BULLETIN (SB24-218)

VULNERABILITY SUMMARY FOR THE MONTH OF

JULY, 2024

Bulletin (SB24-218)
Vulnerability Summary for the Month of July, 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
2code -- wpqa_builder	The WPQA Builder WordPress plugin before 6.1.1 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	2024-07-03	8.8	CVE-2024-2376
ABB--ASPECT Enterprise (ASP-ENT-x)	Default credential in install package in ABB ASPECT; NEXUS Series; MATRIX Series version 3.07 allows attacker to login to product instances wrongly configured.	2024-07-01	8.8	CVE-2024-4007
Adobe--Acrobat for Edge	Acrobat for Edge versions 126.0.2592.68 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.	2024-07-02	7.8	CVE-2024-34122
aimeos--ai-admin-graphql	aimeos/ai-admin-graphql is the Aimeos GraphQL API admin interface. Starting in version 2022.04.01 and prior to versions 2022.10.10, 2023.10.6, and 2024.04.6, an improper access control vulnerability allows an editor to modify and take over an admin account in the back end. Versions 2022.10.10, 2023.10.6, and 2024.04.6 fix this issue.	2024-07-02	7.1	CVE-2024-39323
Apache Software Foundation--Apache HTTP Server	Potential SSRF in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to cause unsafe RewriteRules to unexpectedly setup URL's to be handled by mod_proxy. Users are recommended to upgrade to version 2.4.60, which fixes this issue.	2024-07-01	7.5	CVE-2024-39573
Arm Ltd--Valhall GPU Firmware	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in Arm Ltd Valhall GPU Firmware, Arm Ltd Arm 5th Gen GPU Architecture Firmware allows a local non-privileged user to make improper GPU processing operations to access a limited amount outside of buffer bounds. If the operations are carefully prepared, then this in turn could give them access to all system memory. This issue affects Valhall GPU Firmware: from r29p0 through r46p0; Arm 5th Gen GPU Architecture Firmware: from r41p0 through r46p0.	2024-07-01	7.8	CVE-2024-0153
certifi--python-certifi	Certifi is a curated collection of Root Certificates for validating the trustworthiness of SSL certificates while verifying the identity of TLS hosts. Certifi starting in 2021.05.30 and prior to 2024.07.4 recognized root certificates from `GLOBALTRUST`. Certifi 2024.07.04 removes root certificates from `GLOBALTRUST` from the root store. These are in the process of being removed from Mozilla's trust store. `GLOBALTRUST`'s root certificates are being removed pursuant to an investigation which identified "long-running and unresolved compliance issues."	2024-07-05	7.5	CVE-2024-39689
CHANGING--Mobile One Time Password	CHANGING Mobile One Time Password's uploading function in a hidden page does not filter file type properly. Remote attackers with administrator privilege can exploit this vulnerability to upload and run malicious file to execute system commands.	2024-07-01	7.2	CVE-2024-3123
CocoaPods--CocoaPods	trunk.cocoapods.org is the authentication server for the CoacoaPods dependency manager. The part of trunk which verifies whether a user has a real email address on signup used a rfc-822 library which executes a shell command to validate the email domain MX records validity. It works via an DNS MX. This lookup could be manipulated to also execute a command on the trunk server, effectively giving root access to the server and the infrastructure. This issue was patched server-side with commit 001cc3a430e75a16307f5fd6cdff1363ad2f40f3 in September 2023. This RCE triggered a full user-session reset, as an attacker could have used this method to write to any Podspec in trunk.	2024-07-01	10	CVE-2024-38366
CocoaPods--CocoaPods	trunk.cocoapods.org is the authentication server for the CoacoaPods dependency manager. A vulnerability affected older pods which migrated from the pre-2014 pull request workflow to trunk. If the pods had never been claimed then it was still possible to do so. It was also possible to have all owners removed from a pod, and that made the pod available for the same claiming system. This was patched server-side in commit 71be5440906b6bdfbc0bcc7f8a9fec33367ea0f4 in September 2023.	2024-07-01	9.3	CVE-2024-38368
CocoaPods--CocoaPods	trunk.cocoapods.org is the authentication server for the CoacoaPods dependency manager. Prior to commit d4fa66f49cedab449af9a56a21ab40697b9f7b97, the trunk sessions verification step could be manipulated for owner session hijacking Compromising a victim's session will result in a full takeover of the CocoaPods trunk account. The threat actor could manipulate their pod specifications, disrupt the distribution of legitimate libraries, or cause widespread disruption within the CocoaPods ecosystem. This was patched server-side with commit d4fa66f49cedab449af9a56a21ab40697b9f7b97 in October 2023.	2024-07-01	8.2	CVE-2024-38367

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dahlia--fedify	Fedify is a TypeScript library for building federated server apps powered by ActivityPub and other standards. At present, when Fedify needs to retrieve an object or activity from a remote activitypub server, it makes a HTTP request to the `@id` or other resources present within the activity it has received from the web. This activity could reference an `@id` that points to an internal IP address, allowing an attacker to send request to resources internal to the fedify server's network. This applies to not just resolution of documents containing activities or objects, but also to media URLs as well. Specifically this is a Server Side Request Forgery attack. Users should upgrade to Fedify version 0.9.2, 0.10.1, or 0.11.1 to receive a patch for this issue.	2024-07-05	7.2	CVE-2024-39687
Delinea--Centrify PAS	Vulnerability in Delinea Centrify PAS v. 21.3 and possibly others. The application is prone to the path traversal vulnerability allowing arbitrary files reading outside the web publish directory. Versions 23.1-HF7 and on have the patch.	2024-07-02	7.7	CVE-2024-5865
dell -- powerscale_onefs	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.0 contain use of a broken or risky cryptographic algorithm vulnerability. An unprivileged network malicious attacker could potentially exploit this vulnerability, leading to data leaks.	2024-07-02	7.5	CVE-2024-32852
dell -- powerscale_onefs	Dell PowerScale OneFS versions 8.2.2.x through 9.7.0.2 contain an execution with unnecessary privileges vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to escalation of privileges.	2024-07-02	7.8	CVE-2024-32853
discourse-- discourse	Discourse is an open-source discussion platform. Prior to version 3.2.3 on the `stable` branch and version 3.3.0.beta3 on the `tests-passed` branch, Oneboxing against a carefully crafted malicious URL can reduce the availability of a Discourse instance. The problem has been patched in version 3.2.3 on the `stable` branch and version 3.3.0.beta3 on the `tests-passed` branch. There are no known workarounds available for this vulnerability.	2024-07-03	7.5	CVE-2024-35227
Edito--Edito CMS	Web services managed by Edito CMS (Content Management System) in versions from 3.5 through 3.25 leak sensitive data as they allow downloading configuration files by an unauthenticated user. The issue in versions 3.5 - 3.25 was removed in releases which dates from 10th of January 2014. Higher versions were never affected.	2024-07-02	7.5	CVE-2024-4836 cvd@cert.pl cvd@cert.pl cvd@cert.pl
evmos--evmos	Evmos is a decentralized Ethereum Virtual Machine chain on the Cosmos Network. Prior to version 19.0.0, a user can create a vesting account with a 3rd party account (EOA or contract) as funder. Then, this user can create an authorization for the contract.CallerAddress, this is the authorization checked in the code. But the funds are taken from the funder address provided in the message. Consequently, the user can fund a vesting account with a 3rd party account without its permission. The funder address can be any address, so this vulnerability can be used to drain all the accounts in the chain. The issue has been patched in version 19.0.0.	2024-07-05	8.8	CVE-2024-39696
expresstech -- quiz_and_survey_ master	The Quiz and Survey Master (QSM) WordPress plugin before 9.0.2 is vulnerable does not validate and escape the question_id parameter in the qsm_bulk_delete_question_from_database AJAX action, leading to a SQL injection exploitable by Contributors and above role	2024-07-02	8.8	CVE-2024-5606
flowiseai -- flowise	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, the `/api/v1/openai-assistants-file` endpoint in `index.ts` is vulnerable to arbitrary file read due to lack of sanitization of the `fileName` body parameter. No known patches for this issue are available.	2024-07-01	7.5	CVE-2024-36420
flowiseai -- flowise	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, A CORS misconfiguration sets the Access-Control-Allow-Origin header to all, allowing arbitrary origins to connect to the website. In the default configuration (unauthenticated), arbitrary origins may be able to make requests to Flowise, stealing information from the user. This CORS misconfiguration may be chained with the path injection to allow an attacker attackers without access to Flowise to read arbitrary files from the Flowise server. As of time of publication, no known patches are available.	2024-07-01	7.5	CVE-2024-36421
geoserver -- geoserver	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.23.6, 2.24.4, and 2.25.2, multiple OGC request parameters allow Remote Code Execution (RCE) by unauthenticated users through specially crafted input against a default GeoServer installation due to unsafely evaluating property names as XPath expressions. The GeoTools library API that GeoServer calls evaluates property/attribute names for feature types in a way that unsafely passes them to the commons-jxpath library which can execute arbitrary code when evaluating XPath expressions. This XPath evaluation is intended to be used only by complex feature types (i.e., Application Schema data stores) but is incorrectly being applied to simple feature types as well which makes this vulnerability apply to **ALL** GeoServer instances. No public PoC is provided but this vulnerability has	2024-07-01	9.8	CVE-2024-36401

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	been confirmed to be exploitable through WFS GetFeature, WFS GetPropertyValue, WMS GetMap, WMS GetFeatureInfo, WMS GetLegendGraphic and WPS Execute requests. This vulnerability can lead to executing arbitrary code. Versions 2.23.6, 2.24.4, and 2.25.2 contain a patch for the issue. A workaround exists by removing the `gt-complex-x.y.jar` file from the GeoServer where `x.y` is the GeoTools version (e.g., `gt-complex-31.1.jar` if running GeoServer 2.25.1). This will remove the vulnerable code from GeoServer but may break some GeoServer functionality or prevent GeoServer from deploying if the gt-complex module is needed.			
geoserver--geoserver	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.23.5 and 2.24.3, if GeoServer is deployed in the Windows operating system using an Apache Tomcat web application server, it is possible to bypass existing input validation in the GeoWebCache ByteStreamController class and read arbitrary classpath resources with specific file name extensions. If GeoServer is also deployed as a web archive using the data directory embedded in the `geoserver.war` file (rather than an external data directory), it will likely be possible to read specific resources to gain administrator privileges. However, it is very unlikely that production environments will be using the embedded data directory since, depending on how GeoServer is deployed, it will be erased and re-installed (which would also reset to the default password) either every time the server restarts or every time a new GeoServer WAR is installed and is therefore difficult to maintain. An external data directory will always be used if GeoServer is running in standalone mode (via an installer or a binary). Versions 2.23.5 and 2.24.3 contain a patch for the issue. Some workarounds are available. One may change from a Windows environment to a Linux environment; or change from Apache Tomcat to Jetty application server. One may also disable anonymous access to the embeded GeoWebCache administration and status pages.	2024-07-01	7.5	CVE-2024-24749
geotools--geotools	GeoTools is an open source Java library that provides tools for geospatial data. Prior to versions 31.2, 30.4, and 29.6, Remote Code Execution (RCE) is possible if an application uses certain GeoTools functionality to evaluate XPath expressions supplied by user input. Versions 31.2, 30.4, and 29.6 contain a fix for this issue. As a workaround, GeoTools can operate with reduced functionality by removing the `gt-complex` jar from one's application. As an example of the impact, application schema `datastore` would not function without the ability to use XPath expressions to query complex content. Alternatively, one may utilize a drop-in replacement GeoTools jar from SourceForge for versions 31.1, 30.3, 30.2, 29.2, 28.2, 27.5, 27.4, 26.7, 26.4, 25.2, and 24.0. These jars are for download only and are not available from maven central, intended to quickly provide a fix to affected applications.	2024-07-02	9.8	CVE-2024-36404
gofiber--fiber	Fiber is an Express-inspired web framework written in Go A vulnerability present in versions prior to 2.52.5 is a session middleware issue in GoFiber versions 2 and above. This vulnerability allows users to supply their own session_id value, resulting in the creation of a session with that key. If a website relies on the mere presence of a session for security purposes, this can lead to significant security risks, including unauthorized access and session fixation attacks. All users utilizing GoFiber's session middleware in the affected versions are impacted. The issue has been addressed in version 2.52.5. Users are strongly encouraged to upgrade to version 2.52.5 or higher to mitigate this vulnerability. Users who are unable to upgrade immediately can apply the following workarounds to reduce the risk: Either implement additional validation to ensure session IDs are not supplied by the user and are securely generated by the server, or regularly rotate session IDs and enforce strict session expiration policies.	2024-07-01	10	CVE-2024-38513
gorilla--schema	gorilla/schema converts structs to and from form values. Prior to version 1.4.1 Running `schema.Decoder.Decode()` on a struct that has a field of type `[]struct{...}` opens it up to malicious attacks regarding memory allocations, taking advantage of the sparse slice functionality. Any use of `schema.Decoder.Decode()` on a struct with arrays of other structs could be vulnerable to this memory exhaustion vulnerability. Version 1.4.1 contains a patch for the issue.	2024-07-01	7.5	CVE-2024-37298
Grandstream--GXP2135	An os command injection vulnerability exists in the CWMP SelfDefinedTimeZone functionality of Grandstream GXP2135 1.0.9.129, 1.0.11.74 and 1.0.11.79. A specially crafted network packet can lead to arbitrary command execution. An attacker can send a sequence of malicious packets to trigger this vulnerability.	2024-07-03	8.1	CVE-2024-32937

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Hitachi--JP1/Extensible SNMP Agent for Windows	Incorrect Default Permissions vulnerability in Hitachi JP1/Extensible SNMP Agent for Windows, Hitachi JP1/Extensible SNMP Agent on Windows, Hitachi Job Management Partner1/Extensible SNMP Agent on Windows allows File Manipulation.This issue affects JP1/Extensible SNMP Agent for Windows: from 12-00 before 12-00-01, from 11-00 through 11-00-*; JP1/Extensible SNMP Agent: from 10-10 through 10-10-01, from 10-00 through 10-00-02, from 09-00 through 09-00-04; Job Management Partner1/Extensible SNMP Agent: from 10-10 through 10-10-01, from 10-00 through 10-00-02, from 09-00 through 09-00-04.	2024-07-02	7.8	CVE-2024-4679
home_owners_collection_management_system_project -- home_owners_collection_management_system	A vulnerability was found in SourceCodester Home Owners Collection Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /classes/Users.php?f=save. The manipulation of the argument img leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-270167.	2024-07-02	9.8	CVE-2024-6439
home_owners_collection_management_system_project -- home_owners_collection_management_system	A vulnerability was found in SourceCodester Home Owners Collection Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /classes/Master.php?f=delete_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. The identifier of this vulnerability is VDB-270168.	2024-07-02	9.8	CVE-2024-6440
icegram -- email_subscribers_\&_newsletters	The Email Subscribers by Icegram Express - Email Marketing, Newsletters, Automation for WordPress & WooCommerce plugin for WordPress is vulnerable to time-based SQL Injection via the db parameter in all versions up to, and including, 5.7.25 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-07-02	9.8	CVE-2024-6172
ICONICS--GENESIS64	Uncontrolled Search Path Element vulnerability in ICONICS GENESIS64 all versions, Mitsubishi Electric GENESIS64 all versions and Mitsubishi Electric MC Works64 all versions allows a local attacker to execute a malicious code by storing a specially crafted DLL in a specific folder when GENESIS64 and MC Works64 are installed with the Pager agent in the alarm multi-agent notification feature.	2024-07-04	7	CVE-2024-1182
Johnson Controls--American Dynamics Illustra Essentials Gen 4	Under certain circumstances the web interface will accept characters unrelated to the expected input.	2024-07-02	9.1	CVE-2024-32755
jungo -- windriver	Improper privilege management in Jungo WinDriver before 12.1.0 allows local attackers to escalate privileges and execute arbitrary code.	2024-07-02	7.8	CVE-2023-51776
jungo -- windriver	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges, execute arbitrary code, or cause a Denial of Service (DoS).	2024-07-02	7.8	CVE-2024-22106
jungo -- windriver	Improper privilege management in Jungo WinDriver before 12.2.0 allows local attackers to escalate privileges and execute arbitrary code.	2024-07-02	7.8	CVE-2024-25086
jungo -- windriver	Improper privilege management in Jungo WinDriver before 12.5.1 allows local attackers to escalate privileges and execute arbitrary code.	2024-07-02	7.8	CVE-2024-25088
jungo -- windriver	Improper privilege management in Jungo WinDriver 6.0.0 through 16.1.0 allows local attackers to escalate privileges and execute arbitrary code.	2024-07-02	7.8	CVE-2024-26314
Juniper Networks--Junos OS	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). If an SRX Series device receives specific valid traffic destined to the device, it will cause the PFE to crash and restart. Continued receipt and processing of this traffic will create a sustained DoS condition. This issue affects Junos OS on SRX Series: * 21.4 versions before 21.4R3-S7.9, * 22.1 versions before 22.1R3-S5.3, * 22.2 versions before 22.2R3-S4.11, * 22.3 versions before 22.3R3, * 22.4 versions before 22.4R3. Junos OS versions prior to 21.4R1 are not affected by this issue.	2024-07-01	7.5	CVE-2024-21586

