2024-08-17	5.3	CVE-2023-4730 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
Blockspare--Blockspare	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Blockspare allows Stored XSS.This issue affects Blockspare: from n/a through 3.2.0.	2024-08-12	6.5	CVE-2024-43164 audit@patchstack.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bPlugins--StreamCast	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in bPlugins StreamCast allows Stored XSS.This issue affects StreamCast: from n/a through 2.2.3.	2024-08-12	5.9	CVE-2024-43148 audit@patchstack.com
Brainstorm Force--Spectra	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brainstorm Force Spectra allows Stored XSS.This issue affects Spectra: from n/a through 2.14.1.	2024-08-12	6.5	CVE-2024-7590 audit@patchstack.com
Brainstorm Force--Ultimate Addons for Beaver Builder Lite	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brainstorm Force Ultimate Addons for Beaver Builder - Lite allows Stored XSS.This issue affects Ultimate Addons for Beaver Builder - Lite: from n/a through 1.5.9.	2024-08-12	6.5	CVE-2024-43151 audit@patchstack.com
Bricks Builder--Bricks	The Bricks theme for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.8.1. This is due to missing or incorrect nonce validation on the 'reset_settings' function. This makes it possible for unauthenticated attackers to reset the theme's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-08-17	5.4	CVE-2023-3409 security@wordfence.com security@wordfence.com
Bricks Builder--Bricks	The Bricks theme for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.8.1. This is due to missing or incorrect nonce validation on the 'save_settings' function. This makes it possible for unauthenticated attackers to modify the theme's settings, including enabling a setting which allows lower-privileged users such as contributors to perform code execution, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-08-17	4.3	CVE-2023-3408 security@wordfence.com security@wordfence.com
cilium--cilium	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.14.14 and 1.15.8, a race condition in the Cilium agent can cause the agent to ignore labels that should be applied to a node. This could in turn cause CiliumClusterwideNetworkPolicies intended for nodes with the ignored label to not apply, leading to policy bypass. This issue has been patched in Cilium v1.14.14 and v1.15.8 As the underlying issue depends on a race condition, users unable to upgrade can restart the Cilium agent on affected nodes until the affected policies are confirmed to be working as expected.	2024-08-15	6.8	CVE-2024-42488 security-advisories@github.com security-advisories@github.com security-advisories@github.com
cilium--cilium	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. In versions on the 1.15.x branch prior to 1.15.8 and the 1.16.x branch prior to 1.16.1, ReferenceGrant changes are not correctly propagated in Cilium's GatewayAPI controller, which could lead to Gateway resources being able to access secrets for longer than intended, or to Routes having the ability to forward traffic to backends in other namespaces for longer than intended. This issue has been patched in Cilium v1.15.8 and v1.16.1. As a workaround, any modification of a related Gateway/HTTPRoute/GRPCRoute/TCPRoute CRD (for example, adding any label to any of these resources) will trigger a reconciliation of ReferenceGrants on an affected cluster.	2024-08-16	5.4	CVE-2024-42486 security-advisories@github.com security-advisories@github.com security-advisories@github.com
cilium--cilium	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. In the 1.15 branch prior to 1.15.8 and the 1.16 branch prior to 1.16.1, Gateway API HTTPRoutes and GRPCRoutes do not follow the match precedence specified in the Gateway API specification. In particular, request headers are matched before request methods, when the specification describes that the request methods must be respected before headers are matched. This could result	2024-08-15	4	CVE-2024-42487 security-advisories@github.com security-advisories@github.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in unexpected behaviour with security This issue is fixed in Cilium v1.15.8 and v1.16.1. There is no workaround for this issue.			com security-advisories@github.com
codersaiful--Sheet to Table Live Sync for Google Sheet	The Sheet to Table Live Sync for Google Sheet plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's STWT_Sheet_Table 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.	2024-08-14	6.4	CVE-2024-6532 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
coffee2code--Linkify Text	The Linkify Text plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.9.1. This is due to the plugin utilizing bootstrap and leaving test files with display_errors on. This makes it possible for unauthenticated attackers 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.	2024-08-12	5.3	CVE-2024-7382 security@wordfence.com security@wordfence.com
coffee2code--No Update Nag	The No Update Nag plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.4.12. This is due to the plugin allowing direct access to the bootstrap.php file which has display_errors on. This makes it possible for unauthenticated attackers 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.	2024-08-12	5.3	CVE-2024-7412 security@wordfence.com security@wordfence.com
coffee2code--Obfuscate Email	The Obfuscate Email plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.8.1. This is due to the plugin allowing direct access to the bootstrap.php file which has display_errors on. This makes it possible for unauthenticated attackers 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.	2024-08-12	5.3	CVE-2024-7413 security@wordfence.com security@wordfence.com
coffee2code--Reveal Template	The Reveal Template plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.7. This is due to the plugin allowing direct access to the bootstrap.php file which has display_errors on. This makes it possible for unauthenticated attackers 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.	2024-08-12	5.3	CVE-2024-7416 security@wordfence.com security@wordfence.com
contrid--Newsletters	The Newsletters plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 4.9.9. This is due the plugin not preventing direct access to the /vendor/mobiledetect/mobiledetectlib/export/exportToJSON.php. This makes it possible for unauthenticated attackers 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.	2024-08-15	5.3	CVE-2024-7411 security@wordfence.com security@wordfence.com security@wordfence.com
CORDEA--oauth	In the OAuth library for nim prior to version 0.11, the `state` values generated by the `generateState` function do not have sufficient entropy. These can be successfully guessed by an attacker allowing them to perform a CSRF vs a user, associating the user's session with the attacker's protected resources. While `state`	2024-08-15	6.5	CVE-2024-42475 security-advisories@github.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	isn't exactly a cryptographic value, it should be generated in a cryptographically secure way. `generateState` should be using a CSPRNG. Version 0.11 modifies the `generateState` function to generate `state` values of at least 128 bits of entropy while using a CSPRNG.			security-advisories@github.com
CORDEA--oauth	In the OAuth library for nim prior to version 0.11, the Authorization Code grant and Implicit grant both rely on the `state` parameter to prevent cross-site request forgery (CSRF) attacks where a resource owner might have their session associated with protected resources belonging to an attacker. When this project is compiled with certain compiler flags set, it is possible that the `state` parameter will not be checked at all, creating a CSRF vulnerability. Version 0.11 checks the `state` parameter using a regular `if` statement or `doAssert` instead of relying on a plain `assert`. `doAssert` will achieve the desired behavior even if `-d:danger` or `--assertions:off` is set.	2024-08-15	6.5	CVE-2024-42476 security-advisories@github.com security-advisories@github.com security-advisories@github.com
CreativeMindsSolutions--CM Tooltip Glossary	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CreativeMindsSolutions CM Tooltip Glossary allows Stored XSS.This issue affects CM Tooltip Glossary: from n/a through 4.3.7.	2024-08-12	6.5	CVE-2024-43149 audit@patchstack.com
Crocoblock--JetBlocks for Elementor	The JetBlocks for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple placeholder parameters in all versions up to, and including, 1.3.12 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.	2024-08-16	6.4	CVE-2024-7147 security@wordfence.com security@wordfence.com
Crocoblock--JetElements	The JetElements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' and 'slide_id' parameters in all versions up to, and including, 2.6.20 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.	2024-08-16	6.4	CVE-2024-7144 security@wordfence.com security@wordfence.com
Crocoblock--JetSearch	The JetSearch plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 3.5.2 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.	2024-08-16	6.4	CVE-2024-7136 security@wordfence.com security@wordfence.com
cservit--affiliate-toolkit WordPress Affiliate Plugin	The affiliate-toolkit - WordPress Affiliate Plugin plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.5.5. This is due display_errors being set to true . This makes it possible for unauthenticated attackers 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.	2024-08-12	5.3	CVE-2024-6562 security@wordfence.com security@wordfence.com
cyberfoxdigital--Christmasify!	The Christmasify! plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.5.5. This is due to missing nonce validation on the 'options' function. This makes it possible for unauthenticated attackers to modify the plugin's 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.	2024-08-12	6.1	CVE-2024-7574 security@wordfence.com security@wordfence.com
D-Link--DI-8100	A vulnerability was found in D-Link DI-8100 16.07. It has been classified as critical. This affects the function upgrade_filter_asp of the file upgrade_filter.asp. The manipulation of the argument path leads to command injection. It is possible to	2024-08-15	6.3	CVE-2024-7833 cna@vuldb.com cna@vuldb.com cna@vuldb.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	initiate the attack remotely. The exploit has been disclosed to the public and may be used.			cna@vuldb.com
David Maucher--Send Users Email	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in David Maucher Send Users Email allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Send Users Email: from n/a through 1.5.1.	2024-08-13	5.3	CVE-2024-38760 audit@patchstack.com
Dell--Dell Client Platform BIOS	Dell BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2024-08-14	5.8	CVE-2024-38483 security_alert@emc.com
Devikia--DevikaAI	A stored cross site scripting vulnerabilities exists in DevikaAI from commitÂ 6acce21fb08c3d1123ef05df6a33912bf0ee77c2 onwards via improperly decoded user input.	2024-08-14	6.5	CVE-2024-7790 vulnreport@tenable.com
Directus--Directus	Directus v10.13.0 allows an authenticated external attacker to execute arbitrary JavaScript on the client. This is possible because the application injects an attacker-controlled parameter that will be stored in the server and used by the client into an unsanitized DOM element. When chained with CVE-2024-6534, it could result in account takeover.	2024-08-15	4.1	CVE-2024-6533 help@fluidattacks.com help@fluidattacks.com
Directus--Directus	Directus v10.13.0 allows an authenticated external attacker to modify presets created by the same user to assign them to another user. This is possible because the application only validates the user parameter in the 'POST /presets'Â request but not in the PATCH request. When chained with CVE-2024-6533, it could result in account takeover.	2024-08-15	4.1	CVE-2024-6534 help@fluidattacks.com help@fluidattacks.com
edgarrojas--PDF Builder for WPForms	The PDF Builder for WPForms plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.2.116. This is due to the plugin allowing direct access to the composer-setup.php file which has display_errors on. This makes it possible for unauthenticated attackers 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.	2024-08-12	5.3	CVE-2024-7414 security@wordfence.com security@wordfence.com security@wordfence.com
elabftw--elabftw	eLabFTW is an open source electronic lab notebook for research labs. In an eLabFTW system, one might disallow user creation except for by system administrators, administrators and trusted services. If administrators are allowed to create new users (which is the default), the vulnerability allows any user to create new users in teams where they are members. The new users are automatically validated and administrators are not notified. This can allow a user with permanent or temporary access to a user account or API key to maintain persistence in an eLabFTW system. Additionally, it allows the user to create separate account under a different name, and produce misleading revision histories. No additional privileges are granted to the new user. Users should upgrade to version 5.0.0 to receive a patch. As a workaround, disabling both options that allow *administrators* to create users will provide a mitigation.	2024-08-15	5.4	CVE-2024-25633 security-advisories@github.com
Ericsson--Ericsson RAN Compute Basebands (all BB variants)	Ericsson RAN Compute and Site Controller 6610 contains a vulnerability in the Control System where Improper Input Validation can lead to arbitrary code execution, for example to obtain a Linux Shell with the same privileges as the attacker. The attacker would require elevated privileges for example a valid OAM user having the system administrator role to exploit the vulnerability.	2024-08-16	6.8	CVE-2024-25008 85b1779b-6ecd-4f52-bcc5-73eac4659dcf
esthertyler--My Custom CSS PHP &	The My Custom CSS PHP & ADS plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.3. This is due the plugin not	2024-08-12	5.3	CVE-2024-7410 security@wordfenc

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ADS	preventing direct access to the /my-custom-css/vendor/mobiledetect/mobiledetectlib/export/exportToJSON.php file and and the file displaying/generating the full path. This makes it possible for unauthenticated attackers 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.			e.com security@wordfence.com
f1logic--Insert PHP Code Snippet	The Insert PHP Code Snippet plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.6. This is due to missing or incorrect nonce validation in the /admin/snippets.php file. This makes it possible for unauthenticated attackers to activate/deactivate and delete code snippets via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-08-15	5.8	CVE-2024-7420 security@wordfence.com security@wordfence.com security@wordfence.com
F5--BIG-IP Next Central Manager	BIG-IP Next Central Manager may allow an attacker to lock out an account that has never been logged in.Â Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	5.3	CVE-2024-37028 f5sirt@f5.com
F5--BIG-IP Next Central Manager	When generating QKView of BIG-IP Next instance from the BIG-IP Next Central Manager (CM), F5 iHealth credentials will be logged in the BIG-IP Central Manager logs.Â Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	4.2	CVE-2024-41719 f5sirt@f5.com
F5--BIG-IP	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	5.9	CVE-2024-41164 f5sirt@f5.com
F5--BIG-IP	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names.Â Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	4.3	CVE-2024-41723 f5sirt@f5.com
F5--NGINX Open Source	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_http_mp4_module, which might allow an attacker to over-read NGINX worker memory resulting in its termination, using a specially crafted mp4 file. The issue only affects NGINX if it is built with the ngx_http_mp4_module and the mp4 directive is used in the configuration file. Additionally, the attack is possible only if an attacker can trigger the processing of a specially crafted mp4 file with the ngx_http_mp4_module.Â Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2024-08-14	4.7	CVE-2024-7347 f5sirt@f5.com
Firewalla--Box Software	Multiple authenticated operating system (OS) command injection vulnerabilities exist in Firewalla Box Software versions before 1.979. A physically close attacker that is authenticated to the Bluetooth Low-Energy (BTLE) interface can use the network configuration service to inject commands in various configuration parameters includingÂ networkConfig.Interface.Phy.Eth0.Extra.PingTestIP,Â networkConfig.Interface.Phy.Eth0.Extra.DNSTestDomain, andÂ networkConfig.Interface.Phy.Eth0.Gateway6. Additionally, because the configuration can be synced to the Firewalla cloud, the attacker may be able to persist access even after hardware resets and firmware re-flashes.	2024-08-12	6.8	CVE-2024-40893 disclosure@vulncheck.com
fish-shop--syntax-check	fish-shop/syntax-check is a GitHub action for syntax checking fish shell files. Improper neutralization of delimiters in the `pattern` input (specifically the command separator `;` and command substitution characters `(` and `)`) mean that arbitrary command injection is possible by modification of the input value used in a workflow. This has the potential for exposure or exfiltration of sensitive information from the workflow runner, such as might be achieved by sending	2024-08-12	4.8	CVE-2024-42482 security-advisories@github.com security-advisories@github.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	environment variables to an external entity. It is recommended that users update to the patched version `v1.6.12` or the latest release version `v2.0.0`, however remediation may be possible through careful control of workflows and the `pattern` input value used by this action.			com security-advisories@github.com
FIWARE--FIWARE Keyrock	Insufficiently random values for generating activation token in FIWARE Keyrock <= 8.4 allow attackers to activate accounts of any user by predicting the token for the activation link.	2024-08-12	6.3	CVE-2024-42165 office@cyberdanube.com
FIWARE--FIWARE Keyrock	Insufficiently random values for generating password reset token in FIWARE Keyrock <= 8.4 allow attackers to disable two factor authorization of any user by predicting the token for the disable_2fa link.	2024-08-12	4.3	CVE-2024-42164 office@cyberdanube.com
Fortinet--FortiDDoS	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiDDoS version 5.5.0 through 5.5.1, 5.4.2 through 5.4.0, 5.3.0 through 5.3.1, 5.2.0, 5.1.0, 5.0.0, 4.7.0, 4.6.0 and 4.5.0 and FortiDDoS-F version 6.3.0 through 6.3.1, 6.2.0 through 6.2.2, 6.1.0 through 6.1.4 allows an authenticated attacker to execute shell code as `root`Â via `execute` CLI commands.	2024-08-13	6.6	CVE-2022-27486 psirt@fortinet.com
Fortinet--FortiManager	A unverified password change in Fortinet FortiManager versions 7.0.0 through 7.0.10, versions 7.2.0 through 7.2.4, and versions 7.4.0 through 7.4.1, as well as Fortinet FortiAnalyzer versions 7.0.0 through 7.0.10, versions 7.2.0 through 7.2.4, and versions 7.4.0 through 7.4.1, allows an attacker to modify admin passwords via the device configuration backup.	2024-08-13	6.1	CVE-2024-21757 psirt@fortinet.com
Fortinet--FortiOS	An improper access control vulnerability [CWE-284] in FortiOS 7.4.0 through 7.4.3, 7.2.5 through 7.2.7, 7.0.12 through 7.0.14 and 6.4.x may allow an attacker who has already successfully obtained write access to the underlying system (via another hypothetical exploit) to bypass the file integrity checking system.	2024-08-13	5.1	CVE-2024-36505 psirt@fortinet.com
Fortinet--FortiSOAR	An improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSOAR 7.3.0 through 7.3.2 allows an authenticated, remote attacker to inject arbitrary web script or HTML via the Communications module.	2024-08-13	6.8	CVE-2023-26211 psirt@fortinet.com
Fortra--GoAnywhere MFT	An authentication bypass vulnerability in GoAnywhere MFT prior to 7.6.0 allows Admin Users with access to the Agent Console to circumvent some permission checks when attempting to visit other pages. This could lead to unauthorized information disclosure or modification.	2024-08-14	6.5	CVE-2024-25157 df4dee71-de3a-4139-9588-11b62fe6c0ff
freebsd -- freebsd	When mounting a remote filesystem using NFS, the kernel did not sanitize remotely provided filenames for the path separator character, "/". This allows readdir(3) and related functions to return filesystem entries with names containing additional path components. The lack of validation described above gives rise to a confused deputy problem. For example, a program copying files from an NFS mount could be tricked into copying from outside the intended source directory, and/or to a location outside the intended destination directory.	2024-08-12	5.3	CVE-2024-6759 secteam@freebsd.org
Fujian--mwcms	A vulnerability was found in Fujian mwcms 1.0.0. It has been declared as critical. Affected by this vulnerability is the function uploadeditor of the file /uploadeditor.html?action=uploadimage of the component Image Upload. The manipulation of the argument upfile leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-12	4.7	CVE-2024-7705 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Fujian--mwcms	A vulnerability was found in Fujian mwcms 1.0.0. It has been rated as critical. Affected by this issue is the function uploadimage of the file /uploadfile.html. The manipulation of the argument upfile leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-12	4.7	CVE-2024-7706 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
gfazioli--WP Bannerize Pro	The WP Bannerize Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via banner alt data 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 editor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-08-13	4	CVE-2024-7388 security@wordfence.com security@wordfence.com
gilacms -- gila_cms	A vulnerability classified as problematic was found in Gila CMS 1.10.9. This vulnerability affects unknown code of the file /cm/update_rows/page?id=2 of the component HTTP POST Request Handler. The manipulation of the argument content leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-12	5.4	CVE-2024-7657 cna@vuldb.com cna@vuldb.com cna@vuldb.com
gncchome -- gncc_c2_firmware	Identical Hardcoded Root Password for All Devices in GNCC's GC2 Indoor Security Camera 1080P allows an attacker with physical access to retrieve the root password for all similar devices	2024-08-15	6.8	CVE-2024-31798 cve@mitre.org cve@mitre.org
gncchome -- gncc_c2_firmware	Authentication Bypass in GNCC's GC2 Indoor Security Camera 1080P allows an attacker with physical access to gain a privileged command shell via the UART Debugging Port.	2024-08-15	6.8	CVE-2024-31800 cve@mitre.org cve@mitre.org
gncchome -- gncc_c2_firmware	Information Disclosure in GNCC's GC2 Indoor Security Camera 1080P allows an attacker with physical access to read the WiFi passphrase via the UART Debugging Port.	2024-08-15	4.6	CVE-2024-31799 cve@mitre.org cve@mitre.org
gravitymaster97--Custom Field For WP Job Manager	The Custom Field For WP Job Manager plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.2 via the the 'cm_fieldshow' shortcode due to missing validation on the 'job_id' user controlled key. This makes it possible for authenticated attackers, with contributor-level access and above, to expose potentially sensitive post metadata.	2024-08-16	4.3	CVE-2023-7049 security@wordfence.com security@wordfence.com
HashiCorp--Nomad	In HashiCorp Nomad and Nomad Enterprise from 0.6.1 up to 1.16.13, 1.7.10, and 1.8.2, the archive unpacking process is vulnerable to writes outside the allocation directory during migration of allocation directories when multiple archive headers target the same file. This vulnerability, CVE-2024-7625, is fixed in Nomad 1.6.14, 1.7.11, and 1.8.3. Access or compromise of the Nomad client agent at the source allocation first is a prerequisite for leveraging this vulnerability.	2024-08-15	5.8	CVE-2024-7625 security@hashicorp.com
humanityco--Cookie Notice & Compliance for GDPR / CCPA	The Cookie Notice & Compliance for GDPR / CCPA plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cookie_notice_options[refuse_code_head]' parameter in versions up to, and including, 2.4.17.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrative privileges and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the injected /wp-admin/admin.php?page=cookie-notice page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2024-08-16	4.4	CVE-2022-3399 security@wordfence.com security@wordfence.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
iberezansky--3D FlipBook PDF Flipbook Viewer, Flipbook Image Gallery	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in iberezansky 3D FlipBook - PDF Flipbook Viewer, Flipbook Image Gallery allows Stored XSS.This issue affects 3D FlipBook - PDF Flipbook Viewer, Flipbook Image Gallery: from n/a through 1.15.6.	2024-08-12	5.9	CVE-2024-43152 audit@patchstack.com
ibm -- infosphere_information_server	IBM InfoSphere Information Server could allow an authenticated user to consume file space resources due to unrestricted file uploads. IBM X-Force ID: 298279.	2024-08-15	6.5	CVE-2024-40705 psirt@us.ibm.com psirt@us.ibm.com
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 could allow a privileged user to obtain sensitive information from authentication request headers. IBM X-Force ID: 298277.	2024-08-15	4.9	CVE-2024-40704 psirt@us.ibm.com psirt@us.ibm.com
IBM--Aspera Shares	IBM Aspera Shares 1.10.0 PL2 does not invalidate session after a password change which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 260574.	2024-08-12	6.3	CVE-2023-38018 psirt@us.ibm.com
IBM--Common Licensing	IBM Common Licensing 9.0 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 350348.	2024-08-13	5.5	CVE-2024-41774 psirt@us.ibm.com psirt@us.ibm.com
IBM--Db2 for Linux, UNIX and Windows	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 could allow an authenticated user to cause a denial of service with a specially crafted query due to improper memory allocation. IBM X-Force ID: 292639.	2024-08-14	6.5	CVE-2024-35152 psirt@us.ibm.com psirt@us.ibm.com
IBM--Db2 for Linux, UNIX and Windows	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 could allow an authenticated user to cause a denial of service with a specially crafted query due to improper memory allocation. IBM X-Force ID: 294295.	2024-08-14	6.5	CVE-2024-37529 psirt@us.ibm.com psirt@us.ibm.com
IBM--Db2 for Linux, UNIX and Windows	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to a denial of service, under specific configurations, as the server may crash when using a specially crafted SQL statement by an authenticated user. IBM X-Force ID: 287614.	2024-08-14	5.3	CVE-2024-31882 psirt@us.ibm.com psirt@us.ibm.com
IBM--Db2 for Linux, UNIX and Windows	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) federated server 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query under certain conditions. IBM X-Force ID: 291307.	2024-08-14	5.3	CVE-2024-35136 psirt@us.ibm.com psirt@us.ibm.com
IBM--QRadar Network Packet Capture	IBM QRadar Network Packet Capture 7.5 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 289858.	2024-08-15	5.9	CVE-2024-31905 psirt@us.ibm.com psirt@us.ibm.com
IBM--QRadar Suite Software	IBM QRadar Suite Software 1.10.12.0 through 1.10.23.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 281430.	2024-08-15	6.2	CVE-2024-25024 psirt@us.ibm.com psirt@us.ibm.com
IBM--QRadar Suite Software	IBM QRadar Suite Software 1.10.12.0 through 1.10.23.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 displays sensitive data improperly during back-end commands which may result in the unexpected disclosure of this information. IBM X-Force ID: 287173.	2024-08-14	5.6	CVE-2024-28799 psirt@us.ibm.com psirt@us.ibm.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--QRadar Suite Software	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.11.0 and IBM QRadar Suite Software 1.10.12.0 through 1.10.23.0 does not invalidate session after logout which could allow another user to obtain sensitive information. IBM X-Force ID: 233672.	2024-08-13	4.7	CVE-2022-38382 psirt@us.ibm.com psirt@us.ibm.com
IBM--QRadar Suite Software	IBM QRadar Suite Software 1.10.12.0 through 1.10.22.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the request. This information could be used in further attacks against the system. IBM X-Force ID: 272201.	2024-08-16	4.9	CVE-2023-47728 psirt@us.ibm.com psirt@us.ibm.com
IBM--SDK, Java Technology Edition	The Object Request Broker (ORB) in IBM SDK, Java Technology Edition 7.1.0.0 through 7.1.5.18 and 8.0.0.0 through 8.0.8.26 is vulnerable to remote denial of service, caused by a race condition in the management of ORB listener threads. IBM X-Force ID: 284573.	2024-08-14	5.9	CVE-2024-27267 psirt@us.ibm.com psirt@us.ibm.com
IBM--WebSphere Application Liberty	IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.8 could allow an attacker with access to the network to conduct spoofing attacks. An attacker could exploit this vulnerability using a certificate issued by a trusted authority to obtain sensitive information. IBM X-Force ID: 274713.	2024-08-14	5.3	CVE-2023-50314 psirt@us.ibm.com psirt@us.ibm.com
IBM--WebSphere Application Server	IBM WebSphere Application Server 8.5 and 9.0 could allow an attacker with access to the network to conduct spoofing attacks. An attacker could exploit this vulnerability using a certificate issued by a trusted authority to obtain sensitive information. IBM X-Force ID: 274714.	2024-08-14	5.3	CVE-2023-50315 psirt@us.ibm.com psirt@us.ibm.com
Igor Beni--Recipe Maker For Your Food Blog from Zip Recipes	Missing Authorization vulnerability in Igor BeniÄ‡ Recipe Maker For Your Food Blog from Zip Recipes allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Recipe Maker For Your Food Blog from Zip Recipes: from n/a through 8.2.6.	2024-08-13	5.3	CVE-2024-38688 audit@patchstack.com
Iqonic Design--Graphina	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Iqonic Design Graphina allows Stored XSS.This issue affects Graphina: from n/a through 1.8.10.	2024-08-12	6.5	CVE-2024-43124 audit@patchstack.com
itsourcecode--Vehicle Management System	A vulnerability was found in itsourcecode Vehicle Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file mybill.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-14	6.3	CVE-2024-7794 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Jeroen Sormani--WP Dashboard Notes	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jeroen Sormani WP Dashboard Notes allows Stored XSS.This issue affects WP Dashboard Notes: from n/a through 1.0.11.	2024-08-12	6.5	CVE-2024-43226 audit@patchstack.com