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Kiloview--P1/P2	Inadequate input validation exposes the system to potential remote code execution (RCE) risks. Attackers can exploit this vulnerability by appending shell commands to the Speed-Measurement feature, enabling unauthorized code execution.	2024-07-02	10	CVE-2023-41917
Kiloview--P1/P2	A vulnerability allows unauthorized access to functionality inadequately constrained by ACLs. Attackers may exploit this to unauthenticated execute commands potentially leading to unauthorized data manipulation, access to privileged functions, or even the execution of arbitrary code.	2024-07-02	10	CVE-2023-41918
Kiloview--P1/P2	Hardcoded credentials are discovered within the application's source code, creating a potential security risk for unauthorized access.	2024-07-02	9.8	CVE-2023-41919
Kiloview--P1/P2	The vulnerability allows attackers access to the root account without having to authenticate. Specifically, if the device is configured with the IP address of 10.10.10.10, the root user is automatically logged in.	2024-07-02	9.8	CVE-2023-41920
Kiloview--P1/P2	A vulnerability allows attackers to download source code or an executable from a remote location and execute the code without sufficiently verifying the origin and integrity of the code. This vulnerability can allow attackers to modify the firmware before uploading it to the system, thus achieving the modification of the target's integrity to achieve an insecure state.	2024-07-02	9.8	CVE-2023-41921
Kiloview--P1/P2	The webserver utilizes basic authentication for its user login to the configuration interface. As encryption is disabled on port 80, it enables potential eavesdropping on user traffic, making it possible to intercept their credentials.	2024-07-02	8.8	CVE-2023-41926
Kiloview--P1/P2	The user management section of the web application permits the creation of user accounts with excessively weak passwords, including single-character passwords.	2024-07-02	7.2	CVE-2023-41923
kylephillips -- nested_pages	The Nested Pages plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.2.7. This is due to missing or incorrect nonce validation on the 'settingsPage' function and missing santization of the 'tab' parameter. This makes it possible for unauthenticated attackers to call local php files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-07-04	8.8	CVE-2024-5943
LA-Studio--LA-Studio Element Kit for Elementor	Local File Inclusion vulnerability in LA-Studio LA-Studio Element Kit for Elementor via "LaStudioKit Progress Bar" widget in New Post, specifically in the "progress_type" attribute.This issue affects LA-Studio Element Kit for Elementor: from n/a through 1.3.8.1.	2024-07-02	8.5	CVE-2024-37479
la-studioweb -- element_kit_for_elementor	The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.3.8.1 via the 'map_style' 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.	2024-07-02	8.8	CVE-2024-5349
livemeshelementor -- addons_for_elementor	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 8.3.7 via several of the plugin's widgets through the 'style' attribute. 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.	2024-07-04	8.8	CVE-2024-2385
mastodon--mastodon	Mastodon is a self-hosted, federated microblogging platform. Starting in version 2.6.0 and prior to versions 4.1.18 and 4.2.10, by crafting specific activities, an attacker can extend the audience of a post they do not own to other Mastodon users on a target server, thus gaining access to the contents of a post not intended for them. Versions 4.1.18 and 4.2.10 contain a patch for this issue.	2024-07-05	8.2	CVE-2024-37903
MediaTek, Inc.--MT2731, MT6739, MT6761, MT6762, MT6763, MT6765, MT6767, MT6768, MT6769, MT6771, MT8666, MT8667, MT8765, MT8766, MT8768, MT8781, MT8786, MT8788	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01297806; Issue ID: MSV-1481.	2024-07-01	7.5	CVE-2024-20076 security@mediatek.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
MediaTek, Inc.--MT2731, MT6739, MT6761, MT6762, MT6763, MT6765, MT6767, MT6768, MT6769, MT6771, MT8666, MT8667, MT8765, MT8766, MT8768, MT8781, MT8786, MT8788	In Modem, there is a possible system crash due to incorrect error handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01297807; Issue ID: MSV-1482.	2024-07-01	7.5	CVE-2024-20077 security@mediatek.com
MediaTek, Inc.--MT6768, MT6779, MT8321, MT8385, MT8755, MT8765, MT8766, MT8768, MT8771, MT8775, MT8781, MT8786, MT8788, MT8789, MT8791T, MT8792, MT8795T, MT8796, MT8797, MT8798	In venc, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08737250; Issue ID: MSV-1452.	2024-07-01	9.8	CVE-2024-20078 security@mediatek.com
mesbook -- mesbook	Information exposure vulnerability in MESbook 20221021.03 version, the exploitation of which could allow a local attacker, with user privileges, to access different resources by changing the API value of the application.	2024-07-03	7.1	CVE-2024-6426
mesbook -- mesbook	Uncontrolled Resource Consumption vulnerability in MESbookÂ 20221021.03 version. An unauthenticated remote attacker can use the "message" parameter to inject a payload with dangerous JavaScript code, causing the application to loop requests on itself, which could lead to resource consumption and disable the application.	2024-07-03	7.5	CVE-2024-6427
MESbook--MESbook	External server-side request vulnerability in MESbook 20221021.03 version, which could allow a remote, unauthenticated attacker to exploit the endpoint "/api/Proxy/Post?userName=&password=&uri=<FILE|INTERNAL URL|IP/HOST" or "/api/Proxy/Get?userName=&password=&uri=<ARCHIVO|URL INTERNA|IP/HOST" to read the source code of web files, read internal files or access network resources.	2024-07-01	9.3	CVE-2024-6424
MESbook--MESbook	Incorrect Provision of Specified Functionality vulnerability in MESbook 20221021.03 version. An unauthenticated remote attacker can register user accounts without being authenticated from the route "/account/Register/" and in the parameters "UserName=<RANDOMUSER>&Password=<PASSWORD>&ConfirmPassword=<PASSWORD-REPEAT>".	2024-07-01	9.1	CVE-2024-6425
Mitsubishi Electric Corporation--MELIPC Series MI5122-VW	Incorrect Default Permissions vulnerability in Smart Device Communication Gateway preinstalled on MELIPC Series MI5122-VW firmware versions "05" to "07" allows a local attacker to execute arbitrary code by saving a malicious file to a specific folder. As a result, the attacker may disclose, tamper with, destroy or delete information in the product, or cause a denial-of-service (DoS) condition on the product.	2024-07-04	8.8	CVE-2024-3904
mongodb -- compass	MongoDB Compass may be susceptible to code injection due to insufficient sandbox protection settings with the usage of ejson shell parser in Compass' connection handling. This issue affects MongoDB Compass versions prior to version 1.42.2	2024-07-01	9.8	CVE-2024-6376
MRW--MRW plugin	Information exposure vulnerability in the MRW plugin, in itsÂ 5.4.3 version,Â affecting the "mrw_log" functionality. This vulnerability could allow a remote attacker to obtain other customers' order information and access sensitive information such as name and phone number. This vulnerability also allows an attacker to create or overwrite shipping labels.	2024-07-04	8.2	CVE-2024-6506
mySCADA--myPRO	mySCADA myPRO uses a hard-coded password which could allow an attacker to remotely execute code on the affected device.	2024-07-02	9.8	CVE-2024-4708
N-able--N-central	The N-central server is vulnerable to an authentication bypass of the user interface. This vulnerability is present in all deployments of N-central prior to	2024-07-01	9.1	CVE-2024-28200

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2024.2. This vulnerability was discovered through internal N-central source code review and N-able has not observed any exploitation in the wild.			
N-able--N-central	The N-central server is vulnerable to session rebinding of already authenticated users when using Entra SSO, which can lead to authentication bypass. This vulnerability is present in all Entra-supported deployments of N-central prior to 2024.3.	2024-07-01	9.1	CVE-2024-5322
N/A--N/A	Command injection when ingesting a remote Kaggle dataset due to a lack of input sanitization in the ingest_kaggle() API	2024-07-04	8.1	CVE-2024-6507
n/a--n/a	rjrodger jsonic-next v2.12.1 was discovered to contain a prototype pollution via the function empty. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	9.8	CVE-2024-38993
n/a--n/a	ag-grid-community v31.3.2 and ag-grid-enterprise v31.3.2 were discovered to contain a prototype pollution via the _.mergeDeep function. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	9.8	CVE-2024-38996
n/a--n/a	cafebazaar hod v0.4.14 was discovered to contain a prototype pollution via the function request. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	9.8	CVE-2024-39015
n/a--n/a	agreejs shared v0.0.1 was discovered to contain a prototype pollution via the function mergeInternalComponents. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	9.8	CVE-2024-39017
n/a--n/a	Gradio v4.36.1 was discovered to contain a code injection vulnerability via the component /gradio/component_meta.py. This vulnerability is triggered via a crafted input.	2024-07-01	9.8	CVE-2024-39236
n/a--n/a	The built-in SSH server of Gogs through 0.13.0 allows argument injection in internal/ssh/ssh.go, leading to remote code execution. Authenticated attackers can exploit this by opening an SSH connection and sending a malicious --split-string env request if the built-in SSH server is activated. Windows installations are unaffected.	2024-07-04	9.9	CVE-2024-39930
n/a--n/a	Gogs through 0.13.0 allows deletion of internal files.	2024-07-04	9.9	CVE-2024-39931
n/a--n/a	Gogs through 0.13.0 allows argument injection during the previewing of changes.	2024-07-04	9.9	CVE-2024-39932
n/a--n/a	rejetto HFS (aka HTTP File Server) 3 before 0.52.10 on Linux, UNIX, and macOS allows OS command execution by remote authenticated users (if they have Upload permissions). This occurs because a shell is used to execute df (i.e., with execSync instead of spawnSync in child_process in Node.js).	2024-07-04	9.9	CVE-2024-39943
n/a--n/a	akbr patch-into v1.0.1 was discovered to contain a prototype pollution via the function patchInto. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	8.8	CVE-2024-38991
n/a--n/a	airvertco frappejs v0.0.11 was discovered to contain a prototype pollution via the function registerView. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	8.8	CVE-2024-38992
n/a--n/a	jrburke requirejs v2.3.6 was discovered to contain a prototype pollution via the function config. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	8.4	CVE-2024-38998
n/a--n/a	che3vinci c3/utils-1 1.0.131 was discovered to contain a prototype pollution via the function assign. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	8.1	CVE-2024-39016
n/a--n/a	An issue was discovered in HTTP2 in Qt before 5.15.18, 6.x before 6.2.13, 6.3.x through 6.5.x before 6.5.7, and 6.6.x through 6.7.x before 6.7.3. Code to make security-relevant decisions about an established connection may execute too early, because the encrypted() signal has not yet been emitted and processed..	2024-07-04	8.6	CVE-2024-39936
n/a--n/a	supOS 5.0 allows api/image/download?fileName=../ directory traversal for reading files.	2024-07-04	8.6	CVE-2024-39937
n/a--n/a	amoyjs amoy common v1.0.10 was discovered to contain a prototype pollution via the function extend. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	7.3	CVE-2024-38994
n/a--n/a	amoyjs amoy common v1.0.10 was discovered to contain a prototype pollution via the function setValue. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	7.3	CVE-2024-39003
n/a--n/a	Gogs through 0.13.0 allows argument injection during the tagging of a new release.	2024-07-04	7.7	CVE-2024-39933

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	Robotmk before 2.0.1 allows a local user to escalate privileges (e.g., to SYSTEM) if automated Python environment setup is enabled, because the "shared holotree usage" feature allows any user to edit any Python environment.	2024-07-04	7.8	CVE-2024-39934
openbsd -- openssh	A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead to sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.	2024-07-01	8.1	CVE-2024-6387
openharmony -- openharmony	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through out-of-bounds read and write.	2024-07-02	9.8	CVE-2024-36243
openharmony -- openharmony	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through out-of-bounds write.	2024-07-02	9.8	CVE-2024-36260
openharmony -- openharmony	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through use after free.	2024-07-02	9.8	CVE-2024-37030
openharmony -- openharmony	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through out-of-bounds write.	2024-07-02	9.8	CVE-2024-37077
openharmony -- openharmony	in OpenHarmony v4.0.0 and prior versions allow a remote attacker arbitrary code execution in pre-installed apps through out-of-bounds write.	2024-07-02	9.8	CVE-2024-37185

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
parse-community--parse-server	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. A vulnerability in versions prior to 6.5.7 and 7.1.0 allows SQL injection when Parse Server is configured to use the PostgreSQL database. The algorithm to detect SQL injection has been improved in versions 6.5.7 and 7.1.0. No known workarounds are available.	2024-07-01	9.8	CVE-2024-39309
pi-hole--pi-hole	Pi-hole is a DNS sinkhole that protects devices from unwanted content without installing any client-side software. A vulnerability in versions prior to 5.18.3 allows an authenticated user to make internal requests to the server via the `gravity_DownloadBlocklistFromUrl()` function. Depending on some circumstances, the vulnerability could lead to remote command execution. Version 5.18.3 contains a patch for this issue.	2024-07-05	8.5	CVE-2024-34361
playsms -- playsms	A vulnerability was found in playSMS 1.4.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /index.php?app=main&inc=feature_firewall&op=firewall_list of the component Template Handler. The manipulation of the argument IP address with the input {{`id`} leads to injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-270277 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-03	8.8	CVE-2024-6469
qualcomm -- 315_5g_iot_modem_firmware	Memory corruption while performing finish HMAC operation when context is freed by keymaster.	2024-07-01	7.8	CVE-2024-21461
qualcomm -- 315_5g_iot_modem_firmware	Memory corruption when IOMMU unmap operation fails, the DMA and anon buffers are getting released.	2024-07-01	7.8	CVE-2024-23373
qualcomm -- 9205_lte_modem_firmware	Memory corruption while processing key blob passed by the user.	2024-07-01	7.8	CVE-2024-21465
qualcomm -- 9205_lte_modem_firmware	Memory corruption when an invoke call and a TEE call are bound for the same trusted application.	2024-07-01	7.8	CVE-2024-21469
qualcomm -- apq8064au_firmware	Memory corruption when allocating and accessing an entry in an SMEM partition.	2024-07-01	7.8	CVE-2024-23368
qualcomm -- ar8035_firmware	INformation disclosure while handling Multi-link IE in beacon frame.	2024-07-01	7.5	CVE-2024-21457
qualcomm -- ar8035_firmware	Information disclosure while handling SA query action frame.	2024-07-01	7.5	CVE-2024-21458
qualcomm -- csr8811_firmware	Memory corruption during the secure boot process, when the `bootm` command is used, it bypasses the authentication of the kernel/rootfs image.	2024-07-01	7.8	CVE-2024-21482
qualcomm -- fastconnect_6200_firmware	Memory corruption while invoking IOCTL call for GPU memory allocation and size param is greater than expected size.	2024-07-01	7.8	CVE-2024-23372
qualcomm -- fastconnect_6200_firmware	Memory corruption while handling user packets during VBO bind operation.	2024-07-01	7.8	CVE-2024-23380
qualcomm -- fastconnect_7800_firmware	Information disclosure while parsing sub-IE length during new IE generation.	2024-07-01	7.5	CVE-2024-21466
Qualcomm, Inc.-- Snapdragon	Memory corruption while processing IOCTL handler in FastRPC.	2024-07-01	8.4	CVE-2023-43554