JetBrains--TeamCity	In JetBrains TeamCity before 2024.07.1 multiple stored XSS was possible on Clouds page	2024-08-16	4.6	CVE-2024-43807 cve@jetbrains.com
JetBrains--TeamCity	In JetBrains TeamCity before 2024.07.1 reflected XSS was possible in the AWS Core plugin	2024-08-16	4.6	CVE-2024-43810 cve@jetbrains.com
jfarthing84--Theme My Login	The Theme My Login plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 7.1.7. This is due to missing or incorrect nonce validation on the tml_admin_save_ms_settings() function. This makes it possible for unauthenticated attackers to update the theme's settings via a forged	2024-08-16	4.3	CVE-2024-7422 security@wordfence.com security@wordfenc

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	request granted they can trick a site administrator into performing an action such as clicking on a link. Please note that this only affects multi-site instances.			e.com
kaizencoders--Short URL	The Short URL plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.6.8. This is due to missing or incorrect nonce validation on the configuration_page function. This makes it possible for unauthenticated attackers to add and import redirects, including comments containing cross-site scripting as detailed in CVE-2023-1602, granted they can trick a site administrator into performing an action such as clicking on a link.	2024-08-17	4.7	CVE-2023-1604 security@wordfence.com security@wordfence.com
krut1--LOGIN AND REGISTRATION ATTEMPTS LIMIT	The LOGIN AND REGISTRATION ATTEMPTS LIMIT plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 2.1. This is due to insufficient restrictions on where the IP Address information is being retrieved for request logging and login restrictions. Attackers can supply the X-Forwarded-For header with with a different IP Address that will be logged and can be used to bypass settings that may have blocked out an IP address from logging in.	2024-08-17	6.5	CVE-2022-4532 security@wordfence.com security@wordfence.com
LA-Studio--LA-Studio Element Kit for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LA-Studio LA-Studio Element Kit for Elementor allows Stored XSS.This issue affects LA-Studio Element Kit for Elementor: from n/a through 1.3.9.2.	2024-08-12	6.5	CVE-2024-43210 audit@patchstack.com
Lenovo--Printers	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to crash printer communications until the system is rebooted.	2024-08-16	6.5	CVE-2024-4781 psirt@lenovo.com
Lenovo--Printers	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to disrupt the printer's functionality until a manual system reboot occurs.	2024-08-16	6.5	CVE-2024-4782 psirt@lenovo.com
Lenovo--Printers	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to deny printing capabilities until the system is rebooted.	2024-08-16	6.5	CVE-2024-5209 psirt@lenovo.com
Lenovo--Printers	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to prevent printer services from being reachable until the system is rebooted.	2024-08-16	6.5	CVE-2024-5210 psirt@lenovo.com
Lenovo--Printers	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to deny printer connections until the system is rebooted.	2024-08-16	6.5	CVE-2024-6004 psirt@lenovo.com
linux -- linux_kernel	In the Linux kernel, the following vulnerability has been resolved: mm: huge_memory: use !CONFIG_64BIT to relax huge page alignment on 32 bit machines Yves-Alexis Perez reported commit 4ef9ad19e176 ("mm: huge_memory: don't force huge page alignment on 32 bit") didn't work for x86_32 [1]. It is because x86_32 uses CONFIG_X86_32 instead of CONFIG_32BIT. !CONFIG_64BIT should cover all 32 bit machines. [1] https://lore.kernel.org/linux-mm/CAHbLzkr1LwH3pcTgM+aGQ31ip2bKqiqEQ8=FQB+t2c3dhNKNHA@mail.gmail.com/	2024-08-12	5.5	CVE-2024-42258 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67 416baaa9-dc9f-4396-8d5f-8c081fb06d67
MagePeople Team--Event Manager for	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in MagePeople Team Event Manager for WooCommerce allows PHP Local File Inclusion.This issue affects Event Manager for WooCommerce: from n/a through 4.2.1.	2024-08-13	6.5	CVE-2024-43138 audit@patchstack.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WooCommerce				
mayurik -- best_house_rental_management_system	A Stored Cross Site Scripting (XSS) vulnerability was found in "manage_houses.php" in SourceCodester Best House Rental Management System v1.0. It allows remote attackers to execute arbitrary code via "House_no" and "Description" parameter fields.	2024-08-12	5.4	CVE-2024-40473 cve@mitre.org cve@mitre.org
mayurik -- best_house_rental_management_system	A Reflected Cross Site Scripting (XSS) vulnerability was found in "edit-cate.php" in SourceCodester House Rental Management System v1.0.	2024-08-12	5.4	CVE-2024-40474 cve@mitre.org cve@mitre.org
MBE Worldwide S.p.A.--MBE eShip	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in MBE Worldwide S.P.A. MBE eShip allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects MBE eShip: from n/a through 2.1.2.	2024-08-13	5.3	CVE-2024-38742 audit@patchstack.com
Mediavine--Mediavine Control Panel	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mediavine Mediavine Control Panel allows Stored XSS.This issue affects Mediavine Control Panel: from n/a through 2.10.4.	2024-08-12	6.5	CVE-2024-43218 audit@patchstack.com
Merkulove--Selection Lite	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Merkulove Selection Lite allows Stored XSS.This issue affects Selection Lite: from n/a through 1.11.	2024-08-12	6.5	CVE-2024-43147 audit@patchstack.com
microsoft -- .net	.NET and Visual Studio Information Disclosure Vulnerability	2024-08-13	6.5	CVE-2024-38167 secure@microsoft.com
microsoft -- 365_apps	Microsoft Outlook Remote Code Execution Vulnerability	2024-08-13	6.7	CVE-2024-38173 secure@microsoft.com
microsoft -- 365_apps	Microsoft Office Spoofing Vulnerability	2024-08-12	6.5	CVE-2024-38200 secure@microsoft.com
microsoft -- teams	Microsoft Teams for iOS Spoofing Vulnerability	2024-08-13	6.5	CVE-2024-38197 secure@microsoft.com
microsoft -- windows_10_1507	Windows Mark of the Web Security Feature Bypass Vulnerability	2024-08-13	6.5	CVE-2024-38213 secure@microsoft.com
microsoft -- windows_10_1507	Windows Initial Machine Configuration Elevation of Privilege Vulnerability	2024-08-13	6.8	CVE-2024-38223 secure@microsoft.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10_1507	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability	2024-08-13	5.5	CVE-2024-38118 secure@microsoft.com
microsoft -- windows_10_1507	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability	2024-08-13	5.5	CVE-2024-38122 secure@microsoft.com
microsoft -- windows_10_1507	Windows Kernel Information Disclosure Vulnerability	2024-08-13	5.5	CVE-2024-38151 secure@microsoft.com
microsoft -- windows_10_1507	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability	2024-08-13	4.2	CVE-2024-38143 secure@microsoft.com
microsoft -- windows_10_1809	Windows Mobile Broadband Driver Remote Code Execution Vulnerability	2024-08-13	6.8	CVE-2024-38161 secure@microsoft.com
microsoft -- windows_10_1809	Security Center Broker Information Disclosure Vulnerability	2024-08-13	5.5	CVE-2024-38155 secure@microsoft.com
microsoft -- windows_11_22h2	Windows Compressed Folder Tampering Vulnerability	2024-08-13	6.5	CVE-2024-38165 secure@microsoft.com
microsoft -- windows_11_24h2	Windows Bluetooth Driver Information Disclosure Vulnerability	2024-08-13	4.4	CVE-2024-38123 secure@microsoft.com
microsoft -- windows_server_2008	Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability	2024-08-13	6.5	CVE-2024-38214 secure@microsoft.com
Microsoft-- Microsoft Edge (Chromium-based)	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-08-12	6.5	CVE-2024-38219 secure@microsoft.com
Microsoft-- Microsoft Edge (Chromium-based)	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2024-08-16	5.8	CVE-2024-43472 secure@microsoft.com
mongodb -- mongodb	"Hot" backup files may be downloaded by underprivileged users, if they are capable of acquiring a unique backup identifier. This issue affects MongoDB Enterprise Server v6.0 versions prior to 6.0.16, MongoDB Enterprise Server v7.0 versions prior to 7.0.11 and MongoDB Enterprise Server v7.3 versions prior to 7.3.3	2024-08-13	5.3	CVE-2024-6384 cna@mongodb.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
msaari--Relevanssi A Better Search	The Relevanssi - A Better Search plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 4.22.2 via the relevanssi_do_query() due to insufficient limitations on the posts that are returned when searching. This makes it possible for unauthenticated attackers to extract potentially sensitive information from password protected posts.	2024-08-16	5.3	CVE-2024-7630 security@wordfence.com security@wordfence.com
n/a--3rd Generation Intel(R) Xeon(R) Scalable Processors	Mirrored regions with different values in 3rd Generation Intel(R) Xeon(R) Scalable Processors may allow a privileged user to potentially enable denial of service via local access.	2024-08-14	6	CVE-2024-25939 secure@intel.com
n/a--3rd, 4th, and 5th Generation Intel(R) Xeon(R) Processors	Protection mechanism failure in some 3rd, 4th, and 5th Generation Intel(R) Xeon(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	2024-08-14	6.1	CVE-2024-24980 secure@intel.com
n/a--BMRA software	Inadequate encryption strength for some BMRA software before version 22.08 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.4	CVE-2024-21787 secure@intel.com
n/a--EMON software	Uncontrolled search path in some EMON software before version 11.44 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-28953 secure@intel.com
n/a--Flexlm License Daemons for Intel(R) FPGA software	Insecure inherited permissions in some Flexlm License Daemons for Intel(R) FPGA software before version v11.19.5.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-23908 secure@intel.com
n/a--InnoCMS	A vulnerability, which was classified as critical, has been found in InnoCMS 0.3.1. This issue affects some unknown processing of the file /panel/pages/1/edit of the component Backend. The manipulation leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-17	4.7	CVE-2024-7899 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
n/a--installation software for Intel(R) Ethernet Adapter Driver Pack	Uncontrolled search path element in some installation software for Intel(R) Ethernet Adapter Driver Pack before version 28.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-22376 secure@intel.com
n/a--Intel Unite(R) Client Extended Display Plugin software installers	Incorrect default permissions in some Intel Unite(R) Client Extended Display Plugin software installers before version 1.1.352.157 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-22378 secure@intel.com
n/a--Intel(R) Advisor software	Incorrect default permissions for some Intel(R) Advisor software before version 2024.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-26025 secure@intel.com
n/a--Intel(R) AMT and Intel(R) Standard	Improper buffer restrictions in firmware for some Intel(R) AMT and Intel(R) Standard Manageability may allow a privileged user to potentially enable denial of service via network access.	2024-08-14	6.8	CVE-2023-38655 secure@intel.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Manageability				
n/a--Intel(R) Arc(TM) & Iris(R) Xe Graphics software	Improper access control in some Intel(R) Arc(TM) & Iris(R) Xe Graphics software before version 31.0.101.4824 may allow an authenticated user to potentially enable denial of service via local access.	2024-08-14	5	CVE-2024-28050 secure@intel.com
n/a--Intel(R) CIP software	Improper access control for some Intel(R) CIP software before version 2.4.10717 may allow an authenticated user to potentially enable denial of service via local access.	2024-08-14	5.5	CVE-2023-43489 secure@intel.com
n/a--Intel(R) Connectivity Performance Suite software installers	Incorrect default permissions for some Intel(R) Connectivity Performance Suite software installers before version 2.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2023-43747 secure@intel.com
n/a--Intel(R) CSME	Unchecked return value in firmware for some Intel(R) CSME may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	2024-08-14	5.7	CVE-2023-40067 secure@intel.com
n/a--Intel(R) CSME	Improper input validation in firmware for some Intel(R) CSME may allow a privileged user to potentially enable denial of service via local access.	2024-08-14	4.4	CVE-2023-34424 secure@intel.com
n/a--Intel(R) CSME	Integer overflow in firmware for some Intel(R) CSME may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2024-08-14	4.3	CVE-2024-21844 secure@intel.com
n/a--Intel(R) Data Center GPU Max Series 1100 and 1550 products	Improper conditions check in some Intel(R) Data Center GPU Max Series 1100 and 1550 products may allow a privileged user to potentially enable denial of service via local access.	2024-08-14	6.5	CVE-2024-24580 secure@intel.com
n/a--Intel(R) Distribution for GDB software	Uncontrolled search path in some Intel(R) Distribution for GDB software before version 2024.0.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-23491 secure@intel.com
n/a--Intel(R) Distribution for GDB software	Incorrect default permissions in some Intel(R) Distribution for GDB software before version 2024.0.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-23495 secure@intel.com
n/a--Intel(R) Distribution for GDB software	Improper buffer restrictions in some Intel(R) Distribution for GDB software before version 2024.0.1 may allow an authenticated user to potentially enable denial of service via local access.	2024-08-14	5.8	CVE-2024-25562 secure@intel.com
n/a--Intel(R) Ethernet Connection I219-LM install software	Uncontrolled search path in some Intel(R) Ethernet Connection I219-LM install software may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-21769 secure@intel.com
n/a--Intel(R) Ethernet Network Controllers and Adapters E810	Protection mechanism failure in Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters E810 Series before version 28.3 may allow an unauthenticated user to potentially enable denial of service via network access.	2024-08-14	6.5	CVE-2024-23499 secure@intel.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Series				
n/a--Intel(R) Ethernet Network Controllers and Adapters E810 Series	Protection mechanism failure in firmware for some Intel(R) Ethernet Network Controllers and Adapters E810 Series before version 4.4 may allow an unauthenticated user to potentially enable denial of service via network access.	2024-08-14	6.5	CVE-2024-24983 secure@intel.com
n/a--Intel(R) Ethernet Network Controllers and Adapters E810 Series	Improper conditions check in Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters E810 Series before version 28.3 may allow an authenticated user to potentially enable denial of service via local access.	2024-08-14	5.5	CVE-2024-21806 secure@intel.com
n/a--Intel(R) FPGA SDK for OpenCL(TM) software technology	Uncontrolled search path in some Intel(R) FPGA SDK for OpenCL(TM) software technology may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-23909 secure@intel.com
n/a--Intel(R) GPA software	Uncontrolled search path in some Intel(R) GPA software before version 2024.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-28046 secure@intel.com
n/a--Intel(R) HID Event Filter software installers	Insecure inherited permissions in some Intel(R) HID Event Filter software installers before version 2.2.2.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-25561 secure@intel.com
n/a--Intel(R) High Level Synthesis Compiler software	Uncontrolled search path in some Intel(R) High Level Synthesis Compiler software before version 23.4 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-23907 secure@intel.com
n/a--Intel(R) IPP Cryptography software	Uncontrolled search path for some Intel(R) IPP Cryptography software before version 2021.11 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-21784 secure@intel.com
n/a--Intel(R) IPP software	Uncontrolled search path in some Intel(R) IPP software before version 2021.11 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-28887 secure@intel.com
n/a--Intel(R) ISH software installers	Incorrect default permissions in some Intel(R) ISH software installers may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-23974 secure@intel.com
n/a--Intel(R) License Manager for FLEXlm product software	Uncontrolled search path for some Intel(R) License Manager for FLEXlm product software before version 11.19.5.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-24977 secure@intel.com
n/a--Intel(R) MAS (GUI)	Incorrect default permissions in software installer for Intel(R) MAS (GUI) may allow an authenticated user to potentially enable denial of service via local access.	2024-08-14	5.6	CVE-2024-27461 secure@intel.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--Intel(R) MPI Library software	Uncontrolled search path for some Intel(R) MPI Library software before version 2021.12 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-28876 secure@intel.com
n/a--Intel(R) oneAPI Compiler software	Uncontrolled search path for some Intel(R) oneAPI Compiler software before version 2024.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-21857 secure@intel.com
n/a--Intel(R) oneAPI Math Kernel Library software	Uncontrolled search path for some Intel(R) oneAPI Math Kernel Library software before version 2024.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-21766 secure@intel.com
n/a--Intel(R) Quartus(R) Prime Pro Edition Design Software	Uncontrolled search path for some Intel(R) Quartus(R) Prime Pro Edition Design Software before version 24.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-22184 secure@intel.com
n/a--Intel(R) Server Platforms	Out of bounds read in OpenBMC Firmware for some Intel(R) Server Platforms before versions egs-1.15-0, bhs-0.27 may allow a privileged user to potentially enable information disclosure via local access.	2024-08-14	6.7	CVE-2023-49144 secure@intel.com
n/a--Intel(R) Server Platforms	Uncaught exception in OpenBMC Firmware for some Intel(R) Server Platforms before versions egs-1.14-0, bhs-0.27 may allow an authenticated user to potentially enable denial of service via network access.	2024-08-14	4.3	CVE-2023-35123 secure@intel.com
n/a--Intel(R) Simics Package Manager software	Uncontrolled search path for some Intel(R) Simics Package Manager software before version 1.8.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-26027 secure@intel.com
n/a--Intel(R) TDX module software	Incomplete filtering of special elements in Intel(R) TDX module software before version TDX_1.5.01.00.592 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6	CVE-2024-39283 secure@intel.com
n/a--Intel(R) Trace Analyzer and Collector software	Uncontrolled search path for some Intel(R) Trace Analyzer and Collector software before version 2022.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-28172 secure@intel.com
n/a--Intel(R) VROC software	Uncontrolled search path for some Intel(R) VROC software before version 8.6.0.1191 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-23489 secure@intel.com
n/a--Intel(R) VTune(TM) Profiler software	Uncontrolled search path in some Intel(R) VTune(TM) Profiler software before versions 2024.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2024-08-14	6.7	CVE-2024-29015 secure@intel.com
n/a--Intel(R) Xeon Processors	Insufficient control flow management for some Intel(R) Xeon Processors may allow an authenticated user to potentially enable denial of service via local access.	2024-08-14	6.5	CVE-2024-22374 secure@intel.com
n/a--n/a	Cross Site Scripting vulnerability in Friendica v.2023.12 allows a remote attacker to obtain sensitive information via the lack of file type filtering in the file attachment parameter.	2024-08-15	6.1	CVE-2024-27731 cve@mitre.org cve@mitre.org

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	Incorrect access control in the delete_category function of Sourcecodester Computer Laboratory Management System v1.0 allows authenticated attackers with low-level privileges to arbitrarily delete categories.	2024-08-12	6.5	CVE-2024-41332 cve@mitre.org cve@mitre.org
n/a--n/a	A vulnerability in the Mitel 6800 Series, 6900 Series, and 6900w Series SIP Phones, including the 6970 Conference Unit, through R6.4.0.HF1 (R6.4.0.136) could allow an authenticated attacker with administrative privilege to conduct an argument injection attack, due to insufficient parameter sanitization during the boot process. A successful exploit could allow an attacker to execute arbitrary commands within the context of the system.	2024-08-12	6.8	CVE-2024-41710 cve@mitre.org cve@mitre.org cve@mitre.org
n/a--n/a	A vulnerability in the Mitel 6800 Series, 6900 Series, and 6900w Series SIP Phones, including the 6970 Conference Unit, through R6.4.0.HF1 (R6.4.0.136) could allow an unauthenticated attacker with physical access to the phone to conduct an argument injection attack, due to insufficient parameter sanitization. A successful exploit could allow an attacker to execute arbitrary commands within the context of the system.	2024-08-13	6.8	CVE-2024-41711 cve@mitre.org
n/a--n/a	In TOTOLINK X5000r v9.1.0cu.2350_b20230313, the file /cgi-bin/cstecgi.cgi contains an OS command injection vulnerability in setLedCfg. Authenticated Attackers can send malicious packet to execute arbitrary commands.	2024-08-13	6.8	CVE-2024-42740 cve@mitre.org
n/a--n/a	An issue in Silverpeas v.6.4.2 and lower allows a remote attacker to cause a denial of service via the password change function.	2024-08-16	6.5	CVE-2024-42849 cve@mitre.org cve@mitre.org
n/a--n/a	Cross Site Scripting vulnerability in Super easy enterprise management system v.1.0.0 and before allows a local attacker to execute arbitrary code via a crafted script to the /WebSet/DlgGridSet.html component.	2024-08-15	5	CVE-2024-42678 cve@mitre.org
n/a--n/a	axios 1.7.2 allows SSRF via unexpected behavior where requests for path relative URLs get processed as protocol relative URLs.	2024-08-12	4	CVE-2024-39338 cve@mitre.org cve@mitre.org
n/a--OcoMon	A vulnerability, which was classified as problematic, has been found in OcoMon 4.0RC1/4.0/5.0RC1. This issue affects some unknown processing of the file /includes/common/require_access_recovery.php of the component URL Handler. 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. Upgrading to version 4.0.1 and 5.0 is able to address this issue. It is recommended to upgrade the affected component.	2024-08-13	4.3	CVE-2024-7709 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
nissan-global -- blind_spot_detection_sensor_ecu_firmware	* Unprotected privileged mode access through UDS session in the Blind Spot Detection Sensor ECU firmware in Nissan Altima (2022) allows attackers to trigger denial-of-service (DoS) by unauthorized access to the ECU's programming session. * No preconditions implemented for ECU management functionality through UDS session in the Blind Spot Detection Sensor ECU in Nissan Altima (2022) allows attackers to disrupt normal ECU operations by triggering a control command without authentication.	2024-08-15	6.5	CVE-2024-6347 cve@asrg.io
NVIDIA--NVIDIA CV-CUDA	NVIDIA CV-CUDA for Ubuntu 20.04, Ubuntu 22.04, and Jetpack contains a vulnerability in Python APIs where a user may cause an uncontrolled resource consumption issue by a long running CV-CUDA Python process. A successful exploit of this vulnerability may lead to denial of service and data loss.	2024-08-12	6.1	CVE-2024-0115 psirt@nvidia.com
Olive Themes--Olive One Click	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Olive Themes Olive One Click Demo Import allows Accessing Functionality Not Properly	2024-08-13	5.3	CVE-2024-38749 audit@patchstack.

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Demo Import	Constrained by ACLs.This issue affects Olive One Click Demo Import: from n/a through 1.1.2.			com
open-telemetry--opentelemetry-collector-contrib	OpenTelemetry, also known as OTel, is a vendor-neutral open source Observability framework for instrumenting, generating, collecting, and exporting telemetry data such as traces, metrics, and logs. The bearertokenauth extension's server authenticator performs a simple, non-constant time string comparison of the received & configured bearer tokens. This impacts anyone using the `bearertokenauth` server authenticator. Malicious clients with network access to the collector may perform a timing attack against a collector with this authenticator to guess the configured token, by iteratively sending tokens and comparing the response time. This would allow an attacker to introduce fabricated or bad data into the collector's telemetry pipeline. The observable timing vulnerability was fixed by using constant-time comparison in 0.107.0	2024-08-13	6.5	CVE-2024-42368 security-advisories@github.com security-advisories@github.com security-advisories@github.com
openhab--openhab-webui	openHAB, a provider of open-source home automation software, has add-ons including the visualization add-on CometVisu. Several endpoints in versions prior to 4.2.1 of the CometVisu add-on of openHAB don't require authentication. This makes it possible for unauthenticated attackers to modify or to steal sensitive data. This issue may lead to sensitive information disclosure. Users should upgrade to version 4.2.1 of the CometVisu add-on of openHAB to receive a patch.	2024-08-12	6.5	CVE-2024-42470 security-advisories@github.com security-advisories@github.com
openhab--openhab-webui	openHAB, a provider of open-source home automation software, has add-ons including the visualization add-on CometVisu. CometVisuServlet in versions prior to 4.2.1 is susceptible to an unauthenticated path traversal vulnerability. Local files on the server can be requested via HTTP GET on the CometVisuServlet. This issue may lead to information disclosure. Users should upgrade to version 4.2.1 of the CometVisu add-on of openHAB to receive a patch.	2024-08-12	5.3	CVE-2024-42468 security-advisories@github.com security-advisories@github.com security-advisories@github.com
oretnom23 -- car_driving_school_management_system	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been declared as problematic. This vulnerability affects the function save_package of the file admin/packages/manag_package.php. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	6.5	CVE-2024-7662 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- car_driving_school_management_system	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been declared as problematic. Affected by this vulnerability is the function update_settings_info of the file /classes/SystemSettings.php?f=update_settings. The manipulation of the argument contact/address leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	6.1	CVE-2024-7677 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- car_driving_school_management_system	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /classes/Master.php?f=save_package. The manipulation of the argument name/description/training_duration leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	6.1	CVE-2024-7678 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- car_driving_school_management_sys	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file manage_user.php. The manipulation of the argument id leads	2024-08-12	5.3	CVE-2024-7663 cna@vuldb.com cna@vuldb.com cna@vuldb.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tem	to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.			cna@vuldb.com
oretnom23 -- car_driving_school_management_system	A vulnerability, which was classified as critical, has been found in SourceCodester Car Driving School Management System 1.0. Affected by this issue is some unknown functionality of the file view_package.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	5.3	CVE-2024-7666 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- car_driving_school_management_system	A vulnerability, which was classified as critical, was found in SourceCodester Car Driving School Management System 1.0. This affects the function delete_users of the file User.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.	2024-08-12	5.3	CVE-2024-7667 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- car_driving_school_management_system	A vulnerability has been found in SourceCodester Car Driving School Management System 1.0 and classified as critical. This vulnerability affects the function delete_package of the file Master.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.	2024-08-12	5.3	CVE-2024-7668 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- car_driving_school_management_system	A vulnerability was found in SourceCodester Car Driving School Management System 1.0 and classified as critical. This issue affects the function delete_enrollment of the file Master.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.	2024-08-12	5.3	CVE-2024-7669 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- car_driving_school_management_system	A vulnerability was found in Sourcecodester Car Driving School Management System 1.0. It has been classified as critical. Affected is the function save_package of the file /classes/Master.php?f=save_package. 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.	2024-08-12	5.3	CVE-2024-7676 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- car_driving_school_management_system	A vulnerability classified as critical has been found in SourceCodester Car Driving School Management System 1.0. Affected is an unknown function of the file view_details.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	4.3	CVE-2024-7664 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- car_driving_school_management_system	A vulnerability classified as critical was found in SourceCodester Car Driving School Management System 1.0. Affected by this vulnerability is an unknown functionality of the file manage_package.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.	2024-08-12	4.3	CVE-2024-7665 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- clinics_patient_management_system	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /update_medicine.php. The manipulation of the argument medicine_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.	2024-08-14	6.1	CVE-2024-7752 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
oretnom23 -- clinics_patient_ma	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file users.php of the component User Page. The manipulation leads to cross-	2024-08-12	5.4	CVE-2024-7645 cna@vuldb.com cna@vuldb.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nagement_system	site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.			cna@vuldb.com cna@vuldb.com
Patrick Posner--Filr Secure document library	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Patrick Posner Filr - Secure document library allows Stored XSS.This issue affects Filr - Secure document library: from n/a through 1.2.4.	2024-08-12	6.5	CVE-2024-43216 audit@patchstack.com