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Enterprise Linux 9	A flaw was found in the QEMU disk image utility (qemu-img) 'info' command. A specially crafted image file containing a `json:{}` value describing block devices in QMP could cause the qemu-img process on the host to consume large amounts of memory or CPU time, leading to denial of service or read/write to an existing external file.	2024-07-02	7.8	CVE-2024-4467
Red Lion Europe--mbNET.mini	A high privileged remote attacker canÂ execute arbitrary system commands via GET requests due to improper neutralization of special elements used in an OS command.	2024-07-03	7.2	CVE-2024-5672
Routing Release--Routing Release	Security check loophole in HAProxy release (in combination with routing release) in Cloud Foundry prior to v40.17.0 potentially allows bypass of mTLS authentication to applications hosted on Cloud Foundry.	2024-07-03	9	CVE-2024-37082
samsung -- android	Improper input validation in BLE prior to SMR Jul-2024 Release 1 allows adjacent attackers to trigger abnormal behavior.	2024-07-02	8.8	CVE-2024-20890
samsung -- android	Improper input validation in parsing and distributing RTCP packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability.	2024-07-02	8.8	CVE-2024-34593
samsung -- android	Improper access control in OneUIHome prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities. User interaction is required for triggering this vulnerability.	2024-07-02	7.8	CVE-2024-20888
samsung -- android	Improper access control in launchFullscreenIntent of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities.	2024-07-02	7.8	CVE-2024-20891
samsung -- android	Improper verification of signature in FilterProvider prior to SMR Jul-2024 Release 1 allows local attackers to execute privileged behaviors. User interaction is required for triggering this vulnerability.	2024-07-02	7.8	CVE-2024-20892
samsung -- android	Improper input validation in libmediaextractorservice.so prior to SMR Jul-2024 Release 1 allows local attackers to trigger memory corruption.	2024-07-02	7.8	CVE-2024-20893
samsung -- android	Improper input validation in copying data to buffer cache in libsaped prior to SMR Jul-2024 Release 1 allows local attackers to write out-of-bounds memory.	2024-07-02	7.8	CVE-2024-20901
samsung -- android	Improper access control in launchApp of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities.	2024-07-02	7.8	CVE-2024-34585
samsung -- android	Improper access control in clickAdapterItem of SystemUI prior to SMR Jul-2024 Release 1 allows local attackers to launch privileged activities.	2024-07-02	7.8	CVE-2024-34595
samsung -- smartthings	Improper authentication in SmartThings prior to version 1.8.17 allows remote attackers to bypass the expiration date for members set by the owner.	2024-07-02	7.5	CVE-2024-34596
sitetweet_project -- sitetweet	The sitetweet WordPress plugin through 0.2 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	2024-07-02	8.8	CVE-2024-5767
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.109 and 9.1.2308.207, an authenticated user could create an external lookup that calls a legacy internal function. The authenticated user could use this internal function to insert code into the Splunk platform installation directory. From there, the user could execute arbitrary code on the Splunk platform Instance.	2024-07-01	8	CVE-2024-36983
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 on Windows, an authenticated user could execute a specially crafted query that they could then use to serialize untrusted data. The attacker could use the query to execute arbitrary code.	2024-07-01	8.8	CVE-2024-36984
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10, a low-privileged user that does not hold the admin or power Splunk roles could cause a Remote Code Execution through an external lookup that references the "splunk_archiver" application.	2024-07-01	8.8	CVE-2024-36985
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312, an admin user could store and execute arbitrary JavaScript code in the browser context of another Splunk user through the conf-web/settings REST endpoint. This could potentially cause a persistent cross-site scripting (XSS) exploit.	2024-07-01	8.1	CVE-2024-36997
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.109 and 9.1.2308.207, an attacker could trigger a null pointer reference on the cluster/config REST endpoint, which could result in a crash of the Splunk daemon.	2024-07-01	7.5	CVE-2024-36982
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200, a low-privileged user that does not hold the admin or power Splunk roles could create notifications in Splunk Web Bulletin Messages that all users on the instance receive.	2024-07-01	7.1	CVE-2024-36989

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Splunk--Splunk Enterprise	In Splunk Enterprise on Windows versions below 9.2.2, 9.1.5, and 9.0.10, an attacker could perform a path traversal on the /modules/messaging/ endpoint in Splunk Enterprise on Windows. This vulnerability should only affect Splunk Enterprise on Windows.	2024-07-01	7.5	CVE-2024-36991
Theme-Ruby--Foxiz	Server-Side Request Forgery (SSRF) vulnerability in Theme-Ruby Foxiz.This issue affects Foxiz: from n/a through 2.3.5.	2024-07-06	7.2	CVE-2024-37260
traefik--traefik	Traefik is an HTTP reverse proxy and load balancer. Versions prior to 2.11.6, 3.0.4, and 3.1.0-rc3 have a vulnerability that allows bypassing IP allow-lists via HTTP/3 early data requests in QUIC 0-RTT handshakes sent with spoofed IP addresses. Versions 2.11.6, 3.0.4, and 3.1.0-rc3 contain a patch for this issue. No known workarounds are available.	2024-07-05	7.5	CVE-2024-39321
wbolt -- imgspider	The IMGspider plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload_img_file' function in all versions up to, and including, 2.3.10. This makes it possible for authenticated attackers, with contributor-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-07-04	8.8	CVE-2024-6318
wbolt -- imgspider	The IMGspider plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload' function in all versions up to, and including, 2.3.10. This makes it possible for authenticated attackers, with contributor-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-07-04	8.8	CVE-2024-6319
WofficeIO--Woffice Core	Cross Site Scripting (XSS) vulnerability in WofficeIO Woffice Core allows Reflected XSS.This issue affects Woffice Core: from n/a through 5.4.8.	2024-07-04	7.1	CVE-2024-37471
WofficeIO--Woffice	Cross Site Scripting (XSS) vulnerability in WofficeIO Woffice allows Reflected XSS.This issue affects Woffice: from n/a through 5.4.8.	2024-07-04	7.1	CVE-2024-37472
yt-dlp--yt-dlp	`yt-dlp` and `youtube-dl` are command-line audio/video downloaders. Prior to the fixed versions,Â `yt-dlp` and `youtube-dl` do not limit the extensions of downloaded files, which could lead to arbitrary filenames being created in the download folder (and path traversal on Windows). Since `yt-dlp` and `youtube-dl` also read config from the working directory (and on Windows executables will be executed from the `yt-dlp` or `youtube-dl` directory), this could lead to arbitrary code being executed. `yt-dlp` version 2024.07.01 fixes this issue by whitelisting the allowed extensions. `youtube-dl` fixes this issue in commit `d42a222` on the `master` branch and in nightly builds tagged 2024-07-03 or later. This might mean some very uncommon extensions might not get downloaded, however it will also limit the possible exploitation surface. In addition to upgrading, have `.%(ext)s` at the end of the output template and make sure the user trusts the websites that they are downloading from. Also, make sure to never download to a directory within PATH or other sensitive locations like one's user directory, `system32`, or other binaries locations. For users who are not able to upgrade, keep the default output template (`-o "%(title)s [%(id)s].%(ext)s`); make sure the extension of the media to download is a common video/audio/sub/... one; try to avoid the generic extractor; and/or use `--ignore-config --config-location ...` to not load config from common locations.	2024-07-02	7.8	CVE-2024-38519
Adobe--Bridge	Bridge versions 14.0.4, 13.0.7, 14.1 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.	2024-07-09	7.8	CVE-2024-34139
Adobe--InDesign Desktop	InDesign Desktop versions ID19.3, 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.	2024-07-09	7.8	CVE-2024-20781
Adobe--InDesign Desktop	InDesign Desktop versions ID19.3, 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.	2024-07-09	7.8	CVE-2024-20782
Adobe--InDesign Desktop	InDesign Desktop versions ID19.3, 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.	2024-07-09	7.8	CVE-2024-20783
Adobe--InDesign Desktop	InDesign Desktop versions ID19.3, ID18.5.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in	2024-07-09	7.8	CVE-2024-20785

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
Adobe--Premiere Pro	Premiere Pro versions 23.6.5, 24.4.1 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 when the application uses a search path to locate executables or libraries. Exploitation of this issue requires user interaction, attack complexity is high.	2024-07-09	7	CVE-2024-34123
Advanced File Manager--Advanced File Manager Shortcodes	The Advanced File Manager Shortcodes plugin for WordPress is vulnerable to arbitrary file uploads in all versions up to, and including, 2.5.3. This makes it possible for authenticated attackers with contributor access or above to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-07-10	8.8	CVE-2023-7061
Advanced File Manager--Advanced File Manager Shortcodes	The Advanced File Manager Shortcodes plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.4. This makes it possible for attackers with contributor access or higher to read the contents of arbitrary files on the server, which can contain sensitive information.	2024-07-10	8.8	CVE-2023-7062
airbytehq--airbyte	Airbyte is a data integration platform for ELT pipelines. Airbyte connection builder docker image is vulnerable to RCE via SSTI which allows an authenticated remote attacker to execute arbitrary code on the server as the web server user. The connection builder is used to create and test new connectors. Sensitive information, such as credentials, could be exposed if a user tested a new connector on a compromised instance. The connection builder does not have access to any data processes. This vulnerability is fixed in 0.62.2.	2024-07-09	8.5	CVE-2024-38363
Ali2Woo Team--Ali2Woo Lite	Cross-Site Request Forgery (CSRF) vulnerability in Ali2Woo Team Ali2Woo Lite allows Cross-Site Scripting (XSS).This issue affects Ali2Woo Lite: from n/a through 3.3.9.	2024-07-12	7.1	CVE-2024-37213
Andy Moyle--Church Admin	Unrestricted Upload of File with Dangerous Type vulnerability in Andy Moyle Church Admin allows Upload a Web Shell to a Web Server.This issue affects Church Admin: from n/a through 4.4.6.	2024-07-09	9.9	CVE-2024-37418
anhvnit--Woocommerce OpenPos	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in anhvnit Woocommerce OpenPos.This issue affects Woocommerce OpenPos: from n/a through 6.4.4.	2024-07-12	9.3	CVE-2024-37933
anhvnit--Woocommerce OpenPos	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in anhvnit Woocommerce OpenPos allows File Manipulation.This issue affects Woocommerce OpenPos: from n/a through 6.4.4.	2024-07-12	8.6	CVE-2024-37932
ashanjay--EventON	The EventON plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'eventon_import_settings' ajax action in all versions up to, and including, 2.2.15. This makes it possible for unauthenticated attackers to update plugin settings, including adding stored cross-site scripting to settings options displayed on event calendar pages.	2024-07-09	7.2	CVE-2024-6180
Automattic--Newspack Blocks	Unrestricted Upload of File with Dangerous Type vulnerability in Automattic Newspack Blocks allows Upload a Web Shell to a Web Server.This issue affects Newspack Blocks: from n/a through 3.0.8.	2024-07-09	9.9	CVE-2024-37424
Automattic--Newspack Blocks	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Automattic Newspack Blocks.This issue affects Newspack Blocks: from n/a through 3.0.8.	2024-07-10	7.5	CVE-2024-37115
bitpressadmin--Contact Form by Bit Form: Multi Step Form, Calculation Contact Form, Payment Contact Form & Custom Contact Form builder	The Bit Form plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'iconUpload' function in all versions up to, and including, 2.12.2. 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.	2024-07-09	7.2	CVE-2024-6123

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Booking Ultra Pro--Booking Ultra Pro	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Booking Ultra Pro allows PHP Local File Inclusion.This issue affects Booking Ultra Pro: from n/a through 1.1.13.	2024-07-12	7.1	CVE-2024-38717
Brainstorm Force--Ultimate Addons for Elementor	Improper Privilege Management vulnerability in Brainstorm Force Ultimate Addons for Elementor allows Privilege Escalation.This issue affects Ultimate Addons for Elementor: from n/a through 1.36.31.	2024-07-09	8.8	CVE-2024-37455
Checkmk GmbH--Checkmk	Incorrect permissions on the Checkmk Windows Agent's data directory in Checkmk < 2.3.0p8, < 2.2.0p29, < 2.1.0p45, and <= 2.0.0p39 (EOL) allows a local attacker to gain SYSTEM privileges.	2024-07-10	8.8	CVE-2024-28827
Checkmk GmbH--Checkmk	Cross-Site request forgery in Checkmk < 2.3.0p8, < 2.2.0p29, < 2.1.0p45, and <= 2.0.0p39 (EOL) could lead to 1-click compromize of the site.	2024-07-10	8.8	CVE-2024-28828
code-projects--Simple Task List	A vulnerability was found in code-projects Simple Task List 1.0. It has been declared as critical. This vulnerability affects unknown code of the file loginForm.php of the component Login. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-271060.	2024-07-11	7.3	CVE-2024-6653
Codeless--Cowidgets Elementor Addons	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Codeless Cowidgets - Elementor Addons allows Path Traversal.This issue affects Cowidgets - Elementor Addons: from n/a through 1.1.1.	2024-07-09	7.5	CVE-2024-37419
codermy -- my-springsecurity-plus	my-springsecurity-plus before v2024.07.03 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /api/user.	2024-07-12	9.8	CVE-2024-40539
codermy -- my-springsecurity-plus	my-springsecurity-plus before v2024.07.03 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /api/dept.	2024-07-12	9.8	CVE-2024-40540
codermy -- my-springsecurity-plus	my-springsecurity-plus before v2024.07.03 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /api/dept/build.	2024-07-12	9.8	CVE-2024-40541
codermy -- my-springsecurity-plus	my-springsecurity-plus before v2024.07.03 was discovered to contain a SQL injection vulnerability via the dataScope parameter at /api/role?offset.	2024-07-12	9.8	CVE-2024-40542
Crocoblock--JetThemeCore	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Crocoblock JetThemeCore allows File Manipulation.This issue affects JetThemeCore: from n/a before 2.2.1.	2024-07-09	7.7	CVE-2024-37497
deano1987--Advanced AJAX Page Loader	The Advanced AJAX Page Loader plugin for WordPress is vulnerable to Cross-Site Request Forgery to Arbitrary File Upload in versions up to, and including, 2.7.7. This is due to missing nonce validation in the 'admin_init_AAPL' function and missing file type validation in the 'AAPL_options_validate' function. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-07-09	8.8	CVE-2024-6310
decidim--decidim	Decidim is a participatory democracy framework. The pagination feature used in searches and filters is subject to potential XSS attack through a malformed URL using the GET parameter `per_page`. This vulnerability is fixed in 0.27.6 and 0.28.1.	2024-07-10	7.1	CVE-2024-32469
Delta Electronics--CNCSoft-G2	Delta Electronics CNCSoft-G2 lacks proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. If a target visits a malicious page or opens a malicious file an attacker can leverage this vulnerability to execute code in the context of the current process.	2024-07-09	7.8	CVE-2024-39880
directus--directus	Directus is a real-time API and App dashboard for managing SQL database content. When relying on SSO providers in combination with local authentication it can be possible to enumerate existing SSO users in the instance. This is possible because if an email address exists in Directus and belongs to a known SSO provider then it will throw a "helpful" error that the user belongs to another provider. This vulnerability is fixed in 10.13.0.	2024-07-08	7.5	CVE-2024-39896
dlink -- dir-823x_ax3000_firmware	D-Link DIR-823X firmware - 240126 was discovered to contain a remote command execution (RCE) vulnerability via the dhcpd_startip parameter at /goform/set_lan_settings.	2024-07-08	8.8	CVE-2024-39202
docker -- desktop	In Docker Desktop before v4.29.0, an attacker who has gained access to the Docker Desktop VM through a container breakout can further escape to the host by passing extensions and dashboard related IPC messages. Docker Desktop v4.29.0 https://docs.docker.com/desktop/release-notes/#4290 fixes the issue on MacOS,	2024-07-09	7	CVE-2024-6222 security@docker.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Linux and Windows with Hyper-V backend. As exploitation requires "Allow only extensions distributed through the Docker Marketplace" to be disabled, Docker DesktopÂ v4.31.0 https://docs.docker.com/desktop/release-notes/#4310 Â additionally changes the default configuration to enable this setting by default.			
dwieeb--ScrollTo Bottom	The ScrollTo Bottom plugin for WordPress is vulnerable to Cross-Site Request Forgery to Arbitrary File Upload in versions up to, and including, 1.1.1. This is due to missing nonce validation and missing file type validation in the 'options_page' function. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-07-09	8.8	CVE-2024-6321
dwieeb--ScrollTo Top	The ScrollTo Top plugin for WordPress is vulnerable to Cross-Site Request Forgery to Arbitrary File Upload in versions up to, and including, 1.2.2. This is due to missing nonce validation and missing file type validation in the 'options_page' function. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-07-09	8.8	CVE-2024-6320
Dylan James--Zephyr Project Manager	Improper Privilege Management vulnerability in Dylan James Zephyr Project Manager allows Privilege Escalation.This issue affects Zephyr Project Manager: from n/a through 3.3.97.	2024-07-09	8.8	CVE-2024-37484
e4jconnect -- vikrentcar	The VikRentCar Car Rental Management System WordPress plugin before 1.3.2 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	2024-07-11	8.8	CVE-2024-1845
electron -- electron-builder	electron-updater allows for automatic updates for Electron apps. The file `packages/electron-updater/src/windowsExecutableCodeSignatureVerifier.ts` implements the signature validation routine for Electron applications on Windows. Because of the surrounding shell, a first pass by `cmd.exe` expands any environment variable found in command-line above. This creates a situation where `verifySignature()` can be tricked into validating the certificate of a different file than the one that was just downloaded. If the step is successful, the malicious update will be executed even if its signature is invalid. This attack assumes a compromised update manifest (server compromise, Man-in-the-Middle attack if fetched over HTTP, Cross-Site Scripting to point the application to a malicious updater server, etc.). The patch is available starting from 6.3.0-alpha.6.	2024-07-09	7.5	CVE-2024-39698
embedded-solutions -- freemodbus	Buffer Overflow vulnerability in SILA Embedded Solutions GmbH freemodbus v.2018-09-12 allows a remtoe attacker to cause a denial of service via the LINUXTCP server component.	2024-07-08	7.5	CVE-2024-31504
EVerest--everest-core	EVerest is an EV charging software stack. An integer overflow in the "v2g_incoming_v2gtp" function in the v2g_server.cpp implementation can allow a remote attacker to overflow the process' heap. This vulnerability is fixed in 2024.3.1 and 2024.6.0.	2024-07-10	9	CVE-2024-37310
ExtremePacs--Extreme XDS	Improper Privilege Management vulnerability in Ekstrem Bir Bilgisayar Danismanlik Ic Ve Dis Ticaret Ltd. Sti. Extreme XDS allows Collect Data as Provided by Users.This issue affects Extreme XDS: before 3928.	2024-07-08	7.2	CVE-2024-4341
Favethemes--Houzez Theme - Functionality	The Houzez Theme - Functionality plugin for WordPress is vulnerable to SQL Injection via the 'currency_code' parameter in all versions up to, and including, 3.2.2 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 Custom-level (seller) access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-07-09	8.8	CVE-2024-5793
FOGProject--fogproject	FOG is a cloning/imaging/rescue suite/inventory management system. Prior to 1.5.10.34, packages/web/lib/fog/reportmaker.class.php in FOG was affected by a command injection via the filename parameter to /fog/management/export.php. This vulnerability is fixed in 1.5.10.34.	2024-07-12	9.8	CVE-2024-39914
Fortinet--FortiADC	An improper certificate validation vulnerability [CWE-295] in FortiADC 7.4.0, 7.2.0 through 7.2.3, 7.1 all versions, 7.0 all versions, 6.2 all versions, 6.1 all versions and 6.0 all versions may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and various remote servers such as private SDN connectors and FortiToken Cloud.	2024-07-09	7.4	CVE-2023-50178

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Fortinet--FortiAIOps	Multiple insufficient session expiration vulnerabilities [CWE-613] in FortiAIOps version 2.0.0 may allow an attacker to re-use stolen old session tokens to perform unauthorized operations via crafted requests.	2024-07-09	8.1	CVE-2024-27782
Fortinet--FortiAIOps	Multiple Exposure of sensitive information to an unauthorized actor vulnerabilities [CWE-200] in FortiAIOps version 2.0.0 may allow an authenticated, remote attacker to retrieve sensitive information from the API endpoint or log files.	2024-07-09	8.8	CVE-2024-27784
Fortinet--FortiAIOps	Multiple cross-site request forgery (CSRF) vulnerabilities [CWE-352] in FortiAIOps version 2.0.0 may allow an unauthenticated remote attacker to perform arbitrary actions on behalf of an authenticated user via tricking the victim to execute malicious GET requests.	2024-07-09	7.6	CVE-2024-27783
Fortinet--FortiExtender	An improper access control in Fortinet FortiExtender 4.1.1 - 4.1.9, 4.2.0 - 4.2.6, 5.3.2, 7.0.0 - 7.0.4, 7.2.0 - 7.2.4 and 7.4.0 - 7.4.2 allows an attacker to create users with elevated privileges via a crafted HTTP request.	2024-07-09	8.8	CVE-2024-23663
fullservices--FULL Cliente	The FULL - Cliente plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the license plan parameter in all versions up to, and including, 3.1.12 due to insufficient input sanitization and output escaping as well as missing authorization and capability checks on the related functions. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that will execute whenever an administrative user accesses wp-admin dashboard	2024-07-11	7.2	CVE-2024-6447
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 Path Traversal.This issue affects Ultimate Bootstrap Elements for Elementor: from n/a through 1.4.2.	2024-07-09	8.5	CVE-2024-37462
genetechproducts--Registration Forms User Registration Forms, Invitation-Based Registrations, Front-end User Profile, Login Form & Content Restriction	The Registration Forms - User Registration Forms, Invitation-Based Registrations, Front-end User Profile, Login Form & Content Restriction plugin for WordPress is vulnerable to unauthorized arbitrary plugin installation and activation/deactivation due to missing capability checks on the pieregister_install_addon, pieregister_activate_addon and pieregister_deactivate_addon functions in all versions up to, and including, 3.8.3.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install, activate and deactivate arbitrary plugins. As a result attackers might achieve code execution on the targeted server	2024-07-09	8.8	CVE-2024-6069
gitlab -- gitlab	An issue was discovered in GitLab CE/EE affecting all versions starting from 15.8 prior to 16.11.6, starting from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2, which allows an attacker to trigger a pipeline as another user under certain circumstances.	2024-07-11	9.8	CVE-2024-6385
glpi-project--glpi	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. An authenticated user can exploit a SQL injection vulnerability in some AJAX scripts to alter another user account data and take control of it. Upgrade to 10.0.16.	2024-07-10	8.1	CVE-2024-37148
glpi-project--glpi	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. An authenticated technician user can upload a malicious PHP script and hijack the plugin loader to execute this malicious script. Upgrade to 10.0.16.	2024-07-10	7.2	CVE-2024-37149
Google--Android	In CacheOpPMRExec of cache_km.c, there is a possible out of bounds write 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.	2024-07-09	8.4	CVE-2024-23695
Google--Android	In RGXCreateZSBufferKM of rgxta3d.c, there is a possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	8.4	CVE-2024-23696
Google--Android	In updateNotificationChannelFromPrivilegedListener of NotificationManagerService.java, there is a possible cross-user data leak due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	8.4	CVE-2024-31319
Google--Android	In multiple locations, there is a possible way to bypass a restriction on adding new Wi-Fi connections due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	8.4	CVE-2024-31332

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Google--Android	In multiple locations, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	CVE-2023-21113
Google--Android	In RGXCreateHWRTData_aux of rgxta3d.c, there is a possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.3	CVE-2024-23697
Google--Android	In RGXFWChangeOSidPriority of rgxfwutils.c, there is a possible arbitrary code execution due to a missing bounds check. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	CVE-2024-23698
Google--Android	In DevmemXIntUnreserveRange of devicemem_server.c, there is a possible arbitrary code execution due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	CVE-2024-23711
Google--Android	In onResult of AccountManagerService.java, there is a possible way to perform an arbitrary background activity launch due to parcel mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	CVE-2024-31316
Google--Android	In multiple functions of ZygoteProcess.java, there is a possible way to achieve code execution as any app via WRITE_SECURE_SETTINGS due to unsafe deserialization. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	CVE-2024-31317
Google--Android	In setSkipPrompt of AssociationRequest.java , there is a possible way to establish a companion device association without any confirmation due to CDM. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.4	CVE-2024-31320
Google--Android	In onCreate of multiple files, there is a possible way to trick the user into granting health permissions due to tapjacking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	CVE-2024-31323
Google--Android	In hide of WindowState.java, there is a possible way to bypass tapjacking/overlay protection by launching the activity in portrait mode first and then rotating it to landscape mode. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.	2024-07-09	7.8	CVE-2024-31324
Google--Android	In setMimeGroup of PackageManagerService.java, there is a possible way to hide the service from Settings due to a logic error in the code. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.	2024-07-09	7.8	CVE-2024-31331
Google--Android	In multiple functions of StatsService.cpp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	CVE-2024-31339
Google--Android	In com_android_internal_os_ZygoteCommandBuffer_nativeForkRepeatedly of com_android_internal_os_ZygoteCommandBuffer.cpp, there is a possible method to perform arbitrary code execution in any app zygote processes 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.	2024-07-09	7.4	CVE-2024-34720
Google--Android	In smp_proc_rand of smp_act.cc, there is a possible authentication bypass during legacy BLE pairing due to incorrect implementation of a protocol. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.4	CVE-2024-34722
Google--Android	In _UnrefAndMaybeDestroy of pmr.c, there is a possible arbitrary code execution due to a race condition. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7	CVE-2024-34724
Google--Android	In PVRSRV_MMap of pvr_bridge_k.c, there is a possible arbitrary code execution due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	7.8	CVE-2024-34726
hackmdio--codimd	CodiMD allows realtime collaborative markdown notes on all platforms. The notebook feature of Hackmd.io permits the rendering of iframe `HTML` tags with an improperly sanitized `name` attribute. This vulnerability enables attackers to	2024-07-10	8.1	CVE-2024-38354

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	perform cross-site scripting (XSS) attacks via DOM clobbering. This vulnerability is fixed in 2.5.4.			
HashiCorp--Vault	Vault and Vault Enterprise did not properly handle requests originating from unauthorized IP addresses when the TCP listener option, proxy_protocol_behavior, was set to deny_unauthorized. When receiving a request from a source IP address that was not listed in proxy_protocol_authorized_addrs, the Vault API server would shut down and no longer respond to any HTTP requests, potentially resulting in denial of service. While this bug also affected versions of Vault up to 1.17.1 and 1.16.5, a separate regression in those release series did not allow Vault operators to configure the deny_unauthorized option, thus not allowing the conditions for the denial of service to occur. Fixed in Vault and Vault Enterprise 1.17.2, 1.16.6, and 1.15.12.	2024-07-11	7.5	CVE-2024-6468 security@hashicorp.com
hcltech -- domino	This vulnerability is being re-assessed.Â Vulnerability details will be updated. The security bulletin will be republished when further details are available.	2024-07-08	7.5	CVE-2024-23562
Houzez--Houzez CRM	The Houzez CRM plugin for WordPress is vulnerable to time-based SQL Injection via the notes 'belong_to' parameter in all versions up to, and including, 1.4.2 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 Custom-level (seller) access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-07-10	8.8	CVE-2024-5792
ibm -- i	IBM System Management for i 7.2, 7.3, and 7.4 could allow a local user to gain elevated privileges due to an unqualified library program call. A malicious actor could cause user-controlled code to run with administrator privilege. IBM X-Force ID: 295227.	2024-07-08	7.8	CVE-2024-38330
IBM--MQ Operator	IBM MQ Operator 3.2.2 and IBM MQ Operator 2.0.24 could allow a user to bypass authentication under certain configurations due to a partial string comparison vulnerability. IBM X-Force ID: 297169.	2024-07-08	8.1	CVE-2024-39742
IBM--WebSphere Application Server	IBM WebSphere Application Server 8.5 and 9.0 could allow a remote authenticated attacker, who has authorized access to the administrative console, to execute arbitrary code. Using specially crafted input, the attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 292641.	2024-07-09	7.2	CVE-2024-35154
ifm--Smart PLC AC14xx Firmware	An unauthenticated remote attacker can use the hard-coded credentials to access the SmartSPS devices with high privileges.	2024-07-09	9.8	CVE-2024-28747
ifm--Smart PLC AC14xx Firmware	An high privileged remote attacker can enable telnet access that accepts hardcoded credentials.Â	2024-07-09	9.1	CVE-2024-28751
ifm--Smart PLC AC14xx Firmware	A remote attacker with high privileges may use a reading file function to inject OS commands.	2024-07-09	7.2	CVE-2024-28748
ifm--Smart PLC AC14xx Firmware	A remote attacker with high privileges may use a writing file function to inject OS commands.	2024-07-09	7.2	CVE-2024-28749
ifm--Smart PLC AC14xx Firmware	A remote attacker with high privileges may use a deleting file function to inject OS commands.	2024-07-09	7.2	CVE-2024-28750
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 all versions up to, and including, 4.14.7. This is due to insufficient verification on the 'phone' parameter of the 'firebase_sms_login' and 'firebase_sms_login_v2' functions. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email address or phone number. Additionally, if a new email address is supplied, a new user account is created with the default role, even if registration is disabled.	2024-07-12	9.8	CVE-2024-6328
instawp -- instawp_connect	The InstaWP Connect - 1-click WP Staging & Migration plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 0.1.0.44. This is due to insufficient verification of the API key. 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 username, and to perform a variety of other administrative tasks. NOTE: This vulnerability was partially fixed in 0.1.0.44, but was still exploitable via Cross-Site Request Forgery.	2024-07-11	9.8	CVE-2024-6397
IqbalRony--WP User Switch	Improper Privilege Management vulnerability in IqbalRony WP User Switch allows Privilege Escalation.This issue affects WP User Switch: from n/a through 1.1.0.	2024-07-12	8	CVE-2024-37560

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
isc -- stork	The TLS certificate validation code is flawed. An attacker can obtain a TLS certificate from the Stork server and use it to connect to the Stork agent. Once this connection is established with the valid certificate, the attacker can send malicious commands to a monitored service (Kea or BIND 9), possibly resulting in confidential data loss and/or denial of service. It should be noted that this vulnerability is not related to BIND 9 or Kea directly, and only customers using the Stork management tool are potentially affected. This issue affects Stork versions 0.15.0 through 1.15.0.	2024-07-11	8.1	CVE-2024-28872
jevnet--Easy Pixels	The Easy Pixels plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin settings in all versions up to, and including, 2.13 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.	2024-07-09	7.2	CVE-2024-5479
Juniper Networks, Inc.--Junos OS	An Improper Neutralization of Data within XPath Expressions ('XPath Injection') vulnerability in J-Web shipped with Juniper Networks Junos OS allows an unauthenticated, network-based attacker toÂ executeÂ remote commands on the target device.Â While an administrator is logged into a J-Web session or has previously logged in and subsequently logged out of their J-Web session, the attacker can arbitrarily execute commands on the target device with the other user's credentials. In the worst case, the attacker will have full control over the device. This issue affects Junos OS:Â * All versions before 21.2R3-S8,Â * from 21.4 before 21.4R3-S7, * from 22.2 before 22.2R3-S4, * from 22.3 before 22.3R3-S3, * from 22.4 before 22.4R3-S2, * from 23.2 before 23.2R2, * from 23.4 before 23.4R1-S1, 23.4R2.	2024-07-10	8.8	CVE-2024-39565
Juniper Networks--Junos OS Evolved	AnÂ Improper Neutralization of Special Elements vulnerability in Juniper Networks Junos OS Evolved commands allows a local, authenticated attacker with low privileges to escalate their privileges to 'root' leading to a full compromise of the system. The Junos OS Evolved CLI doesn't properly handle command options in some cases, allowing users which execute specific CLI commands with a crafted set of parameters to escalate their privileges to root on shell level. This issue affects Junos OS Evolved: * All version before 20.4R3-S6-EVO,Â * 21.2-EVO versions before 21.2R3-S4-EVO, * 21.4-EVO versions before 21.4R3-S6-EVO,Â * 22.2-EVO versions before 22.2R2-S1-EVO, 22.2R3-EVO,Â * 22.3-EVO versions before 22.3R2-EVO.	2024-07-11	7.8	CVE-2024-39520
Juniper Networks--Junos OS Evolved	An Improper Neutralization of Special Elements vulnerability in Juniper Networks Junos OS Evolved commands allows a local, authenticated attacker with low privileges to escalate their privileges to 'root' leading to a full compromise of the system. The Junos OS Evolved CLI doesn't properly handle command options in some cases, allowing users which execute specific CLI commands with a crafted set of parameters to escalate their privileges to root on shell level. This issue affects Junos OS Evolved:Â * 21.1-EVO versions 21.1R1-EVO and later before 21.2R3-S8-EVO,Â * 21.4-EVO versions before 21.4R3-S7-EVO, * 22.1-EVO versions before 22.1R3-S6-EVO,Â * 22.2-EVO versions before 22.2R3-EVO, * 22.3-EVO versions before 22.3R2-EVO.	2024-07-11	7.8	CVE-2024-39521
Juniper Networks--Junos OS Evolved	An Improper Neutralization of Special Elements vulnerability in Juniper Networks Junos OS Evolved commands allows a local, authenticated attacker with low privileges to escalate their privileges to 'root' leading to a full compromise of the system. The Junos OS Evolved CLI doesn't properly handle command options in some cases, allowing users which execute specific CLI commands with a crafted set of parameters to escalate their privileges to root on shell level. This issue affects Junos OS Evolved: * 22.3-EVO versions before 22.3R2-EVO, * 22.4-EVO versions before 22.4R1-S1-EVO, 22.4R2-EVO.	2024-07-11	7.8	CVE-2024-39522
Juniper Networks--Junos OS Evolved	An Improper Neutralization of Special Elements vulnerability in Juniper Networks Junos OS Evolved commands allows a local, authenticated attacker with low privileges to escalate their privileges to 'root' leading to a full compromise of the system. The Junos OS Evolved CLI doesn't properly handle command options in some cases, allowing users which execute specific CLI commands with a crafted set of parameters to escalate their privileges to root on shell level. This issue affects Junos OS Evolved:Â * All versions before 20.4R3-S7-EVO, * 21.2-EVO versions before 21.2R3-S8-EVO, * 21.4-EVO versions before 21.4R3-S7-EVO, * 22.1-EVO versions before 22.1R3-S6-EVO,Â * 22.2-EVO versions before 22.2R3-EVO, * 22.3-EVO versions before 22.3R2-EVO, * 22.4-EVO versions before 22.4R2-EVO.	2024-07-11	7.8	CVE-2024-39523
Juniper Networks--Junos OS Evolved	An Improper Neutralization of Special Elements vulnerability in Juniper Networks Junos OS Evolved commands allows a local, authenticated attacker with low privileges to escalate their privileges to 'root' leading to a full compromise of the system. The Junos OS Evolved CLI doesn't properly handle command options in	2024-07-11	7.8	CVE-2024-39524