Pepperl+Fuchs--ICDM-RX/TCP-DB9/RJ45-DIN	An unauthenticated remote attacker may use a HTML injection vulnerability with limited length to inject malicious HTML code and gain low-privileged access on the affected device.	2024-08-13	6.1	CVE-2024-38501 info@cert.vde.com
phpgurukul --old_age_home_management_system	A Reflected Cross Site Scripting (XSS) vulnerability was found in "/oahms/search.php" in PHPGurukul Old Age Home Management System v1.0, which allows remote attackers to execute arbitrary code via the "searchdata" parameter.	2024-08-12	6.1	CVE-2024-40484 cve@mitre.org
phpgurukul --old_age_home_management_system	A Stored Cross Site Scripting (XSS) vulnerability was found in "/admin/view-enquiry.php" in PHPGurukul Old Age Home Management System v1.0, which allows remote attackers to execute arbitrary code via the Contact Us page "message" parameter.	2024-08-12	5.4	CVE-2024-40481 cve@mitre.org
PickPlugins--ComboBlocks	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PickPlugins ComboBlocks allows Stored XSS.This issue affects ComboBlocks: from n/a through 2.2.86.	2024-08-12	6.5	CVE-2024-43155 audit@patchstack.com
pickplugins--Gutenberg Blocks, Page Builder ComboBlocks	The Gutenberg Blocks, Page Builder - ComboBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Accordion block in all versions up to, and including, 2.2.87 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.	2024-08-14	6.4	CVE-2024-7588 security@wordfence.com security@wordfence.com
pkp--ojs	A vulnerability was found in pkp ojs up to 3.4.0-6 and classified as problematic. Affected by this issue is some unknown functionality of the file /login/signOut. The manipulation of the argument source with the input .example.com leads to open redirect. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-17	4.3	CVE-2024-7902 cna@vuldb.com cna@vuldb.com cna@vuldb.com
princeahmed--Radio Player Live Shoutcast, Icecast and Any Audio Stream Player for WordPress	The Radio Player plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the delete_player function in versions up to, and including, 2.0.73. This makes it possible for unauthenticated attackers to delete player instances.	2024-08-17	5.3	CVE-2023-4024 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
princeahmed--Radio Player Live Shoutcast, Icecast and Any Audio Stream Player for	The Radio Player plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the update_player function in versions up to, and including, 2.0.73. This makes it possible for unauthenticated attackers to update player instances.	2024-08-17	5.3	CVE-2023-4025 security@wordfence.com security@wordfence.com security@wordfence.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WordPress				security@wordfence.com
princeahmed--Radio Player Live Shoutcast, Icecast and Any Audio Stream Player for WordPress	The Radio Player plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the update_settings function in versions up to, and including, 2.0.73. This makes it possible for unauthenticated attackers to update plugin settings.	2024-08-17	5.3	CVE-2023-4027 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
projectsend --projectsend	A vulnerability, which was classified as problematic, has been found in projectsend up to r1605. This issue affects the function get_preview of the file process.php. The manipulation leads to improper control of resource identifiers. The attack may be initiated remotely. Upgrading to version r1720 is able to address this issue. The patch is named eb5a04774927e5855b9d0e5870a2aae5a3dc5a08. It is recommended to upgrade the affected component.	2024-08-12	5.3	CVE-2024-7658 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
PTC--Kepware ThingWorx Kepware Server	When performing an online tag generation to devices which communicate using the ControlLogix protocol, a machine-in-the-middle, or a device that is not configured correctly, could deliver a response leading to unrestricted or unregulated resource allocation. This could cause a denial-of-service condition and crash the Kepware application. By default, these functions are turned off, yet they remain accessible for users who recognize and require their advantages.	2024-08-16	5.3	CVE-2024-6098 ics-cert@hq.dhs.gov ics-cert@hq.dhs.gov
Pylons--webob	WebOb provides objects for HTTP requests and responses. When WebOb normalizes the HTTP Location header to include the request hostname, it does so by parsing the URL that the user is to be redirected to with Python's urlparse, and joining it to the base URL. `urlparse` however treats a `//` at the start of a string as a URI without a scheme, and then treats the next part as the hostname. `urljoin` will then use that hostname from the second part as the hostname replacing the original one from the request. This vulnerability is patched in WebOb version 1.8.8.	2024-08-14	6.1	CVE-2024-42353 security-advisories@github.com security-advisories@github.com
QNAP Systems Inc.--QTS	A vulnerability has been reported to affect Network & Virtual Switch. If exploited, the vulnerability could allow local authenticated administrators to gain access to and execute certain functions via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 5.1.8.2823 build 20240712 and later QuTS hero h5.1.8.2823 build 20240712 and later	2024-08-12	4.2	CVE-2024-32765 security@qnapsecurity.com.tw
Rashid87--WPSection	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Rashid87 WPSection allows PHP Local File Inclusion.This issue affects WPSection: from n/a through 1.3.8.	2024-08-13	6.5	CVE-2024-43165 audit@patchstack.com
Red Hat--Red Hat Enterprise Linux 6	A heap-buffer-overflow flaw was found in the cfg_mark_ports function within Unbound's config_file.c, which can lead to memory corruption. This issue could allow an attacker with local access to provide specially crafted input, potentially causing the application to crash or allowing arbitrary code execution. This could result in a denial of service or unauthorized actions on the system.	2024-08-12	4.8	CVE-2024-43168 secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Satellite 6	A command injection flaw was found in the "Host Init Config" template in the Foreman application via the "Install Packages" field on the "Register Host" page. This flaw allows an attacker with the necessary privileges to inject arbitrary commands into the configuration, potentially allowing unauthorized command execution during host registration. Although this issue requires user interaction to execute injected commands, it poses a significant risk if an unsuspecting user runs the generated registration script.	2024-08-12	6.5	CVE-2024-7700 secalert@redhat.com secalert@redhat.com
rems -- accounts_manager_app	A vulnerability, which was classified as problematic, was found in SourceCodester Accounts Manager App 1.0. Affected is an unknown function of the file /endpoint/add-account.php. The manipulation of the argument account_name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-13	5.4	CVE-2024-7749 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
rems -- file_manager_app	A vulnerability has been found in SourceCodester File Manager App 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Add File Handler. The manipulation of the argument File Title/Uploaded By leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	6.1	CVE-2024-7660 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
rems -- leads_manager_tool	A vulnerability was found in SourceCodester Leads Manager Tool 1.0. It has been classified as problematic. This affects an unknown part of the file /endpoint/add-leads.php of the component Add Leads Handler. The manipulation of the argument leads_name/phone_number 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.	2024-08-12	5.4	CVE-2024-7644 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
reputeinfosystems --ARMember Membership Plugin, Content Restriction, Member Levels, User Profile & User signup	The ARMember - Membership Plugin, Content Restriction, Member Levels, User Profile & User signup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 4.0.37 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	2024-08-17	6.4	CVE-2024-7703 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
SAP_SE--SAP BusinessObjects Business Intelligence Platform	SAP BusinessObjects Business Intelligence Platform allows an authenticated attacker to upload malicious code over the network, that could be executed by the application. On successful exploitation, the attacker can cause a low impact on the Integrity of the application.	2024-08-13	4.3	CVE-2024-42375 cna@sap.com cna@sap.com
SAP_SE--SAP Commerce Backoffice	SAP Commerce Backoffice does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability causing low impact on confidentiality and integrity of the application.	2024-08-13	5.4	CVE-2024-41735 cna@sap.com cna@sap.com
SAP_SE--SAP Commerce	In SAP Commerce, valid user accounts can be identified during the customer registration and login processes. This allows a potential attacker to learn if a given e-mail is used for an account, but does not grant access to any customer data beyond this knowledge. The attacker must already know the e-mail that they wish to test for. The impact on confidentiality therefore is low and no impact to integrity or availability	2024-08-13	5.3	CVE-2024-41733 cna@sap.com cna@sap.com
SAP_SE--SAP CRM ABAP (Insights	SAP CRM ABAP (Insights Management) allows an authenticated attacker to enumerate HTTP endpoints in the internal network by specially crafting HTTP	2024-08-13	5	CVE-2024-41737 cna@sap.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management)	requests. On successful exploitation this can result in information disclosure. It has no impact on integrity and availability of the application.			cna@sap.com
SAP_SE--SAP Document Builder	SAP Document Builder does not perform necessary authorization checks for one of the function modules resulting in escalation of privileges causing low impact on confidentiality of the application.	2024-08-13	4.3	CVE-2024-39591 cna@sap.com cna@sap.com
SAP_SE--SAP NetWeaver Application Server (ABAP and Java),SAP Web Dispatcher and SAP Content Server	Due to the missing authorization checks in the local systems, the admin users of SAP Web Dispatcher, SAP NetWeaver Application Server (ABAP and Java), and SAP Content Server can impersonate other users and may perform some unintended actions. This could lead to a low impact on confidentiality and a high impact on the integrity and availability of the applications.	2024-08-13	6.3	CVE-2024-33005 cna@sap.com cna@sap.com
SAP_SE--SAP NetWeaver Application Server ABAP and ABAP Platform	Due to missing authorization check in SAP NetWeaver Application Server ABAP and ABAP Platform, an authenticated attacker could call an underlying transaction, which leads to disclosure of user related information. There is no impact on integrity or availability.	2024-08-13	4.3	CVE-2024-41734 cna@sap.com cna@sap.com
SAP_SE--SAP NetWeaver Application Server ABAP	SAP NetWeaver Application Server ABAP allows an unauthenticated attacker to craft a URL link that could bypass allowlist controls. Depending on the web applications provided by this server, the attacker might inject CSS code or links into the web application that could allow the attacker to read or modify information. There is no impact on availability of application.	2024-08-13	4.7	CVE-2024-41732 cna@sap.com cna@sap.com
SAP_SE--SAP Permit to Work	Under certain conditions SAP Permit to Work allows an authenticated attacker to access information which would otherwise be restricted causing low impact on the confidentiality of the application.	2024-08-13	4.3	CVE-2024-41736 cna@sap.com cna@sap.com
SAP_SE--SAP Shared Service Framework	SAP Shared Service Framework does not perform necessary authorization check for an authenticated user, resulting in escalation of privileges. On successful exploitation, an attacker can cause a high impact on confidentiality of the application.	2024-08-13	6.5	CVE-2024-42376 cna@sap.com cna@sap.com
SAP_SE--SAP Shared Service Framework	SAP shared service framework allows an authenticated non-administrative user to call a remote-enabled function, which will allow them to insert value entries into a non-sensitive table, causing low impact on integrity of the application	2024-08-13	4.3	CVE-2024-42377 cna@sap.com cna@sap.com
SAP_SE--SAP Student Life Cycle Management (SLcM)	SAP Student Life Cycle Management (SLcM) fails to conduct proper authorization checks for authenticated users, leading to the potential escalation of privileges. On successful exploitation it could allow an attacker to delete non-sensitive report variants that are typically restricted, causing minimal impact on the integrity of the application.	2024-08-13	4.3	CVE-2024-42373 cna@sap.com cna@sap.com
siemens -- location_intelligence	A vulnerability has been identified in Location Intelligence family (All versions < V4.4). Affected products do not properly enforce restriction of excessive authentication attempts. This could allow an unauthenticated remote attacker to conduct brute force attacks against legitimate user passwords.	2024-08-13	5.3	CVE-2024-41682 productcert@siemens.com
siemens -- location_intelligence	A vulnerability has been identified in Location Intelligence family (All versions < V4.4). Affected products do not properly enforce a strong user password policy. This could facilitate a brute force attack against legitimate user passwords.	2024-08-13	5.3	CVE-2024-41683 productcert@siemens.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- sinec_nms	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The affected application does not properly enforce authorization checks. This could allow an authenticated attacker to bypass the checks and modify settings in the application without authorization.	2024-08-13	4.3	CVE-2024-41941 productcert@siemens.com
siemens -- sinec_traffic_analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application do not have access control for accessing the files. This could allow an authenticated attacker with low privilege's to get access to sensitive information.	2024-08-13	6.5	CVE-2024-41905 productcert@siemens.com
siemens -- sinec_traffic_analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application does not properly handle cacheable HTTP responses in the web service. This could allow an attacker to read and modify data stored in the local cache.	2024-08-13	6.5	CVE-2024-41906 productcert@siemens.com
siemens -- sinec_traffic_analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V2.0). The affected application is missing general HTTP security headers in the web server. This could allow an attacker to make the servers more prone to clickjacking attack.	2024-08-13	5.4	CVE-2024-41907 productcert@siemens.com
Siemens--LOGO! 12/24RCE	A vulnerability has been identified in LOGO! 12/24RCE (6ED1052-1MD08-0BA1) (All versions), LOGO! 12/24RCEo (6ED1052-2MD08-0BA1) (All versions), LOGO! 230RCE (6ED1052-1FB08-0BA1) (All versions), LOGO! 230RCEo (6ED1052-2FB08-0BA1) (All versions), LOGO! 24CE (6ED1052-1CC08-0BA1) (All versions), LOGO! 24CEo (6ED1052-2CC08-0BA1) (All versions), LOGO! 24RCE (6ED1052-1HB08-0BA1) (All versions), LOGO! 24RCEo (6ED1052-2HB08-0BA1) (All versions), SIPLUS LOGO! 12/24RCE (6AG1052-1MD08-7BA1) (All versions), SIPLUS LOGO! 12/24RCEo (6AG1052-2MD08-7BA1) (All versions), SIPLUS LOGO! 230RCE (6AG1052-1FB08-7BA1) (All versions), SIPLUS LOGO! 230RCEo (6AG1052-2FB08-7BA1) (All versions), SIPLUS LOGO! 24CE (6AG1052-1CC08-7BA1) (All versions), SIPLUS LOGO! 24CEo (6AG1052-2CC08-7BA1) (All versions), SIPLUS LOGO! 24RCE (6AG1052-1HB08-7BA1) (All versions), SIPLUS LOGO! 24RCEo (6AG1052-2HB08-7BA1) (All versions). Affected devices store user passwords in plaintext without proper protection. This could allow a physical attacker to retrieve them from the embedded storage ICs.	2024-08-13	4.6	CVE-2024-39922 productcert@siemens.com