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	some cases, allowing users which execute specific CLI commands with a crafted set of parameters to escalate their privileges to root on shell level. This issue affects Junos OS Evolved: All versions before 20.4R3-S7-EVO, 21.2-EVO versions before 21.2R3-S8-EVO, 21.4-EVO versions before 21.4R3-S7-EVO,Â 22.2-EVO versions before 22.2R3-EVO, 22.3-EVO versions before 22.3R2-EVO, 22.4-EVO versions before 22.4R2-EVO.			
Juniper Networks--Junos OS Evolved	An Improper Handling of Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX 7000 Series allows a network-based, unauthenticated attacker to cause a Denial-of-Service (DoS). If a value is configured for DDoS bandwidth or burst parameters for any protocol in a queue, all protocols which share the same queue will have their bandwidth or burst value changed to the new value. If, for example, OSPF was configured with a certain bandwidth value, ISIS would also be limited to this value. So inadvertently either the control plane is open for a high level of specific traffic which was supposed to be limited to a lower value, or the limit for a certain protocol is so low that chances to succeed with a volumetric DoS attack are significantly increased.Â This issue affects Junos OS Evolved on ACX 7000 Series: * All versions before 21.4R3-S7-EVO, * 22.1 versions before 22.1R3-S6-EVO,Â * 22.2 versions before 22.2R3-S3-EVO, * 22.3 versions before 22.3R3-S3-EVO,Â * 22.4 versions before 22.4R3-S2-EVO, * 23.2 versions before 23.2R2-EVO, * 23.4 versions before 23.4R1-S1-EVO, 23.4R2-EVO.	2024-07-11	7.5	CVE-2024-39531
Juniper Networks--Junos OS Evolved	A Missing Authorization vulnerability in the Socket Intercept (SI) command file interface of Juniper Networks Junos OS Evolved allows an authenticated, low-privilege local attacker to modify certain files, allowing the attacker to cause any command to execute with root privileges leading to privilege escalation ultimately compromising the system.Â This issue affects Junos OS Evolved:Â * All versions prior to 21.2R3-S8-EVO,Â * 21.4 versions prior toÂ 21.4R3-S6-EVO,Â * 22.1 versions prior to 22.1R3-S5-EVO,Â * 22.2 versions prior to 22.2R3-S3-EVO,Â * 22.3 versions prior to 22.3R3-S3-EVO,Â * 22.4 versions prior to 22.4R3-EVO,Â * 23.2 versions prior to 23.2R2-EVO.	2024-07-11	7.3	CVE-2024-39546
Juniper Networks--Junos OS Evolved	An Uncontrolled Resource Consumption vulnerability in the aftmand process of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to consume memory resources, resulting in a Denial of Service (DoS) condition. The processes do not recover on their own and must be manually restarted. This issue affects both IPv4 and IPv6.Â Changes in memory usage can be monitored using the following CLI command: user@device> show system memory node <fpc slot> | grep evo-aftmann This issue affects Junos OS Evolved:Â * All versions before 21.2R3-S8-EVO,Â * 21.3 versions before 21.3R3-S5-EVO,Â * 21.4 versions before 21.4R3-S5-EVO,Â * 22.1 versions before 22.1R3-S4-EVO,Â * 22.2 versions before 22.2R3-S4-EVO, * 22.3 versions before 22.3R3-S3-EVO, * 22.4 versions before 22.4R2-S2-EVO, 22.4R3-EVO,Â * 23.2 versions before 23.2R1-S1-EVO, 23.2R2-EVO.	2024-07-11	7.5	CVE-2024-39548
Juniper Networks--Junos OS Evolved	A Missing Release of Resource after Effective Lifetime vulnerability the xinetd process, responsible for spawning SSH daemon (sshd) instances, of Juniper Networks Junos OS Evolved allows an unauthenticated network-based attacker to cause a Denial of Service (DoS) by blocking SSH access for legitimate users. Continued receipt of these connections will create a sustained Denial of Service (DoS) condition. The issue is triggered when a high rate of concurrent SSH requests are received and terminated in a specific way, causing xinetd to crash, and leaving defunct sshd processes. Successful exploitation of this vulnerability blocks both SSH access as well as services which rely upon SSH, such as SFTP, andÂ Netconf over SSH. Once the system is in this state, legitimate users will be unable to SSH to the device until service is manually restored.Â See WORKAROUND section below. Administrators can monitor an increase in defunct sshd processes by utilizing the CLI command: Â > show system processes | match sshd Â root Â 25219 30901 0 Jul16 ? Â Â Â 00:00:00 [sshd] <defunct> This issue affects Juniper Networks Junos OS Evolved: * All versions prior to 21.4R3-S7-EVO * 22.3-EVO versions prior to 22.3R2-S2-EVO, 22.3R3-S2-EVO; * 22.4-EVO versions prior to 22.4R3-EVO; * 23.2-EVO versions prior to 23.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved 22.1-EVO nor 22.2-EVO.	2024-07-10	7.5	CVE-2024-39562
Juniper Networks--Junos OS	A Heap-based Buffer Overflow vulnerability in the telemetry sensor process (sensord) of Juniper Networks Junos OS on MX240, MX480, MX960 platforms using MPC10E causes a steady increase in memory utilization, ultimately leading to a Denial of Service (DoS). When the device is subscribed to a specific subscription on Junos Telemetry Interface, a slow memory leak occurs and eventually all resources are consumed and the device becomes unresponsive. A manual reboot of the Line Card will be required to restore the device to its normal functioning.Â This issue is	2024-07-10	7.5	CVE-2024-39518

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	only seen when telemetry subscription is active. The Heap memory utilization can be monitored using the following command: Â > show system processes extensive The following command can be used to monitor the memory utilization of the specific sensor Â > show system info | match sensord PID NAME MEMORY PEAK MEMORY %CPU THREAD-COUNT CORE-AFFINITY UPTIME 1986 sensord 877.57MB 877.57MB 2 4 0,2-15 7-21:41:32 This issue affects Junos OS:Â * from 21.2R3-S5 before 21.2R3-S7,Â * from 21.4R3-S4 before 21.4R3-S6,Â * from 22.2R3 before 22.2R3-S4,Â * from 22.3R2 before 22.3R3-S2,Â * from 22.4R1 before 22.4R3,Â * from 23.2R1 before 23.2R2.			
Juniper Networks--Junos OS	A Use of Externally-Controlled Format String vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause aÂ Denial-of-Service (DoS). If DNS Domain Generation Algorithm (DGA) detection or tunnel detection, and DNS-filtering traceoptions are configured, and specific valid transit DNS traffic is received this causesÂ a PFE crash and restart, leading to a Denial of Service. This issue affects Junos OS: * All versions before 21.4R3-S6, * 22.2 versions before 22.2R3-S3, * 22.3 versions before 22.3R3-S3, * 22.4 versions before 22.4R3, * 23.2 versions before 23.2R2.	2024-07-11	7.5	CVE-2024-39529
Juniper Networks--Junos OS	An Improper Check for Unusual or Exceptional Conditions vulnerability in the chassis management daemon (chassisd) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). If an attempt is made to access specific sensors on platforms not supporting these sensors, either via GRPC or netconf, chassisd will crash and restart leading to a restart of all FPCs and thereby a complete outage. This issue affects Junos OS: * 21.4 versions from 21.4R3 before 21.4R3-S5, * 22.1 versions from 22.1R3 before 22.1R3-S4, * 22.2 versions from 22.2R2 before 22.2R3, * 22.3 versions from 22.3R1 before 22.3R2-S2, 22.3R3, * 22.4 versions from 22.4R1 before 22.4R2. This issue does not affect Junos OS versions earlier than 21.4.	2024-07-11	7.5	CVE-2024-39530
Juniper Networks--Junos OS	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS on SRX Series, and MX Series with SPC3 allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). When an affected device receives specific valid TCP traffic, the pfe crashes and restarts leading to a momentary but complete service outage. This issue affects Junos OS: 21.2 releases from 21.2R3-S5 before 21.2R3-S6. This issue does not affect earlier or later releases.	2024-07-11	7.5	CVE-2024-39540
Juniper Networks--Junos OS	An Improper Validation of Syntactic Correctness of Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series with MPC10/11 or LC9600, MX304, and Junos OS Evolved on ACX Series and PTX Series allows an unauthenticated, network based attacker to cause a Denial-of-Service (DoS). This issue can occur in two scenarios: 1. If a device, which is configured with SFLOW and ECMP, receives specific valid transit traffic, which is subject to sampling, the packetio process crashes, which in turn leads to an evo-aftman crash and causes the FPC to stop working until it is restarted. (This scenario is only applicable to PTX but not to ACX or MX.) 2. If a device receives a malformed CFM packet on an interface configured with CFM, the packetio process crashes, which in turn leads to an evo-aftman crash and causes the FPC to stop working until it is restarted.Â Please note that the CVSS score is for the formally more severe issue 1. The CVSS score for scenario 2. is: 6.5 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) This issue affects Junos OS: * All versions beforeÂ 21.2R3-S4, * 21.4 versions before 21.4R2, * 22.2 versions before 22.2R3-S2;Â Junos OS Evolved: * All versions beforeÂ 21.2R3-S8-EVO, * 21.4 versions before 21.4R2-EVO.	2024-07-11	7.5	CVE-2024-39542
Juniper Networks--Junos OS	An Improper Check for Unusual or Exceptional Conditions vulnerability in the the IKE daemon (iked) of Juniper Networks Junos OS on SRX Series, MX Series with SPC3 and NFX350 allows allows an unauthenticated, network-based attacker sending specific mismatching parameters as part of the IPsec negotiation to trigger an iked crash leading to Denial of Service (DoS). This issue is applicable to all platforms that run iked.Â This issue affects Junos OS on SRX Series, MX Series with SPC3 and NFX350:Â * All versions before 21.2R3-S8,Â * from 21.4 before 21.4R3-S7,Â * from 22.1 before 22.1R3-S2,Â * from 22.2 before 22.2R3-S1,Â * from 22.3 before 22.3R2-S1, 22.3R3,Â * from 22.4 before 22.4R1-S2, 22.4R2, 22.4R3.	2024-07-11	7.5	CVE-2024-39545
Juniper Networks--Junos OS	A Missing Release of Memory after Effective Lifetime vulnerability in the routing process daemon (rpd) ofÂ Juniper Networks Junos OS and Junos OS Evolved allows an attacker to send a malformed BGP Path attribute update which allocates memory used to log the bad path attribute. This memory is not properly freed in all circumstances, leading to a Denial of Service (DoS). Consumed memory can be	2024-07-11	7.5	CVE-2024-39549

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	freed by manually restarting Routing Protocol Daemon (rpd). Memory utilization could be monitored by:Â user@host> show system memory or show system monitor memory status This issue affects: Junos OS:Â * All versions before 21.2R3-S8,Â * from 21.4 before 21.4R3-S8, * from 22.2 before 22.2R3-S4,Â * from 22.3 before 22.3R3-S3,Â * from 22.4 before 22.4R3-S3, * from 23.2 before 23.2R2-S1,Â * from 23.4 before 23.4R1-S2, 23.4R2, * from 24.2 beforeÂ 24.2R2-EVO. Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * from 21.4 before 21.4R3-S8-EVO, * from 22.2 before 22.2R3-S4-EVO, * from 22.3 before 22.3R3-S3-EVO, * from 22.4 before 22.4R3-S3-EVO, * from 23.2 before 23.2R2-S1-EVO, * from 23.4 before 23.4R1-S2, 23.4R2, * from 24.2 before 24.2R2-EVO.			
Juniper Networks--Junos OS	An Uncontrolled Resource Consumption vulnerability in the H.323 ALG (Application Layer Gateway) ofÂ Juniper Networks Junos OS on SRX Series and MX Series with SPC3 and MS-MPC/MIC, allows anÂ unauthenticated network-based attacker to send specific packets causing traffic loss leading to Denial of Service (DoS).Â Continued receipt and processing of these specific packets will sustain the Denial of Service condition. The memory usage can be monitored using the below command. â€fâ€fuser@host> show usp memory segment sha data objcache jsfÂ This issue affects SRX Series and MX Series with SPC3 and MS-MPC/MIC:Â * â€f20.4 before 20.4R3-S10,Â * â€f21.2 before 21.2R3-S6,Â * â€f21.3 before 21.3R3-S5,Â * â€f21.4 before 21.4R3-S6,Â * â€f22.1 before 22.1R3-S4,Â * â€f22.2 before 22.2R3-S2,Â * â€f22.3 before 22.3R3-S1,Â * â€f22.4 before 22.4R3,Â * â€f23.2 before 23.2R2.	2024-07-11	7.5	CVE-2024-39551
Juniper Networks--Junos OS	An Improper Handling of Exceptional Conditions vulnerability in the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause the RPD process to crash leading to a Denial of Service (DoS). When a malformed BGP UPDATE packet is received over an established BGP session, RPD crashes and restarts. Continuous receipt of the malformed BGP UPDATE messages will create a sustained Denial of Service (DoS) condition for impacted devices. This issue affects eBGP and iBGP, in both IPv4 and IPv6 implementations. This issue requires a remote attacker to have at least one established BGP session. This issue affects: Juniper Networks Junos OS: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S4; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R2. Juniper Networks Junos OS Evolved: * All versions earlier than 21.2R3-S7; * 21.3-EVO versions earlier than 21.3R3-S5; * 21.4-EVO versions earlier than 21.4R3-S8; * 22.1-EVO versions earlier than 22.1R3-S4; * 22.2-EVO versions earlier than 22.2R3-S3; * 22.3-EVO versions earlier than 22.3R3-S2; * 22.4-EVO versions earlier than 22.4R3; * 23.2-EVO versions earlier than 23.2R2.	2024-07-11	7.5	CVE-2024-39552
Juniper Networks--Junos OS	An Improper Handling of Exceptional Conditions vulnerability in the Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an attacker sending a specific malformed BGP update message to cause the session to reset, resulting in a Denial of Service (DoS). Continued receipt and processing of these malformed BGP update messages will create a sustained Denial of Service (DoS) condition. Upon receipt of a BGP update message over an established BGP session containing a specifically malformed tunnel encapsulation attribute, when segment routing is enabled, internal processing of the malformed attributes within the update results in improper parsing of remaining attributes, leading to session reset: BGP SEND Notification code 3 (Update Message Error) subcode 1 (invalid attribute list) Only systems with segment routing enabled are vulnerable to this issue. This issue affects eBGP and iBGP, in both IPv4 and IPv6 implementations, and requires a remote attacker to have at least one established BGP session. This issue affects: Junos OS: * All versions before 21.4R3-S8, * from 22.2 before 22.2R3-S4, * from 22.3 before 22.3R3-S3, * from 22.4 before 22.4R3-S3, * from 23.2 before 23.2R2-S1, * from 23.4 before 23.4R1-S2, 23.4R2. Junos OS Evolved:Â * All versions before 21.4R3-S8-EVO, * from 22.2-EVO before 22.2R3-S4-EVO, * from 22.3-EVO before 22.3R3-S3-EVO, * from 22.4-EVO before 22.4R3-S3-EVO, * from 23.2-EVO before 23.2R2-S1-EVO, * from 23.4-EVO before 23.4R1-S2-EVO, 23.4R2-EVO.	2024-07-10	7.5	CVE-2024-39555
KaineLabs--Youzify	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in KaineLabs Youzify.This issue affects Youzify: from n/a through 1.2.5.	2024-07-09	8.5	CVE-2024-37494
kaptinlin--Striking	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in kaptinlin Striking allows Path Traversal.This issue affects Striking: from n/a through 2.3.4.	2024-07-09	8.5	CVE-2024-37268

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
level1 -- wbr-6013_firmware	A hard-coded password vulnerability exists in the telnetd functionality of LevelOne WBR-6013 RER4_A_v3411b_2T2R_LEV_09_170623. A set of specially crafted network packets can lead to arbitrary command execution.	2024-07-08	9.8	CVE-2023-46685
level1 -- wbr-6013_firmware	Leftover debug code exists in the boa formSysCmd functionality of LevelOne WBR-6013 RER4_A_v3411b_2T2R_LEV_09_170623. A specially crafted network request can lead to arbitrary command execution.	2024-07-08	7.2	CVE-2023-49593
Membership Software--WishList Member X	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Membership Software WishList Member X.This issue affects WishList Member X: from n/a before 3.26.7.	2024-07-09	10	CVE-2024-37112
Membership Software--WishList Member X	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Membership Software WishList Member X.This issue affects WishList Member X: from n/a before 3.26.7.	2024-07-10	9.8	CVE-2024-37113
Membership Software--WishList Member X	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Membership Software WishList Member X.This issue affects WishList Member X: from n/a before 3.26.7.	2024-07-10	7.5	CVE-2024-37110
metagauss--ProfileGrid User Profiles, Groups and Communities	The ProfileGrid - User Profiles, Groups and Communities plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 5.8.9. This is due to a lack of validation on user-supplied data in the 'pm_upload_image' AJAX action. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update their user capabilities to Administrator.	2024-07-10	8.8	CVE-2024-6411
microsoft -- .net	.NET and Visual Studio Denial of Service Vulnerability	2024-07-09	7.5	CVE-2024-38095
microsoft -- 365_apps	Microsoft Outlook Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-38021
microsoft -- azure_cyclecloud	Azure CycleCloud Elevation of Privilege Vulnerability	2024-07-09	8.8	CVE-2024-38092
microsoft -- defender_for_iot	Microsoft Defender for IoT Elevation of Privilege Vulnerability	2024-07-09	9.9	CVE-2024-38089
microsoft -- sharepoint_server	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-07-09	7.2	CVE-2024-38023
microsoft -- sharepoint_server	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-07-09	7.2	CVE-2024-38024
microsoft -- sharepoint_server	Microsoft SharePoint Remote Code Execution Vulnerability	2024-07-09	7.2	CVE-2024-38094
microsoft -- windows_10_1507	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-37986
microsoft -- windows_10_1507	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-37987
microsoft -- windows_10_1507	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-37988
microsoft -- windows_10_1507	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-37989
microsoft -- windows_10_1507	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-38010
microsoft -- windows_10_1507	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-38011
microsoft -- windows_10_1507	Windows Distributed Transaction Coordinator Remote Code Execution Vulnerability	2024-07-09	8.1	CVE-2024-38049

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10_1507	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-38053
microsoft -- windows_10_1507	Windows Imaging Component Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-38060
microsoft -- windows_10_1507	Windows Fax Service Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-38104
microsoft -- windows_10_1507	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability	2024-07-09	7.2	CVE-2024-38019
microsoft -- windows_10_1507	Windows Image Acquisition Elevation of Privilege Vulnerability	2024-07-09	7	CVE-2024-38022
microsoft -- windows_10_1507	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability	2024-07-09	7.2	CVE-2024-38025
microsoft -- windows_10_1507	Microsoft Windows Performance Data Helper Library Remote Code Execution Vulnerability	2024-07-09	7.2	CVE-2024-38028
microsoft -- windows_10_1507	PowerShell Elevation of Privilege Vulnerability	2024-07-09	7.3	CVE-2024-38033
microsoft -- windows_10_1507	Windows Filtering Platform Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38034
microsoft -- windows_10_1507	Windows Workstation Service Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38050
microsoft -- windows_10_1507	Windows Graphics Component Remote Code Execution Vulnerability	2024-07-09	7.8	CVE-2024-38051
microsoft -- windows_10_1507	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38052
microsoft -- windows_10_1507	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38054
microsoft -- windows_10_1507	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38057
microsoft -- windows_10_1507	DCOM Remote Cross-Session Activation Elevation of Privilege Vulnerability	2024-07-09	7.5	CVE-2024-38061
microsoft -- windows_10_1507	Windows TCP/IP Information Disclosure Vulnerability	2024-07-09	7.5	CVE-2024-38064
microsoft -- windows_10_1507	Windows Win32k Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38066
microsoft -- windows_10_1507	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability	2024-07-09	7.5	CVE-2024-38068
microsoft -- windows_10_1507	Windows Enroll Engine Security Feature Bypass Vulnerability	2024-07-09	7	CVE-2024-38069
microsoft -- windows_10_1507	Windows LockDown Policy (WLDP) Security Feature Bypass Vulnerability	2024-07-09	7.8	CVE-2024-38070
microsoft -- windows_10_1507	Windows Graphics Component Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38079

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10_1507	Windows Graphics Component Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38085
microsoft -- windows_10_1507	Microsoft WS-Discovery Denial of Service Vulnerability	2024-07-09	7.5	CVE-2024-38091
microsoft -- windows_10_1507	Windows MSHTML Platform Spoofing Vulnerability	2024-07-09	7.5	CVE-2024-38112
microsoft -- windows_10_1607	PowerShell Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38043
microsoft -- windows_10_1607	PowerShell Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38047
microsoft -- windows_10_1607	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38062
microsoft -- windows_10_21h2	Microsoft Xbox Remote Code Execution Vulnerability	2024-07-09	7.1	CVE-2024-38032
microsoft -- windows_10_21h2	Win32k Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38059
microsoft -- windows_11_21h2	Xbox Wireless Adapter Remote Code Execution Vulnerability	2024-07-09	7.5	CVE-2024-38078
microsoft -- windows_11_21h2	Windows Hyper-V Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38080
microsoft -- windows_server_2008	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	2024-07-09	9.8	CVE-2024-38074
microsoft -- windows_server_2008	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	2024-07-09	9.8	CVE-2024-38077
microsoft -- windows_server_2008	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability	2024-07-09	7.5	CVE-2024-38031
microsoft -- windows_server_2008	Windows Online Certificate Status Protocol (OCSP) Server Denial of Service Vulnerability	2024-07-09	7.5	CVE-2024-38067
microsoft -- windows_server_2008	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	2024-07-09	7.5	CVE-2024-38071
microsoft -- windows_server_2008	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	2024-07-09	7.5	CVE-2024-38073
microsoft -- windows_server_2012	Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability	2024-07-09	7.5	CVE-2024-38015
microsoft -- windows_server_2012	DHCP Server Service Remote Code Execution Vulnerability	2024-07-09	7.2	CVE-2024-38044
microsoft -- windows_server_2	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	2024-07-09	9.8	CVE-2024-38076

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
016				
microsoft -- windows_server_2016	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	2024-07-09	7.5	CVE-2024-38072
microsoft -- windows_server_2016	Windows File Explorer Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-38100
Microsoft--.NET 8.0	.NET and Visual Studio Remote Code Execution Vulnerability	2024-07-09	8.1	CVE-2024-35264
Microsoft--.NET 8.0	.NET Core and Visual Studio Denial of Service Vulnerability	2024-07-09	7.5	CVE-2024-30105
Microsoft--Azure DevOps Server 2022	Azure DevOps Server Spoofing Vulnerability	2024-07-09	7.6	CVE-2024-35266
Microsoft--Azure DevOps Server 2022	Azure DevOps Server Spoofing Vulnerability	2024-07-09	7.6	CVE-2024-35267
Microsoft--Azure Network Watcher VM Extension	Azure Network Watcher VM Extension Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-35261
Microsoft--Microsoft Dynamics 365 (on-premises) version 9.1	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	2024-07-09	7.3	CVE-2024-30061
Microsoft--Microsoft SharePoint Enterprise Server 2016	Microsoft SharePoint Server Information Disclosure Vulnerability	2024-07-09	7.5	CVE-2024-32987
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-20701
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21308
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21317
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21331
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21332
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21333

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21335
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21373
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21398
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21414
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21415
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21428
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21449
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-28928
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-35256
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-35271
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-35272
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37319
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37320
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37321
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37322
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37323

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37326
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37327
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37328
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37329
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37330
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37331
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37332
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37333
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37336
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-38087
Microsoft--Microsoft SQL Server 2017 (GDR)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-38088
Microsoft--Microsoft SQL Server 2019 (GDR)	Microsoft OLE DB Driver for SQL Server Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37334
Microsoft--Microsoft SQL Server 2019 for x64-based Systems (CU 27)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21425
Microsoft--Microsoft SQL Server 2019 for x64-based Systems (CU 27)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37318
Microsoft--Microsoft SQL Server 2022 for (CU 13)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-21303

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Microsoft SQL Server 2022 for (CU 13)	SQL Server Native Client OLE DB Provider Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-37324
Microsoft--Microsoft Visual Studio 2022 version 17.4	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability	2024-07-09	7.3	CVE-2024-38081
Microsoft--Windows 10 Version 1809	Windows Text Services Framework Elevation of Privilege Vulnerability	2024-07-10	8.8	CVE-2024-21417
Microsoft--Windows 10 Version 1809	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8.8	CVE-2024-28899
Microsoft--Windows 10 Version 1809	Windows MultiPoint Services Remote Code Execution Vulnerability	2024-07-09	8.8	CVE-2024-30013
Microsoft--Windows 10 Version 1809	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-37969
Microsoft--Windows 10 Version 1809	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-37970
Microsoft--Windows 10 Version 1809	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-37971
Microsoft--Windows 10 Version 1809	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-37972
Microsoft--Windows 10 Version 1809	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8.4	CVE-2024-37973
Microsoft--Windows 10 Version 1809	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-37974
Microsoft--Windows 10 Version 1809	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-37975
Microsoft--Windows 10 Version 1809	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-37981
Microsoft--Windows 10 Version 1809	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8.4	CVE-2024-37984
Microsoft--Windows 10 Version 1809	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	2024-07-09	7.8	CVE-2024-30079
Microsoft--Windows 10	Windows NTLM Spoofing Vulnerability	2024-07-09	7.1	CVE-2024-30081

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Version 1809				
Microsoft--Windows 10 Version 1809	Windows Cryptographic Services Security Feature Bypass Vulnerability	2024-07-09	7.5	CVE-2024-30098
Microsoft--Windows 11 version 22H2	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-37978
Microsoft--Windows Server 2022	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	8	CVE-2024-37977
Mozilla--Firefox	A mismatch between allocator and deallocator could have lead to memory corruption. This vulnerability affects Firefox < 128 and Firefox ESR < 115.13.	2024-07-09	9.8	CVE-2024-6602 security@mozilla.org security@mozilla.org security@mozilla.org
Mozilla--Firefox	Clipboard code failed to check the index on an array access. This could have lead to an out-of-bounds read. This vulnerability affects Firefox < 128.	2024-07-09	9.8	CVE-2024-6606 security@mozilla.org security@mozilla.org
Mozilla--Firefox	A nested iframe, triggering a cross-site navigation, could send SameSite=Strict or Lax cookies. This vulnerability affects Firefox < 128.	2024-07-09	9.8	CVE-2024-6611 security@mozilla.org security@mozilla.org
Mozilla--Firefox	In an out-of-memory scenario an allocation could fail but free would have been called on the pointer afterwards leading to memory corruption. This vulnerability affects Firefox < 128 and Firefox ESR < 115.13.	2024-07-09	7.4	CVE-2024-6603 security@mozilla.org security@mozilla.org security@mozilla.org
N.O.U.S. Open Useful and Simple--Event post	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in N.O.U.S. Open Useful and Simple Event post allows PHP Local File Inclusion.This issue affects Event post: from n/a through 5.9.5.	2024-07-12	7.5	CVE-2024-38735
n/a--@discordjs/opus	All versions of the package @discordjs/opus are vulnerable to Denial of Service (DoS) due to providing an input object with a property toString to several different functions. Exploiting this vulnerability could lead to a system crash.	2024-07-10	7.5	CVE-2024-21521
n/a--audify	All versions of the package audify are vulnerable to Improper Validation of Array Index when frameSize is provided to the new OpusDecoder().decode or new OpusDecoder().decodeFloat functions it is not checked for negative values. This can lead to a process crash.	2024-07-10	7.5	CVE-2024-21522
N/A--easyappointments	A BOLA vulnerability in POST /admins allows a low privileged user to create a high privileged user (admin) in the system. This results in privilege escalation.	2024-07-09	9.9	CVE-2023-3287
N/A--easyappointments	A BOLA vulnerability in GET, PUT, DELETE /providers/{providerId} allows a low privileged user to fetch, modify or delete a privileged user (provider). This results in unauthorized access and unauthorized data manipulation.	2024-07-09	9.9	CVE-2023-38048
N/A--easyappointments	A BOLA vulnerability in GET, PUT, DELETE /appointments/{appointmentId} allows a low privileged user to fetch, modify or delete an appointment of any user (including admin). This results in unauthorized access and unauthorized data manipulation.	2024-07-09	9.9	CVE-2023-38049
N/A--easyappointments	A BOLA vulnerability in GET, PUT, DELETE /webhooks/{webhookId} allows a low privileged user to fetch, modify or delete a webhook of any user (including admin). This results in unauthorized access and unauthorized data manipulation.	2024-07-09	9.1	CVE-2023-38050
N/A--easyappointments	A BOLA vulnerability in GET, PUT, DELETE /secretaries/{secretaryId} allows a low privileged user to fetch, modify or delete a low privileged user (secretary). This results in unauthorized access and unauthorized data manipulation.	2024-07-09	9.9	CVE-2023-38051