Siemens--RUGGEDCOM RM1224 LTE(4G) EU	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.1), RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2) (All versions < V8.1), SCALANCE M804PB (6GK5804-0AP00-2AA2) (All versions < V8.1), SCALANCE M812-1 ADSL-Router family (All versions < V8.1), SCALANCE M816-1 ADSL-Router family (All versions < V8.1), SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2) (All versions < V8.1), SCALANCE M874-2 (6GK5874-2AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 (6GK5874-3AA00-2AA2) (All versions < V8.1), SCALANCE M874-3 3G-Router (CN) (6GK5874-3AA00-2FA2) (All versions < V8.1), SCALANCE M876-3 (6GK5876-3AA02-2BA2) (All versions < V8.1), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.1), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.1), SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2) (All versions < V8.1), SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2) (All versions < V8.1), SCALANCE MUM853-1 (A1) (6GK5853-2EA10-2AA1) (All versions < V8.1), SCALANCE MUM853-1 (B1) (6GK5853-2EA10-2BA1) (All versions < V8.1), SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1) (All versions < V8.1), SCALANCE MUM856-1 (A1) (6GK5856-2EA10-3AA1) (All versions < V8.1), SCALANCE MUM856-1 (B1) (6GK5856-2EA10-3BA1) (All versions < V8.1), SCALANCE MUM856-1 (CN) (6GK5856-2EA00-3FA1) (All versions < V8.1), SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1) (All versions < V8.1), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.1), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.1), SCALANCE S615 LAN-Router (6GK5615-0AA00-2AA2) (All versions < V8.1). Affected devices insert sensitive information about the generation of 2FA tokens into log files. This could allow an authenticated remote attacker to forge 2FA tokens of other users.	2024-08-13	6.5	CVE-2024-41978 productcert@siemens.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
smub--Easy Digital Downloads eCommerce Payments and Subscriptions made easy	The Easy Digital Downloads - Sell Digital Files & Subscriptions (eCommerce Store + Payments Made Easy) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the currency value in all versions up to, and including, 3.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, 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.	2024-08-12	4.4	CVE-2024-6691 security@wordfence.com security@wordfence.com
Soliloquy Team--Slider by Soliloquy	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting'), Improper Authentication vulnerability in Soliloquy Team Slider by Soliloquy allows Cross-Site Scripting (XSS).This issue affects Slider by Soliloquy: from n/a through 2.7.6.	2024-08-12	5.9	CVE-2024-35775 audit@patchstack.com
SourceCodester--Clinics Patient Management System	A vulnerability classified as critical was found in SourceCodester Clinics Patient Management System 1.0. This vulnerability affects unknown code of the file /pms/ajax/check_user_name.php. The manipulation of the argument user_name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	6.3	CVE-2024-7841 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Daily Expenses Monitoring App	A vulnerability classified as critical has been found in SourceCodester Daily Expenses Monitoring App 1.0. This affects an unknown part of the file /endpoint/delete-expense.php. The manipulation of the argument expense leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	6.3	CVE-2024-7811 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Online Graduate Tracer System	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /tracking/admin/view_itprofile.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	6.3	CVE-2024-7810 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Online Graduate Tracer System	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /tracking/admin/fetch_it.php. The manipulation of the argument request leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-16	6.3	CVE-2024-7845 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Online Graduate Tracer System	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /tracking/nbproject/. The manipulation leads to exposure of information through directory listing. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	5.3	CVE-2024-7809 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Online Graduate Tracer System	A vulnerability, which was classified as problematic, has been found in SourceCodester Online Graduate Tracer System 1.0. This issue affects some unknown processing of the file /tracking/admin/export_it.php. The manipulation leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	5.3	CVE-2024-7842 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Online Graduate Tracer System	A vulnerability, which was classified as problematic, was found in SourceCodester Online Graduate Tracer System 1.0. Affected is an unknown function of the file /tracking/admin/exportcs.php. The manipulation leads to information disclosure. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	5.3	CVE-2024-7843 cna@vuldb.com cna@vuldb.com cna@vuldb.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				cna@vuldb.com
SourceCodester--Prison Management System	A vulnerability, which was classified as problematic, has been found in SourceCodester Prison Management System 1.0. This issue affects some unknown processing of the file /uploadImage/Profile/ of the component Profile Image Handler. The manipulation leads to insufficiently protected credentials. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	5.3	CVE-2024-7813 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Simple Online Bidding System	A vulnerability classified as critical has been found in SourceCodester Simple Online Bidding System 1.0. This affects an unknown part of the file /simple-online-bidding-system/bidding/admin/ajax.php?action=delete_product. 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.	2024-08-15	6.3	CVE-2024-7800 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Simple Online Bidding System	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /simple-online-bidding-system/bidding/admin/users.php. The manipulation leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	5.3	CVE-2024-7799 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Task Progress Tracker	A vulnerability was found in SourceCodester Task Progress Tracker 1.0. It has been classified as critical. Affected is an unknown function of the file /endpoint/delete-task.php. The manipulation of the argument task leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-14	6.3	CVE-2024-7792 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Yoga Class Registration System	A vulnerability has been found in SourceCodester Yoga Class Registration System 1.0 and classified as critical. This vulnerability affects unknown code of the file /classes/Users.php?f=save of the component Add User Handler. The manipulation leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-16	6.3	CVE-2024-7851 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Yoga Class Registration System	A vulnerability was found in SourceCodester Yoga Class Registration System up to 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/?page=categories/view_category. 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.	2024-08-16	6.3	CVE-2024-7853 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
sprecher-automation --sprecon-e_cp-2500_firmware	Improper Privilege ManagementÂ inÂ Sprecher Automation SPRECON-E below version 8.71j allows a remote attacker with low privileges to save unauthorized protection assignments.	2024-08-12	6.5	CVE-2024-6758 info@cert.vde.com
steve-community -- steve	SteVe is an open platform that implements different version of the OCPP protocol for Electric Vehicle charge points, acting as a central server for management of registered charge points. Attackers can inject arbitrary HTML and Javascript code via WebSockets leading to persistent Cross-Site Scripting in the SteVe management interface.	2024-08-12	6.1	CVE-2024-21550 report@snyk.io report@snyk.io report@snyk.io report@snyk.io
symphony-cms --symphony_cms	A Cross Site Scripting (XSS) vulnerability in Symphony CMS 2.7.10 allows remote attackers to inject arbitrary web script or HTML by editing note.	2024-08-13	5.4	CVE-2024-41613 cve@mitre.org

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
symphony-cms -- symphony_cms	symphonycms <=2.7.10 is vulnerable to Cross Site Scripting (XSS) in the Comment component for articles.	2024-08-13	4.8	CVE-2024-41614 cve@mitre.org
Techeshta--Card Elements for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Techeshta Card Elements for Elementor allows Stored XSS.This issue affects Card Elements for Elementor: from n/a through 1.2.2.	2024-08-12	6.5	CVE-2024-43123 audit@patchstack.com
ThemeLooks--Enter Addons	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeLooks Enter Addons allows Stored XSS.This issue affects Enter Addons: from n/a through 2.1.7.	2024-08-12	6.5	CVE-2024-43225 audit@patchstack.com
ThemeSphere--SmartMag	Exposure of Sensitive Information to an Unauthorized Actor, Missing Authorization vulnerability in ThemeSphere SmartMag allows Excavation, Accessing Functionality Not Properly Constrained by ACLs.This issue affects SmartMag: from n/a through 9.3.0.	2024-08-12	5.3	CVE-2024-37930 audit@patchstack.com
Themeum--Tutor LMS	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themeum Tutor LMS allows Stored XSS.This issue affects Tutor LMS: from n/a through 2.7.3.	2024-08-12	6.5	CVE-2024-43231 audit@patchstack.com
Themify--Themify Shortcodes	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themify Themify Shortcodes allows Stored XSS.This issue affects Themify Shortcodes: from n/a through 2.1.1.	2024-08-12	6.5	CVE-2024-43133 audit@patchstack.com
ThimPress--LearnPress	Authorization Bypass Through User-Controlled Key vulnerability in ThimPress LearnPress allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects LearnPress: from n/a through 4.2.6.8.2.	2024-08-13	6.5	CVE-2024-39642 audit@patchstack.com
Tosei--Online Store Management System	A vulnerability was found in Tosei Online Store Management System ãƒ‍ãƒƒãƒˆå¤—èˆ—ç®¡ç†ã‚·ã‚¹ãƒ†ãƒ 4.02/4.03/4.04. It has been rated as critical. Affected by this issue is some unknown functionality of the file /cgi-bin/p1_ftpserver.php. The manipulation of the argument adr_txt leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-17	6.3	CVE-2024-7896 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Tosei--Online Store Management System	A vulnerability classified as critical has been found in Tosei Online Store Management System ãƒ‍ãƒƒãƒˆå¤—èˆ—ç®¡ç†ã‚·ã‚¹ãƒ†ãƒ 4.02/4.03/4.04. This affects an unknown part of the file /cgi-bin/tosei_kikai.php. The manipulation of the argument kikaibangou leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-17	6.3	CVE-2024-7897 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
typora -- typora	Typora before 1.9.3 Markdown editor has a cross-site scripting (XSS) vulnerability via the Mermaid component.	2024-08-12	6.1	CVE-2024-41481 cve@mitre.org
typora -- typora	Typora before 1.9.3 Markdown editor has a cross-site scripting (XSS) vulnerability via the MathJax component.	2024-08-12	6.1	CVE-2024-41482 cve@mitre.org
Unknown--Category Posts Widget	The Category Posts Widget WordPress plugin before 4.9.17, term-and-category-based-posts-widget WordPress plugin before 4.9.13 does not validate and escape some of its "Category Posts" widget settings before outputting them back in a page/post where the Widget is embed, which could allow high privilege users such	2024-08-12	4.8	CVE-2024-6158 contact@wpscan.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)			
Unknown--Generate Images	The Generate Images WordPress plugin before 5.2.8 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)	2024-08-13	4.8	CVE-2024-6724 contact@wpscan.com
Unknown--wp-cart-for-digital-products	The wp-cart-for-digital-products WordPress plugin before 8.5.6 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	2024-08-12	6.5	CVE-2024-6133 contact@wpscan.com
Unknown--wp-cart-for-digital-products	The wp-cart-for-digital-products WordPress plugin before 8.5.6 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	2024-08-12	5.4	CVE-2024-6134 contact@wpscan.com
Unknown--wp-cart-for-digital-products	The wp-cart-for-digital-products WordPress plugin before 8.5.6 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	2024-08-12	5.4	CVE-2024-6136 contact@wpscan.com
vim--vim	The UNIX editor Vim prior to version 9.1.0678 has a use-after-free error in argument list handling. When adding a new file to the argument list, this triggers `Buf*` autocommands. If in such an autocommand the buffer that was just opened is closed (including the window where it is shown), this causes the window structure to be freed which contains a reference to the argument list that we are actually modifying. Once the autocommands are completed, the references to the window and argument list are no longer valid and as such cause an use-after-free. Impact is low since the user must either intentionally add some unusual autocommands that wipe a buffer during creation (either manually or by sourcing a malicious plugin), but it will crash Vim. The issue has been fixed as of Vim patch v9.1.0678.	2024-08-16	4.5	CVE-2024-43374 security-advisories@github.com security-advisories@github.com
wanglongcn--ltcms	A vulnerability was found in wanglongcn ltcms 1.0.20 and classified as critical. This issue affects the function downloadFile of the file /api/file/downloadfile of the component API Endpoint. The manipulation of the argument file leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-13	5.3	CVE-2024-7741 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
WappPress Team--WappPress	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WappPress Team WappPress allows Stored XSS.This issue affects WappPress: from n/a through 6.0.4.	2024-08-12	5.9	CVE-2024-43137 audit@patchstack.com
WC Product Table--WooCommerce Product Table Lite	Improper Control of Generation of Code ('Code Injection') vulnerability in WC Product Table WooCommerce Product Table Lite allows Code Injection.This issue affects WooCommerce Product Table Lite: from n/a through 3.5.1.	2024-08-13	6.5	CVE-2024-43128 audit@patchstack.com
Weaver--e-cology	A vulnerability was found in Weaver e-cology 8. It has been classified as problematic. Affected is an unknown function of the file /cloudstore/ecode/setup/ecology_dev.zip of the component Source Code Handler. The manipulation leads to information disclosure. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-12	5.3	CVE-2024-7704 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Weblizar--Coming Soon	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Weblizar Coming Soon allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Coming Soon: from n/a through 1.6.3.	2024-08-13	5.3	CVE-2024-38756 audit@patchstack.com