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
N/A--easyappointments	A BOLA vulnerability in GET, PUT, DELETE /admins/{adminId} allows a low privileged user to fetch, modify or delete a high privileged user (admin). This results in unauthorized access and unauthorized data manipulation.	2024-07-09	9.9	CVE-2023-38052
N/A--easyappointments	A BOLA vulnerability in GET, PUT, DELETE /settings/{settingName} allows a low privileged user to fetch, modify or delete the settings of any user (including admin). This results in unauthorized access and unauthorized data manipulation.	2024-07-09	9.9	CVE-2023-38053
N/A--easyappointments	A BOLA vulnerability in GET, PUT, DELETE /customers/{customerId} allows a low privileged user to fetch, modify or delete a low privileged user (customer). This results in unauthorized access and unauthorized data manipulation.	2024-07-09	9.9	CVE-2023-38054
N/A--easyappointments	A BOLA vulnerability in GET, PUT, DELETE /services/{serviceId} allows a low privileged user to fetch, modify or delete the services of any user (including admin). This results in unauthorized access and unauthorized data manipulation.	2024-07-09	9.6	CVE-2023-38055
N/A--easyappointments	A BOLA vulnerability in POST /providers allows a low privileged user to create a privileged user (provider) in the system. This results in privilege escalation.	2024-07-09	8.5	CVE-2023-3288
N/A--easyappointments	A BOLA vulnerability in GET, PUT, DELETE /categories/{categoryId} allows a low privileged user to fetch, modify or delete the category of any user (including admin). This results in unauthorized access and unauthorized data manipulation.	2024-07-09	8.5	CVE-2023-38047
N/A--easyappointments	A BOLA vulnerability in POST /appointments allows a low privileged user to create an appointment for any user in the system (including admin). This results in unauthorized data manipulation.	2024-07-09	7.7	CVE-2023-3285
N/A--easyappointments	A BOLA vulnerability in POST /secretaries allows a low privileged user to create a low privileged user (secretary) in the system. This results in unauthorized data manipulation.	2024-07-09	7.7	CVE-2023-3286
N/A--easyappointments	A BOLA vulnerability in POST /services allows a low privileged user to create a service for any user in the system (including admin). This results in unauthorized data manipulation.	2024-07-09	7.7	CVE-2023-3289
n/a--images	All versions of the package images are vulnerable to Denial of Service (DoS) due to providing unexpected input types to several different functions. This makes it possible to reach an assert macro, leading to a process crash. **Note:** By providing some specific integer values (like 0) to the size function, it is possible to obtain a Segmentation fault error, leading to the process crash.	2024-07-10	7.5	CVE-2024-21523
N/A--N/A	A race condition vulnerability was discovered in how signals are handled by OpenSSH's server (sshd). If a remote attacker does not authenticate within a set time period, then sshd's SIGALRM handler is called asynchronously. However, this signal handler calls various functions that are not async-signal-safe, for example, syslog(). As a consequence of a successful attack, in the worst case scenario, an attacker may be able to perform a remote code execution (RCE) as an unprivileged user running the sshd server.	2024-07-08	7	CVE-2024-6409
n/a--n/a	An issue was discovered on Supermicro BMC firmware in select X11, X12, H12, B12, X13, H13, and B13 motherboards (and CMM6 modules). An unauthenticated user can post crafted data to the interface that triggers a stack buffer overflow, and may lead to arbitrary remote code execution on a BMC.	2024-07-11	9.8	CVE-2024-36435
n/a--n/a	14Finger v1.1 was discovered to contain a remote command execution (RCE) vulnerability in the fingerprint function. This vulnerability allows attackers to execute arbitrary commands via a crafted payload.	2024-07-10	9.1	CVE-2024-37770
n/a--n/a	SQL injection vulnerability in processscore.php in Learning Management System Project In PHP With Source Code 1.0 allows attackers to execute arbitrary SQL commands via the id parameter.	2024-07-09	9.8	CVE-2024-37870
n/a--n/a	Fujian Kelixun <=7.6.6.4391 is vulnerable to SQL Injection in send_event.php.	2024-07-09	9.8	CVE-2024-39071
n/a--n/a	A vulnerability was discovered in Samsung Mobile Processor, Wearable Processor, and Modems with versions Exynos 9820, Exynos 9825, Exynos 980, Exynos 990, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 9110, Exynos W920, Exynos W930, Exynos Modem 5123,	2024-07-09	8.1	CVE-2023-50805

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Exynos Modem 5300 that allows an out-of-bounds write in the heap in 2G (no auth).			
n/a--n/a	A vulnerability was discovered in Samsung Mobile Processor, Wearable Processor, and Modems with versions Exynos 9820, Exynos 9825, Exynos 980, Exynos 990, Exynos 850 Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380 Exynos 1330, Exynos 9110, Exynos W920, Exynos W930, Exynos Modem 5123, Exynos Modem 5300 that allows out-of-bounds access to a heap buffer in the SIM Proactive Command.	2024-07-09	8.4	CVE-2023-50806
n/a--n/a	A vulnerability was discovered in Samsung Wearable Processor and Modems with versions Exynos 9110, Exynos Modem 5123, Exynos Modem 5300 that allows an out-of-bounds write in the heap in 2G (no auth).	2024-07-09	8.1	CVE-2023-50807
n/a--n/a	A vulnerability was discovered in Samsung Mobile Processor, Wearable Processor, and Modems with versions Exynos 9820, Exynos 9825, Exynos 980, Exynos 990, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 9110, Exynos W920, Exynos W930, Exynos Modem 5123, and Exynos Modem 5300 that involves incorrect authorization of LTE NAS messages and leads to downgrading to lower network generations and repeated DDOS.	2024-07-09	8.1	CVE-2024-29153
n/a--n/a	An issue in Outline <= v0.76.1 allows attackers to execute a session hijacking attack via user interaction with a crafted magic sign-in link.	2024-07-09	8.8	CVE-2024-37829
n/a--n/a	SQL injection vulnerability in login.php in Itsourcecode Online Discussion Forum Project in PHP with Source Code 1.0 allows remote attackers to execute arbitrary SQL commands via the email parameter.	2024-07-09	8.2	CVE-2024-37871
n/a--n/a	SQL injection vulnerability in process.php in Itsourcecode Billing System in PHP 1.0 allows remote attackers to execute arbitrary SQL commands via the username parameter.	2024-07-09	8.1	CVE-2024-37872
n/a--n/a	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/userGroup_deal.php?mudi=add&nohrefStr=close	2024-07-09	8.8	CVE-2024-40036
n/a--n/a	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/softBak_deal.php?mudi=backup	2024-07-10	8.8	CVE-2024-40329
n/a--n/a	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/dbBakMySQL_deal.php?mudi=backup	2024-07-10	8.8	CVE-2024-40331
n/a--n/a	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/softBak_deal.php?mudi=del&dataID=2	2024-07-10	8.8	CVE-2024-40333
n/a--n/a	Incorrect access control in BookStack before v24.05.1 allows attackers to confirm existing system users and perform targeted notification email DoS via public facing forms.	2024-07-09	7.5	CVE-2024-36676
n/a--n/a	An issue was discovered in Django 4.2 before 4.2.14 and 5.0 before 5.0.7. urlize and urlizetrunc were subject to a potential denial of service attack via certain inputs with a very large number of brackets.	2024-07-10	7.5	CVE-2024-38875
n/a--node-stringbuilder	All versions of the package node-stringbuilder are vulnerable to Out-of-bounds Read due to incorrect memory length calculation, by calling ToBuffer, ToString, or CharAt on a StringBuilder object with a non-empty string value input. It's possible to return previously allocated memory, for example, by providing negative indexes, leading to an Information Disclosure.	2024-07-10	8.2	CVE-2024-21524
n/a--node-twain	All versions of the package node-twain are vulnerable to Improper Check or Handling of Exceptional Conditions due to the length of the source data not being checked. Creating a new twain.TwainSDK with a productName or productFamily, manufacturer, version.info property of length >= 34 chars leads to a buffer overflow vulnerability.	2024-07-10	8.3	CVE-2024-21525
n/a--speaker	All versions of the package speaker are vulnerable to Denial of Service (DoS) when providing unexpected input types to the channels property of the Speaker object makes it possible to reach an assert macro. Exploiting this vulnerability can lead to a process crash.	2024-07-10	7.5	CVE-2024-21526
NAVER--NAVER Whale browser	Whale browser before 3.26.244.21 allows an attacker to execute malicious JavaScript due to improper sanitization when processing a built-in extension.	2024-07-11	9.6	CVE-2024-40618 cve@navercorp.com
neutrinolabs--xrdp	xrdp is an open source RDP server. xrdp versions prior to 0.10.0 have a vulnerability that allows attackers to make an infinite number of login attempts. The number of max login attempts is supposed to be limited by a configuration parameter `MaxLoginRetry` in `/etc/xrdp/sesman.ini`. However, this mechanism was not effectively working. As a result, xrdp allows an infinite number of login attempts.	2024-07-12	7.2	CVE-2024-39917
nikolaystrikhar--Gutenberg Forms WordPress Form	The Gutenberg Forms plugin for WordPress is vulnerable to arbitrary file uploads due to the users can specify the allowed file types in the 'upload' function in versions up to, and including, 2.2.9. This makes it possible for unauthenticated	2024-07-09	9.8	CVE-2024-6313

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Builder Plugin	attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.			
NooTheme--Jobmonster	Improper Privilege Management vulnerability in NooTheme Jobmonster allows Privilege Escalation.This issue affects Jobmonster: from n/a through 4.7.0.	2024-07-12	9.8	CVE-2024-37927
NooTheme--Jobmonster	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in NooTheme Jobmonster allows File Manipulation.This issue affects Jobmonster: from n/a through 4.7.0.	2024-07-12	8.6	CVE-2024-37928
oisf -- suricata	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Mishandling of multiple fragmented packets using the same IP ID value can lead to packet reassembly failure, which can lead to policy bypass. Upgrade to 7.0.6 or 6.0.20. When using af-packet, enable `defrag` to reduce the scope of the problem.	2024-07-11	7.5	CVE-2024-37151
oisf -- suricata	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Crafted modbus traffic can lead to unlimited resource accumulation within a flow. Upgrade to 7.0.6. Set a limited stream.reassembly.depth to reduce the issue.	2024-07-11	7.5	CVE-2024-38534
oisf -- suricata	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. Suricata can run out of memory when parsing crafted HTTP/2 traffic. Upgrade to 6.0.20 or 7.0.6.	2024-07-11	7.5	CVE-2024-38535
oisf -- suricata	Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine. A memory allocation failure due to `http.memcap` being reached leads to a NULL-ptr reference leading to a crash. Upgrade to 7.0.6.	2024-07-11	7.5	CVE-2024-38536
openvpn -- openvpn	OpenVPN plug-ins on Windows with OpenVPN 2.6.9 and earlier could be loaded from any directory, which allows an attacker to load an arbitrary plug-in which can be used to interact with the privileged OpenVPN interactive service.	2024-07-08	9.8	CVE-2024-27903
openvpn -- openvpn	The interactive service in OpenVPN 2.6.9 and earlier allows the OpenVPN service pipe to be accessed remotely, which allows a remote attacker to interact with the privileged OpenVPN interactive service.	2024-07-08	7.5	CVE-2024-24974
openvpn -- openvpn	The interactive service in OpenVPN 2.6.9 and earlier allows an attacker to send data causing a stack overflow which can be used to execute arbitrary code with more privileges.	2024-07-08	7.8	CVE-2024-27459
OpenVPN--tap-windows6	tap-windows6 driver version 9.26 and earlier does not properly check the size data of incomming write operations which an attacker can use to overflow memory buffers, resulting in a bug check and potentially arbitrary code execution in kernel space	2024-07-08	9.8	CVE-2024-1305
Paid Memberships Pro--Paid Memberships Pro	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Paid Memberships Pro.This issue affects Paid Memberships Pro: from n/a through 3.0.5.	2024-07-09	7.6	CVE-2024-37486
pandavideo--Panda Video	The Panda Video plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.4.0 via the 'selected_button' 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.	2024-07-09	8.8	CVE-2024-5456
parorrey -- json_api_user	The JSON API User plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 3.9.3. This is due to improper controls on custom user meta fields. This makes it possible for unauthenticated attackers to register as administrators on the site. The plugin requires the JSON API plugin to also be installed.	2024-07-11	9.8	CVE-2024-6624
PayPlus LTD--PayPlus Payment Gateway	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in PayPlus LTD PayPlus Payment Gateway.This issue affects PayPlus Payment Gateway: from n/a through 7.0.7.	2024-07-12	8.5	CVE-2024-37564
Pepperl+Fuchs--OIT1500-F113-B12-CB	An unauthenticated remote attacker can manipulate the device via Telnet, stop processes, read, delete and change data.	2024-07-10	9.8	CVE-2024-6422

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Pepperl+Fuchs--OIT1500-F113-B12-CB	An unauthenticated remote attacker can read out sensitive device information through a incorrectly configured FTP service.	2024-07-10	7.5	CVE-2024-6421
photoweblog--OSM OpenStreetMap	The OSM - OpenStreetMap plugin for WordPress is vulnerable to SQL Injection via the 'tagged_filter' attribute of the 'osm_map_v3' shortcode in all versions up to, and including, 6.0.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-07-09	9.9	CVE-2024-3604
phpvibe -- phpvibe	Directory Travel in PHPVibe v11.0.46 due to incomplete blacklist checksums and directory checks, which can lead to code execution via writing specific statements to .htaccess and code to a file with a .png suffix.	2024-07-09	9.8	CVE-2024-39171
pjgalbraith--Default Thumbnail Plus	The Default Thumbnail Plus plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'get_cache_image' function in all versions up to, and including, 1.0.2.3. This makes it possible for authenticated attackers, with contributor-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-07-09	8.8	CVE-2024-6161
PluginsWare--Advanced Classifieds & Directory Pro	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in PluginsWare Advanced Classifieds & Directory Pro allows Path Traversal.This issue affects Advanced Classifieds & Directory Pro: from n/a through 3.1.3.	2024-07-09	8.5	CVE-2024-37501
praveen-rajan--Attachment File Icons (AF Icons)	The Attachment File Icons (AF Icons) plugin for WordPress is vulnerable to Cross-Site Request Forgery to Arbitrary File Upload in versions up to, and including, 1.3. This is due to missing nonce validation in the 'afi_overview' function and missing file type validation in the 'upload_icons' function. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-07-09	8.8	CVE-2024-6309
publiccms -- publiccms	PublicCMS v4.0.202302.e was discovered to contain a Server-Side Request Forgery (SSRF) via the component /admin/ueditor?action=catchimage.	2024-07-12	8.8	CVE-2024-40543
publiccms -- publiccms	PublicCMS v4.0.202302.e was discovered to contain a Server-Side Request Forgery (SSRF) via the component /admin/#maintenance_sysTask/edit.	2024-07-12	8.8	CVE-2024-40544
publiccms -- publiccms	An arbitrary file upload vulnerability in the component /admin/cmsWebFile/doUpload of PublicCMS v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file.	2024-07-12	8.8	CVE-2024-40545
publiccms -- publiccms	An arbitrary file upload vulnerability in the component /admin/cmsWebFile/save of PublicCMS v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file.	2024-07-12	8.8	CVE-2024-40546
publiccms -- publiccms	An arbitrary file upload vulnerability in the component /admin/cmsTemplate/save of PublicCMS v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file.	2024-07-12	8.8	CVE-2024-40548
publiccms -- publiccms	An arbitrary file upload vulnerability in the component /admin/cmsTemplate/savePlace of PublicCMS v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file.	2024-07-12	8.8	CVE-2024-40549
publiccms -- publiccms	An arbitrary file upload vulnerability in the component /admin/cmsTemplate/savePlaceMetaData of Public CMS v.4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file.	2024-07-12	8.8	CVE-2024-40550
publiccms -- publiccms	An arbitrary file upload vulnerability in the component /admin/cmsTemplate/doUpload of PublicCMS v4.0.202302.e allows attackers to execute arbitrary code via uploading a crafted file.	2024-07-12	8.8	CVE-2024-40551
publiccms -- publiccms	PublicCMS v4.0.202302.e was discovered to contain a remote commande execution (RCE) vulnerability via the cmdarray parameter at /site/ScriptComponent.java.	2024-07-12	8.8	CVE-2024-40552
realtek -- rtl819x_jungle_software_development_kit	A cross-site request forgery (csrf) vulnerability exists in the boa CSRF protection functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted network request can lead to CSRF. An attacker can send an HTTP request to trigger this vulnerability.	2024-07-08	8.8	CVE-2023-47677
realtek -- rtl819x_jungle_sof	A firmware update vulnerability exists in the boa formUpload functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted network packets can lead to	2024-07-08	7.2	CVE-2023-34435