WP Table Builder--WP Table Builder WordPress Table Plugin	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Table Builder WP Table Builder - WordPress Table Plugin allows Stored XSS.This issue affects WP Table Builder - WordPress Table Plugin: from n/a through 1.4.15.	2024-08-12	6.5	CVE-2024-43125 audit@patchstack.com
Wp2speed--WP2Speed Faster	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wp2speed WP2Speed Faster allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WP2Speed Faster: from n/a through 1.0.1.	2024-08-12	5.3	CVE-2024-37924 audit@patchstack.com
wp_media--BackWPup WordPress Backup & Restore Plugin	The BackWPup plugin for WordPress is vulnerable to Directory Traversal in versions up to, and including, 4.0.1 via the job-specific backup folder. This allows authenticated attackers to store backups in arbitrary folders on the server provided they can be written to by the server. Additionally, default settings will place an index.php and a .htaccess file into the chosen directory (unless already present) when the first backup job is run that are intended to prevent directory listing and file access. This means that an attacker could set the backup directory to the root of another site in a shared environment and thus disable that site.	2024-08-17	6.8	CVE-2023-5505 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
WPDeveloper--BetterDocs	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WPDeveloper BetterDocs allows PHP Local File Inclusion.This issue affects BetterDocs: from n/a through 3.5.8.	2024-08-13	6.5	CVE-2024-43129 audit@patchstack.com
WPDeveloper--BetterDocs	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloper BetterDocs allows Stored XSS.This issue affects BetterDocs: from n/a through 3.5.8.	2024-08-12	6.5	CVE-2024-43227 audit@patchstack.com
wpdevteam--Essential Addons for Elementor Best Elementor Templates, Widgets, Kits & WooCommerce Builders	The Essential Addons for Elementor - Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'no_more_items_text' parameter in all versions up to, and including, 5.9.27 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.	2024-08-13	6.4	CVE-2024-7092 security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com security@wordfence.com
wpfeedback--Visual Website Collaboration, Feedback & Project Management	The Visual Website Collaboration, Feedback & Project Management - Atarim plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the process_wpfeedback_misc_options() function in all versions up to, and including, 4.0.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the plugins settings which can also be leveraged to gain access to the plugin's settings.	2024-08-12	5.4	CVE-2024-7621 security@wordfence.com security@wordfence.com security@wordfenc

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Atarim				e.com
wpmet--ElementsKit Pro	The ElementsKit Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several parameters in all versions up to, and including, 3.6.5 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.	2024-08-15	6.4	CVE-2024-7064 security@wordfence.com security@wordfence.com
wpmet--ElementsKit Pro	The ElementsKit Pro plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.6.6 via the 'render_raw' function. This can allow authenticated attackers, with Contributor-level permissions and above, to extract sensitive data including private, future, and draft posts.	2024-08-15	4.3	CVE-2024-7063 security@wordfence.com security@wordfence.com
wpopal--Opal Membership	The Opal Membership plugin for WordPress is vulnerable to Stored Cross-Site Scripting via checkout form fields in all versions up to, and including, 1.2.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-12	6.1	CVE-2024-7649 security@wordfence.com security@wordfence.com
wpopal--Opal Membership	The Opal Membership plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.2.4 via the private notes functionality on payments which utilizes WordPress comments. This makes it possible for authenticated attackers, with subscriber-level access and above, to view private notes via recent comments that should be restricted to just administrators.	2024-08-12	4.3	CVE-2024-7648 security@wordfence.com security@wordfence.com security@wordfence.com
Xpro--Xpro Elementor Addons	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Xpro Xpro Elementor Addons allows Stored XSS.This issue affects Xpro Elementor Addons: from n/a through 1.4.4.2.	2024-08-12	6.5	CVE-2024-43150 audit@patchstack.com
Xyzscripts--Insert PHP Code Snippet	Cross-Site Request Forgery (CSRF) vulnerability in Xyzscripts Insert PHP Code Snippet.This issue affects Insert PHP Code Snippet: from n/a through 1.3.6.	2024-08-15	5.4	CVE-2024-43275 audit@patchstack.com
yogeshojha--rengine	reNgine is an automated reconnaissance framework for web applications. Versions 2.1.2 and prior are susceptible to Stored Cross-Site Scripting (XSS) attacks. This vulnerability occurs when scanning a domain, and if the target domain's DNS record contains an XSS payload, it leads to the execution of malicious scripts in the reNgine's dashboard view when any user views the scan results. The XSS payload is directly fetched from the DNS record of the remote target domain. Consequently, an attacker can execute the attack without requiring any additional input from the target or the reNgine user. A patch is available and expected to be part of version 2.1.3.	2024-08-16	5	CVE-2024-43381 security-advisories@github.com security-advisories@github.com
Yuri Baranov--YaMaps for WordPress	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Yuri Baranov YaMaps for WordPress allows Stored XSS.This issue affects YaMaps for WordPress: from n/a through 0.6.27.	2024-08-12	6.5	CVE-2024-43224 audit@patchstack.com
yzane--vscode-markdown-pdf	A vulnerability, which was classified as problematic, was found in yzane vscode-markdown-pdf 1.5.0. This affects an unknown part. The manipulation leads to cross	2024-08-13	4.3	CVE-2024-7739 cna@vuldb.com cna@vuldb.com cna@vuldb.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.			cna@vuldb.com cna@vuldb.com
Zabbix--Zabbix	A non-admin user can change or remove important features within the Zabbix Agent application, thus impacting the integrity and availability of the application.	2024-08-12	6.1	CVE-2024-22121 security@zabbix.com
Zabbix--Zabbix	User with no permission to any of the Hosts can access and view host count & other statistics through System Information Widget in Global View Dashboard.	2024-08-12	4.3	CVE-2024-22114 security@zabbix.com
zimbra -- collaboration	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. A Cross-Site Scripting (XSS) vulnerability exists in the CalendarInvite feature of the Zimbra webmail classic user interface, because of improper input validation in the handling of the calendar header. An attacker can exploit this via an email message containing a crafted calendar header with an embedded XSS payload. When a victim views this message in the Zimbra webmail classic interface, the payload is executed in the context of the victim's session, potentially leading to execution of arbitrary JavaScript code.	2024-08-12	6.1	CVE-2024-27443 cve@mitre.org cve@mitre.org
zimbra -- collaboration	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0, issue 1 of 2. A reflected cross-site scripting (XSS) vulnerability has been identified in the Zimbra webmail admin interface. This vulnerability occurs due to inadequate input validation of the packages parameter, allowing an authenticated attacker to inject and execute arbitrary JavaScript code within the context of another user's browser session. By uploading a malicious JavaScript file and crafting a URL containing its location in the packages parameter, the attacker can exploit this vulnerability. Subsequently, when another user visits the crafted URL, the malicious JavaScript code is executed.	2024-08-12	5.4	CVE-2024-33533 cve@mitre.org cve@mitre.org
zimbra -- collaboration	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 10.0. The vulnerability occurs due to inadequate input validation of the res parameter, allowing an authenticated attacker to inject and execute arbitrary JavaScript code within the context of another user's browser session. By uploading a malicious JavaScript file, accessible externally, and crafting a URL containing its location in the res parameter, the attacker can exploit this vulnerability. Subsequently, when another user visits the crafted URL, the malicious JavaScript code is executed.	2024-08-12	5.4	CVE-2024-33536 cve@mitre.org cve@mitre.org
Zoho Campaigns--Zoho Campaigns	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Zoho Campaigns allows Cross-Site Scripting (XSS).This issue affects Zoho Campaigns: from n/a through 2.0.8.	2024-08-13	6.5	CVE-2024-38752 audit@patchstack.com
ZoneMinder--zoneminder	ZoneMinder is a free, open source closed-circuit television software application. ZoneMinder has a cross-site scripting vulnerability in the filter view via the filter[Id]. This vulnerability is fixed in 1.36.34 and 1.37.61.	2024-08-12	6.1	CVE-2024-43358 security-advisories@github.com security-advisories@github.com security-advisories@github.com
Zoom Communications Inc.--Zoom	Sensitive information exposure in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow an authenticated user to conduct an information disclosure via network access.	2024-08-14	6.5	CVE-2024-39822 security@zoom.us

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers				
Zoom Communications Inc.--Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers	Buffer overflow in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow an authenticated user to conduct a denial of service via network access.	2024-08-14	6.5	CVE-2024-42436 security@zoom.us
Zoom Communications Inc.--Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers	Buffer overflow in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow an authenticated user to conduct a denial of service via network access.	2024-08-14	6.5	CVE-2024-42437 security@zoom.us
Zoom Communications Inc.--Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers	Buffer overflow in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow an authenticated user to conduct a denial of service via network access.	2024-08-14	6.5	CVE-2024-42438 security@zoom.us
Zoom Communications Inc.--Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers	Sensitive information disclosure in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow a privileged user to conduct an information disclosure via network access.	2024-08-14	4.9	CVE-2024-39823 security@zoom.us
Zoom Communications Inc.--Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers	Sensitive information disclosure in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow a privileged user to conduct an information disclosure via network access.	2024-08-14	4.9	CVE-2024-39824 security@zoom.us
Zoom Communications Inc.--Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers	Sensitive information disclosure in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow a privileged user to conduct an information disclosure via network access.	2024-08-14	4.9	CVE-2024-42434 security@zoom.us

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Zoom Communications Inc.--Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers	Sensitive information disclosure in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow a privileged user to conduct an information disclosure via network access.	2024-08-14	4.9	CVE-2024-42435 security@zoom.us
Zoom Communications Inc.--Zoom Workplace Desktop App for macOS and Zoom Meeting SDK for macOS	Untrusted search path in the installer for Zoom Workplace Desktop App for macOS and Zoom Meeting SDK for macOS before 6.1.0 may allow a privileged user to conduct an escalation of privilege via local access.	2024-08-14	6.5	CVE-2024-42439 security@zoom.us
Zoom Communications Inc.--Zoom Workplace Desktop App for macOS, Zoom Meeting SDK for macOS, Zoom Rooms Client for macOS	Improper privilege management in the installer for Zoom Workplace Desktop App for macOS, Zoom Meeting SDK for macOS and Zoom Rooms Client for macOS before 6.1.5 may allow a privileged user to conduct an escalation of privilege via local access.	2024-08-14	6.2	CVE-2024-42440 security@zoom.us
Zoom Communications Inc.--Zoom Workplace Desktop App for macOS, Zoom Meeting SDK for macOS, Zoom Rooms Client for macOS	Improper privilege management in the installer for Zoom Workplace Desktop App for macOS, Zoom Meeting SDK for macOS and Zoom Rooms Client for macOS before 6.1.5 may allow a privileged user to conduct an escalation of privilege via local access.	2024-08-14	6.2	CVE-2024-42441 security@zoom.us
zvijerka--Admission AppManager	The Admission AppManager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'q' parameter in versions up to, and including, 1.0.0 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.	2024-08-17	6.1	CVE-2023-4507 security@wordfence.com security@wordfence.com

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dell--PowerEdge Platform	Dell PowerEdge Platform, 14G Intel BIOS version(s) prior to 2.22.x, contains an Access of Memory Location After End of Buffer vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2024-08-29	3.8	CVE-2024-38304 security_alert@emc.com
HM Courts & Tribunals Service--Probate Back Office	A vulnerability was found in HM Courts & Tribunals Service Probate Back Office up to c1afe0cdb2b2766d9e24872c4e827f8b82a6cd31. It has been classified as problematic. Affected is an unknown function of the file src/main/java/uk/gov/hmcts/probate/service/NotificationService.java of the component Markdown Handler. The manipulation leads to injection. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The patch is identified as d90230d7cf575e5b0852d56660104c8bd2503c34. It is recommended to apply a patch to fix this issue.	2024-09-01	3.5	CVE-2024-8367 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
hwameistor--hwameistor	Hwameistor is an HA local storage system for cloud-native stateful workloads. This ClusterRole has * verbs of * resources. If a malicious user can access the worker node which has hwameistor's deployment, he/she can abuse these excessive permissions to do whatever he/she likes to the whole cluster, resulting in a cluster-level privilege escalation. This issue has been patched in version 0.14.6. All users are advised to upgrade. Users unable to upgrade should update and limit the ClusterRole using security-role.	2024-08-28	2.8	CVE-2024-45054 security-advisories@github.com security-advisories@github.com security-advisories@github.com security-advisories@github.com
n/a--Grocy	A vulnerability classified as problematic was found in Grocy up to 4.2.0. This vulnerability affects unknown code of the file /api/files/recipepictures/ of the component SVG File Upload Handler. The manipulation of the argument force_serve_as with the input picture' leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. NOTE: The project maintainer explains that "this is 'nonsense' and practically irrelevant according to the project's security policy" which expects additional authentication for the software.	2024-09-01	3.5	CVE-2024-8370 cna@vuldb.com cna@vuldb.com cna@vuldb.com
n/a--n/a	A Cross-Site Request Forgery (CSRF) vulnerability was found in Kashipara Music Management System v1.0 via /music/ajax.php?action=delete_playlist page.	2024-08-26	3.5	CVE-2024-42792 cve@mitre.org cve@mitre.org
n/a--n/a	A cross-site scripting (XSS) vulnerability in the component admin_datarelate.php of SeaCMS v12.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	2024-08-30	3.5	CVE-2024-44918 cve@mitre.org
NVIDIA--NVIDIA CUDA Toolkit	NVIDIA CUDA Toolkit contains a vulnerability in command `cuobjdump` where a user may cause a crash by passing in a malformed ELF file. A successful exploit of this vulnerability may cause an out of bounds read in the unprivileged process memory which could lead to a limited denial of service.	2024-08-31	3.3	CVE-2024-0109 psirt@nvidia.com

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
silabs.com--SE Firmware	An application can be configured to block boot attempts after consecutive tamper resets are detected, which may not occur as expected. This is possible because the TAMPERRSTCAUSE register may not be properly updated when a level 4 tamper event (a tamper reset) occurs. This impacts Series 2 HSE-SVH devices, including xG23B, xG24B, xG25B, and xG28B, but does not impact xG21B. To mitigate this issue, upgrade to SE Firmware version 2.2.6 or later.	2024-08-29	2	CVE-2024-2502 product-security@silabs.com
SourceCodester--Contact Manager with Export to VCF	A vulnerability, which was classified as problematic, has been found in SourceCodester Contact Manager with Export to VCF 1.0. Affected by this issue is some unknown functionality of the file index.html. The manipulation of the argument contact_name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-30	3.5	CVE-2024-8337 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Yassine Idrissi--Maintenance & Coming Soon Redirect Animation	Incorrect Authorization vulnerability in Yassine Idrissi Maintenance & Coming Soon Redirect Animation allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Maintenance & Coming Soon Redirect Animation: from n/a through 2.1.3.	2024-08-29	3.7	CVE-2024-43944 audit@patchstack.com
AMD--AMD EPYC 7001 Series Processors	Insufficient access controls in ASP kernel may allow a privileged attacker with access to AMD signing keys and the BIOS menu or UEFI shell to map DRAM regions in protected areas,Â potentially leading to a loss of platform integrity.	2024-08-13	3.9	CVE-2021-26387 psirt@amd.com psirt@amd.com
AMD--AMD EPYC 7002 Series Processors	Insufficient input validation in the ABL may allow a privileged attacker with access to the BIOS menu or UEFI shell to tamper with the structure headers in SPI ROM causing an out of bounds memory read and write, potentially resulting in memory corruption or denial of service.	2024-08-13	3.9	CVE-2021-46772 psirt@amd.com psirt@amd.com psirt@amd.com
AMD--AMD EPYC 9004 Series Processors	Incomplete cleanup in the ASP may expose the Master Encryption Key (MEK) to a privileged attacker with access to the BIOS menu or UEFI shell and a memory exfiltration vulnerability, potentially resulting in loss of confidentiality.	2024-08-13	1.9	CVE-2023-20518 psirt@amd.com psirt@amd.com
AMD--AMD Radeon RX 6000 Series Graphics Cards	An insufficient bounds check in PMFW (Power Management Firmware) may allow an attacker to utilize a malicious VF (virtualization function) to send a malformed message, potentially resulting in a denial of service.	2024-08-13	3.3	CVE-2023-20513 psirt@amd.com
AMD--AMD Radeon RX 6000 Series Graphics Cards	Improper input validation in SMU may allow an attacker with privileges and a compromised physical function (PF) Â Â to modify the PCIeÂ® lane count and speed, potentially leading to a loss of availability.	2024-08-13	2.3	CVE-2023-31304 psirt@amd.com
AMD--AMD Radeon RX 6000 Series Graphics Cards	Improper validation of array index in Power Management Firmware (PMFW) may allow a privileged attacker to cause an out-of-bounds memory read within PMFW, potentially leading to a denial of service.	2024-08-13	2.3	CVE-2023-31307 psirt@amd.com
AMD--AMD Radeon RX 6000 Series Graphics Cards	A hardcoded AES key in PMFW may result in a privileged attacker gaining access to the key, potentially resulting in internal debug information leakage.	2024-08-13	1.9	CVE-2023-20512 psirt@amd.com

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
AMD--AMD Radeon RX 6000 Series Graphics Cards	Generation of weak and predictable Initialization Vector (IV) in PMFW (Power Management Firmware) may allow an attacker with privileges to reuse IV values to reverse-engineer debug data, potentially resulting in information disclosure.	2024-08-13	1.9	CVE-2023-31305 psirt@amd.com
AMD--Prof Tool	Improper input validation in AMD Î¼Prof could allow an attacker to perform a write to an invalid address, potentially resulting in denial of service.	2024-08-13	3.3	CVE-2023-31366 psirt@amd.com
CodeAstro--Online Railway Reservation System	A vulnerability, which was classified as problematic, was found in CodeAstro Online Railway Reservation System 1.0. Affected is an unknown function of the file /admin/admin-add-employee.php of the component Add Employee Page. The manipulation of the argument emp_fname /emp_lname /emp_nat_idno/emp_addr 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.	2024-08-15	2.4	CVE-2024-7814 cna@vuldb.com cna@vuldb.com cna@vuldb.com
CodeAstro--Online Railway Reservation System	A vulnerability has been found in CodeAstro Online Railway Reservation System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/admin-update-employee.php of the component Update Employee Page. The manipulation of the argument emp_fname /emp_lname /emp_nat_idno/emp_addr leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	2.4	CVE-2024-7815 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Fortinet--FortiPAM	An insufficient session expiration vulnerability [CWE-613] vulnerability in FortiOS 7.2.5 and below, 7.0 all versions, 6.4 all versions; FortiProxy 7.2 all versions, 7.0 all versions; FortiPAM 1.3 all versions, 1.2 all versions, 1.1 all versions, 1.0 all versions; FortiSwitchManager 7.2.1 and below, 7.0 all versions GUI may allow attackers to re-use websessions after GUI logout, should they manage to acquire the required credentials.	2024-08-13	3.7	CVE-2022-45862 psirt@fortinet.com
JetBrains--TeamCity	In JetBrains TeamCity before 2024.07.1 self XSS was possible in the HashiCorp Vault plugin	2024-08-16	3.7	CVE-2024-43808 cve@jetbrains.com
JetBrains--TeamCity	In JetBrains TeamCity before 2024.07.1 reflected XSS was possible on the agentPushPreset page	2024-08-16	3.5	CVE-2024-43809 cve@jetbrains.com
N-able--Ecosystem Agent	Ecosystem Agent version 4 < 4.5.1.2597 and Ecosystem Agent version 5 < 5.1.4.2473 did not properly validate SSL/TLS certificates, which could allow a malicious actor to perform a Man-in-the-Middle and intercept traffic between the agent and N-able servers from a privileged network position.	2024-08-12	3.8	CVE-2024-5445 a5532a13-c4dd-4202-bef1-e0b8f2f8d12b a5532a13-c4dd-4202-bef1-e0b8f2f8d12b a5532a13-c4dd-4202-bef1-e0b8f2f8d12b
n/a--FastCMS	A vulnerability, which was classified as problematic, was found in FastCMS up to 0.1.5. Affected is an unknown function of the component New Article Category Page. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2024-08-13	3.5	CVE-2024-7733 cna@vuldb.com cna@vuldb.com cna@vuldb.com
n/a--Intel(R) CSME	Improper initialization in firmware for some Intel(R) CSME may allow a privileged user to potentially enable information disclosure via local access.	2024-08-14	2.3	CVE-2023-48361 secure@intel.com

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--Intel(R) Distribution for GDB software	Improper input validation for some Intel(R) Distribution for GDB software before version 2024.0.1 may allow an authenticated user to potentially enable denial of service via local access.	2024-08-14	2.2	CVE-2024-24973 secure@intel.com
n/a--LimeSurvey	A vulnerability was found in LimeSurvey 6.3.0-231016 and classified as problematic. Affected by this issue is some unknown functionality of the file /index.php of the component File Upload. The manipulation of the argument size leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-17	2.7	CVE-2024-7887 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
n/a--Scada-LTS	A vulnerability has been found in Scada-LTS 2.7.8 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /Scada-LTS/app.shtm#/alarms/Scada of the component Message Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-17	3.5	CVE-2024-7901 cna@vuldb.com cna@vuldb.com cna@vuldb.com
Red Hat--Red Hat Enterprise Linux 6	A NULL pointer dereference flaw was found in the ub_ctx_set_fwd function in Unbound. This issue could allow an attacker who can invoke specific sequences of API calls to cause a segmentation fault. When certain API functions such as ub_ctx_set_fwd and ub_ctx_resolvconf are called in a particular order, the program attempts to read from a NULL pointer, leading to a crash. This issue can result in a denial of service by causing the application to terminate unexpectedly.	2024-08-12	2.8	CVE-2024-43167 secalert@redhat.com secalert@redhat.com secalert@redhat.com secalert@redhat.com
SAP_SE--SAP BusinessObjects Business Intelligence Platform	SAP BusinessObjects Business Intelligence Platform allows an authenticated attacker to upload malicious code over the network, that could be executed by the application. On successful exploitation, the attacker can cause a low impact on the Integrity of the application.	2024-08-13	3.7	CVE-2024-28166 cna@sap.com cna@sap.com
SAP_SE--SAP BusinessObjects Business Intelligence Platform	SAP BusinessObjects Business Intelligence Platform allows an authenticated attacker to upload malicious code over the network, that could be executed by the application. On successful exploitation, the attacker can cause a low impact on the Integrity of the application.	2024-08-13	3.1	CVE-2024-41731 cna@sap.com cna@sap.com
siemens -- sinec_nms	A vulnerability has been identified in SINEC NMS (All versions < V3.0). The importCertificate function of the SINEC NMS Control web application contains a path traversal vulnerability. This could allow an authenticated attacker it to delete arbitrary certificate files on the drive SINEC NMS is installed on.	2024-08-13	3.8	CVE-2024-41938 productcert@siemens.com
smub--Easy Digital Downloads eCommerce Payments and Subscriptions made easy	The Easy Digital Downloads - Sell Digital Files & Subscriptions (eCommerce Store + Payments Made Easy) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Agreement Text value in all versions up to, and including, 3.3.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, 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.	2024-08-12	3.3	CVE-2024-6692 security@wordfence.com security@wordfence.com
SourceCodester--Best House Rental Management	A vulnerability classified as problematic was found in SourceCodester Best House Rental Management System 1.0. This vulnerability affects unknown code of the file /rental_0/rental/ajax.php?action=save_tenant of the component POST Parameter	2024-08-15	3.5	CVE-2024-7812 cna@vuldb.com cna@vuldb.com

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
System	Handler. The manipulation of the argument lastname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.			cna@vuldb.com cna@vuldb.com
SourceCodester--Kortex Lite Advocate Office Management System	A vulnerability classified as problematic has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected is an unknown function of the file addcase_stage.php. The manipulation of the argument cname 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.	2024-08-12	3.5	CVE-2024-7683 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Kortex Lite Advocate Office Management System	A vulnerability classified as problematic was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected by this vulnerability is an unknown functionality of the file add_act.php. The manipulation of the argument aname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	3.5	CVE-2024-7684 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Kortex Lite Advocate Office Management System	A vulnerability, which was classified as problematic, has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected by this issue is some unknown functionality of the file adds.php. The manipulation of the argument name/dob/email/mobile/address leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-12	3.5	CVE-2024-7685 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Kortex Lite Advocate Office Management System	A vulnerability, which was classified as problematic, was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This affects an unknown part of the file register_case.php. The manipulation of the argument title/description/opposite_lawyer 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.	2024-08-12	3.5	CVE-2024-7686 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Online Graduate Tracer System	A vulnerability has been found in SourceCodester Online Graduate Tracer System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /tracking/admin/add_acc.php. The manipulation of the argument name/user/position leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-15	3.5	CVE-2024-7844 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Task Progress Tracker	A vulnerability was found in SourceCodester Task Progress Tracker 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /endpoint/add-task.php. The manipulation of the argument task_name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2024-08-14	3.5	CVE-2024-7793 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
SourceCodester--Yoga Class Registration System	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/inquiries/view_inquiry.php. The manipulation of the argument message leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-08-16	3.5	CVE-2024-7852 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
xiaohe4966--TpMeCMS	A vulnerability, which was classified as problematic, was found in xiaohe4966 TpMeCMS 1.3.3.2. Affected is an unknown function of the file /h.php/general/config?ref=addtabs of the component Basic Configuration Handler. The manipulation of the argument Site Name/Beian/Contact address/copyright/technical support 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. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-17	2.4	CVE-2024-7900 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
yzane--vscode-markdown-pdf	A vulnerability, which was classified as problematic, has been found in yzane vscode-markdown-pdf 1.5.0. Affected by this issue is some unknown functionality of the component Markdown File Handler. The manipulation leads to pathname traversal. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used.	2024-08-13	3.3	CVE-2024-7738 cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com cna@vuldb.com
Zabbix--Zabbix	Zabbix allows to configure SMS notifications. AT command injection occurs on "Zabbix Server" because there is no validation of "Number" field on Web nor on Zabbix server side. Attacker can run test of SMS providing specially crafted phone number and execute additional AT commands on modem.	2024-08-12	3	CVE-2024-22122 security@zabbix.com
Zabbix--Zabbix	Setting SMS media allows to set GSM modem file. Later this file is used as Linux device. But due everything is a file for Linux, it is possible to set another file, e.g. log file and zabbix_server will try to communicate with it as modem. As a result, log file will be broken with AT commands and small part for log file content will be leaked to UI.	2024-08-12	2.7	CVE-2024-22123 security@zabbix.com