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tware_developme nt_kit	arbitrary firmware update. An attacker can provide a malicious file to trigger this vulnerability.			
realtek -- rtl819x_jungle_sof tware_developme nt_kit	A stack-based buffer overflow vulnerability exists in the boa formRoute functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send an HTTP request to trigger this vulnerability.	2024-07-08	7.2	CVE-2023-41251
realtek -- rtl819x_jungle_sof tware_developme nt_kit	A stack-based buffer overflow vulnerability exists in the boa setRepeaterSsid functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability.	2024-07-08	7.2	CVE-2023-45215
realtek -- rtl819x_jungle_sof tware_developme nt_kit	An integer overflow vulnerability exists in the boa updateConfigIntoFlash functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability.	2024-07-08	7.2	CVE-2023-45742
realtek -- rtl819x_jungle_sof tware_developme nt_kit	A stack-based buffer overflow vulnerability exists in the boa set_RadvdPrefixParam functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.	2024-07-08	7.2	CVE-2023-47856
realtek -- rtl819x_jungle_sof tware_developme nt_kit	A stack-based buffer overflow vulnerability exists in the boa formDnsv6 functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability.	2024-07-08	7.2	CVE-2023-48270
realtek -- rtl819x_jungle_sof tware_developme nt_kit	A stack-based buffer overflow vulnerability exists in the boa formFilter functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability.	2024-07-08	7.2	CVE-2023-49073
realtek -- rtl819x_jungle_sof tware_developme nt_kit	A stack-based buffer overflow vulnerability exists in the boa rollback_control_code functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to arbitrary code execution. An attacker can send a sequence of requests to trigger this vulnerability.	2024-07-08	7.2	CVE-2023-49595
realtek -- rtl819x_jungle_sof tware_developme nt_kit	A stack-based buffer overflow vulnerability exists in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger this vulnerability.	2024-07-08	7.2	CVE-2023-49867
realtek -- rtl819x_jungle_sof tware_developme nt_kit	Two stack-based buffer overflow vulnerabilities exist in the boa set_RadvdInterfaceParam functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `interfacename` request's parameter.	2024-07-08	7.2	CVE-2023-50239
realtek -- rtl819x_jungle_sof tware_developme nt_kit	Two stack-based buffer overflow vulnerabilities exist in the boa set_RadvdInterfaceParam functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `AdvDefaultPreference` request's parameter.	2024-07-08	7.2	CVE-2023-50240
realtek -- rtl819x_jungle_sof tware_developme nt_kit	Two stack-based buffer overflow vulnerabilities exist in the boa formIpQoS functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `comment` request's parameter.	2024-07-08	7.2	CVE-2023-50243
realtek -- rtl819x_jungle_sof tware_developme nt_kit	Two stack-based buffer overflow vulnerabilities exist in the boa formIpQoS functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This stack-based buffer overflow is related to the `entry_name` request's parameter.	2024-07-08	7.2	CVE-2023-50244

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
realtek -- rtl819x_jungle_software_development_kit	A stack-based buffer overflow vulnerability exists in the boa getInfo functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to remote code execution. An attacker can send a series of HTTP requests to trigger this vulnerability.	2024-07-08	7.2	CVE-2023-50330
realtek -- rtl819x_jungle_software_development_kit	Three os command injection vulnerabilities exist in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `targetAPSsid` request's parameter.	2024-07-08	7.2	CVE-2023-50381
realtek -- rtl819x_jungle_software_development_kit	Three os command injection vulnerabilities exist in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `peerPin` request's parameter.	2024-07-08	7.2	CVE-2023-50382
realtek -- rtl819x_jungle_software_development_kit	Three os command injection vulnerabilities exist in the boa formWsc functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted series of HTTP requests can lead to arbitrary command execution. An attacker can send a series of HTTP requests to trigger these vulnerabilities.This command injection is related to the `localPin` request's parameter.	2024-07-08	7.2	CVE-2023-50383
realtek -- rtl819x_jungle_software_development_kit	A heap-based buffer overflow vulnerability exists in the configuration file mib_init_value_array functionality of Realtek rtl819x Jungle SDK v3.4.11. A specially crafted .dat file can lead to arbitrary code execution. An attacker can upload a malicious file to trigger this vulnerability.	2024-07-08	7.2	CVE-2024-21778
Realtyna--Realtyna Organic IDX plugin	Unrestricted Upload of File with Dangerous Type vulnerability in Realtyna Realtyna Organic IDX plugin allows Code Injection.This issue affects Realtyna Organic IDX plugin: from n/a through 4.14.13.	2024-07-12	9.1	CVE-2024-38736
Red Hat--Red Hat JBoss Enterprise Application Platform 8	A vulnerability was found in Undertow, where the chunked response hangs after the body was flushed. The response headers and body were sent but the client would continue waiting as Undertow does not send the expected 0\r\n termination of the chunked response. This results in uncontrolled resource consumption, leaving the server side to a denial of service attack. This happens only with Java 17 TLSv1.3 scenarios.	2024-07-08	7.5	CVE-2024-5971
rmac0001--IQ Testimonials	The IQ Testimonials plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the 'process_image_upload' function in versions up to, and including, 2.2.7. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. This can only be exploited if the 'gd' php extension is not loaded on the server.	2024-07-09	9.8	CVE-2024-6314
samsung -- exynos_1280_firmware	A vulnerability was discovered in Samsung Mobile Processors Exynos 1280, Exynos 2200, Exynos 1330, Exynos 1380, and Exynos 2400 where they do not properly check the length of the data, which can lead to a Information disclosure.	2024-07-09	7.5	CVE-2024-27362
samsung -- exynos_2200_firmware	A vulnerability was discovered in Samsung Mobile Processors Exynos 2200 and Exynos 2400 where they lack a check for the validation of native handles, which can result in a DoS(Denial of Service) attack by unmapping an invalid length.	2024-07-09	7.5	CVE-2024-31957
samsung -- exynos_850_firmware	A vulnerability was discovered in Samsung Mobile Processors Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, and Exynos W930 where they do not properly check length of the data, which can lead to a Denial of Service.	2024-07-09	7.5	CVE-2024-27360
SAP_SE--SAP Commerce	In SAP Commerce, a user can misuse the forgotten password functionality to gain access to a Composable Storefront B2B site for which early login and registration is activated, without requiring the merchant to approve the account beforehand. If the site is not configured as isolated site, this can also grant access to other non-isolated early login sites, even if registration is not enabled for those other sites.	2024-07-09	7.2	CVE-2024-39597
SAP_SE--SAP PDCE	Elements of PDCE does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This allows an attacker to read sensitive information causing high impact on the confidentiality of the application.	2024-07-09	7.7	CVE-2024-39592
schneider-electric -- ecostruxure_foxboro_dcs_control_co	CWE-787: Out-of-Bounds Write vulnerability exists that could cause local denial-of-service, or kernel memory leak when a malicious actor with local user access crafts a script/program using an IOCTL call in the Foxboro.sys driver.	2024-07-11	7.1	CVE-2024-5679 cybersecurity@se.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
re_services				
schneider-electric -- ecostruxure_foxboro_dcs_control_core_services	CWE-20: Improper Input Validation vulnerability exists that could cause local denial-of-service, privilege escalation, and potentially kernel execution when a malicious actor with local user access crafts a script/program using an IOCTL call in the Foxboro.sys driver.	2024-07-11	7.8	CVE-2024-5681 cybersecurity@se.com
schneider-electric -- foxrtu_station	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could result in remote code execution when an authenticated user executes a saved project file that has been tampered by a malicious actor.	2024-07-11	7.8	CVE-2024-2602 cybersecurity@se.com
schneider-electric -- whc-5918a_firmware	CWE-200: Information Exposure vulnerability exists that could cause disclosure of credentials when a specially crafted message is sent to the device.	2024-07-11	7.5	CVE-2024-6407 cybersecurity@se.com
seacms -- seacms	SeaCMS 12.9 has a remote code execution vulnerability. The vulnerability is caused by admin_weixin.php directly splicing and writing the user input data into weixin.php without processing it, which allows authenticated attackers to exploit the vulnerability to execute arbitrary commands and obtain system permissions.	2024-07-12	8.8	CVE-2024-40518
seacms -- seacms	SeaCMS 12.9 has a remote code execution vulnerability. The vulnerability is caused by admin_smtp.php directly splicing and writing the user input data into weixin.php without processing it, which allows authenticated attackers to exploit the vulnerability to execute arbitrary commands and obtain system permissions.	2024-07-12	8.8	CVE-2024-40519
seacms -- seacms	SeaCMS 12.9 has a remote code execution vulnerability. The vulnerability is caused by admin_config_mark.php directly splicing and writing the user input data into inc_photowatermark_config.php without processing it, which allows authenticated attackers to exploit the vulnerability to execute arbitrary commands and obtain system permissions.	2024-07-12	8.8	CVE-2024-40520
seacms -- seacms	SeaCMS 12.9 has a remote code execution vulnerability. The vulnerability is due to the fact that although admin_template.php imposes certain restrictions on the edited file, attackers can still bypass the restrictions and write code in some way, allowing authenticated attackers to exploit the vulnerability to execute arbitrary commands and gain system privileges.	2024-07-12	8.8	CVE-2024-40521
seacms -- seacms	There is a remote code execution vulnerability in SeaCMS 12.9. The vulnerability is caused by phomebak.php writing some variable names passed in without filtering them before writing them into the php file. An authenticated attacker can exploit this vulnerability to execute arbitrary commands and obtain system permissions.	2024-07-12	8.8	CVE-2024-40522
Seraphinite Solutions--Seraphinite Accelerator (Full, premium)	Cross-Site Request Forgery (CSRF) vulnerability in Seraphinite Solutions Seraphinite Accelerator (Full, premium).This issue affects Seraphinite Accelerator (Full, premium): from n/a through 2.21.13.	2024-07-12	7.4	CVE-2024-37940
ServiceNow--Now Platform	ServiceNow has addressed an input validation vulnerability that was identified in Vancouver and Washington DC Now Platform releases. This vulnerability could enable an unauthenticated user to remotely execute code within the context of the Now Platform.Â ServiceNow applied an update to hosted instances, and ServiceNow released the update to our partners and self-hosted customers. Listed below are the patches and hot fixes that address the vulnerability. If you have not done so already, we recommend applying security patches relevant to your instance as soon as possible.	2024-07-10	9.8	CVE-2024-4879
ServiceNow--Now Platform	ServiceNow has addressed an input validation vulnerability that was identified in the Washington DC, Vancouver, and earlier Now Platform releases. This vulnerability could enable an unauthenticated user to remotely execute code within the context of the Now Platform.Â The vulnerability is addressed in the listed patches and hot fixes below, which were released during the June 2024 patching cycle. If you have not done so already, we recommend applying security patches relevant to your instance as soon as possible.	2024-07-10	9.8	CVE-2024-5217
siemens -- medicalis_workflow_orchestrator	A vulnerability has been identified in Medicalis Workflow Orchestrator (All versions). The affected application executes as a trusted account with high privileges and network access. This could allow an authenticated local attacker to escalate privileges.	2024-07-08	7.8	CVE-2024-37999
Siemens--JT Open	A vulnerability has been identified in JT Open (All versions < V11.5), PLM XML SDK (All versions < V7.1.0.014). The affected applications contain a stack based	2024-07-09	7.8	CVE-2024-37997

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	overflow vulnerability while parsing specially crafted XML files. This could allow an attacker to execute code in the context of the current process.			
Siemens--Mendix Encryption	A vulnerability has been identified in Mendix Encryption (All versions >= V10.0.0 < V10.0.2). Affected versions of the module define a specific hard-coded default value for the EncryptionKey constant, which is used in projects where no individual EncryptionKey was specified. This could allow to an attacker to decrypt any encrypted project data, as the default encryption key can be considered compromised.	2024-07-09	7.5	CVE-2024-39888
Siemens--RUGGEDCOM i800	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC, RUGGEDCOM i802, RUGGEDCOM i802NC, RUGGEDCOM i803, RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM M2100NC, RUGGEDCOM M2200, RUGGEDCOM M2200NC, RUGGEDCOM M969, RUGGEDCOM M969NC, RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC, RUGGEDCOM RS400, RUGGEDCOM RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC, RUGGEDCOM RS416, RUGGEDCOM RS416NC, RUGGEDCOM RS416NCv2 V4.X, RUGGEDCOM RS416NCv2 V5.X, RUGGEDCOM RS416P, RUGGEDCOM RS416PNC, RUGGEDCOM RS416PNCv2 V4.X, RUGGEDCOM RS416PNCv2 V5.X, RUGGEDCOM RS416Pv2 V4.X, RUGGEDCOM RS416Pv2 V5.X, RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC, RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GNC, RUGGEDCOM RS900GNC(32M) V4.X, RUGGEDCOM RS900GNC(32M) V5.X, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPNC, RUGGEDCOM RS900L, RUGGEDCOM RS900LNC, RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-GETS-XX, RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM RS900MNC-STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM RS900NC(32M) V4.X, RUGGEDCOM RS900NC(32M) V5.X, RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GNC, RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200NC, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300NC V4.X, RUGGEDCOM RSG2300NC V5.X, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488NC V4.X, RUGGEDCOM RSG2488NC V5.X, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM RSL910, RUGGEDCOM RSL910NC, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. The web server of the affected devices allow a low privileged user to access hashes and password salts of all system's users, including admin users. An attacker could use the obtained information to brute force the passwords offline.	2024-07-09	7.5	CVE-2023-52237
Siemens--RUGGEDCOM RMC30	A vulnerability has been identified in RUGGEDCOM RMC30 (All versions < V4.3.10), RUGGEDCOM RMC30NC (All versions < V4.3.10), RUGGEDCOM RP110 (All versions < V4.3.10), RUGGEDCOM RP110NC (All versions < V4.3.10), RUGGEDCOM RS400 (All versions < V4.3.10), RUGGEDCOM RS400NC (All versions < V4.3.10), RUGGEDCOM RS401 (All versions < V4.3.10), RUGGEDCOM RS401NC (All versions < V4.3.10), RUGGEDCOM RS416 (All versions < V4.3.10), RUGGEDCOM RS416NC (All versions < V4.3.10), RUGGEDCOM RS416NCv2 V4.X (All versions < V4.3.10),	2024-07-09	8.8	CVE-2024-39675

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	RUGGEDCOM RS416NCv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416P (All versions < V4.3.10), RUGGEDCOM RS416PNC (All versions < V4.3.10), RUGGEDCOM RS416PNCv2 V4.X (All versions < V4.3.10), RUGGEDCOM RS416PNCv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416Pv2 V4.X (All versions < V4.3.10), RUGGEDCOM RS416Pv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416v2 V4.X (All versions < V4.3.10), RUGGEDCOM RS416v2 V5.X (All versions < V5.9.0), RUGGEDCOM RS910 (All versions < V4.3.10), RUGGEDCOM RS910L (All versions), RUGGEDCOM RS910LNC (All versions), RUGGEDCOM RS910NC (All versions < V4.3.10), RUGGEDCOM RS910W (All versions < V4.3.10), RUGGEDCOM RS920L (All versions), RUGGEDCOM RS920LNC (All versions), RUGGEDCOM RS920W (All versions). In some configurations the affected products wrongly enable the Modbus service in non-managed VLANS. Only serial devices are affected by this vulnerability.			
Siemens--SIMATIC PCS neo V4.0	A vulnerability has been identified in SIMATIC PCS neo V4.0 (All versions), SIMATIC STEP 7 V16 (All versions), SIMATIC STEP 7 V17 (All versions), SIMATIC STEP 7 V18 (All versions < V18 Update 2). Affected applications do not properly restrict the .NET BinaryFormatter when deserializing user-controllable input. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application. This is the same issue that exists for .NET BinaryFormatter https://docs.microsoft.com/en-us/visualstudio/code-quality/ca2300.	2024-07-09	7.8	CVE-2022-45147
Siemens--Simcenter Femap	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted IGS part file. This could allow an attacker to execute code in the context of the current process.	2024-07-09	7.8	CVE-2024-32056
Siemens--Simcenter Femap	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted BMP files. This could allow an attacker to execute code in the context of the current process.	2024-07-09	7.8	CVE-2024-33653
Siemens--Simcenter Femap	A vulnerability has been identified in Simcenter Femap (All versions < V2406). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted BMP files. This could allow an attacker to execute code in the context of the current process.	2024-07-09	7.8	CVE-2024-33654
Siemens--SINEMA Remote Connect Client	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 HF1). The system service of affected applications is vulnerable to command injection due to missing server side input sanitation when loading VPN configurations. This could allow an authenticated local attacker to execute arbitrary code with system privileges.	2024-07-09	7.8	CVE-2024-39567
Siemens--SINEMA Remote Connect Client	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 HF1). The system service of affected applications is vulnerable to command injection due to missing server side input sanitation when loading proxy configurations. This could allow an authenticated local attacker to execute arbitrary code with system privileges.	2024-07-09	7.8	CVE-2024-39568
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application does not properly assign rights to temporary files created during its update process. This could allow an authenticated attacker with the 'Manage firmware updates' role to escalate their privileges on the underlying OS level.	2024-07-09	9.6	CVE-2024-39872
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 HF1). Affected applications are vulnerable to command injection due to missing server side input sanitation when loading VxLAN configurations. This could allow an authenticated attacker to execute arbitrary code with root privileges.	2024-07-09	8.8	CVE-2024-39570
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 HF1). Affected applications are vulnerable to command injection due to missing server side input sanitation when loading SNMP configurations. This could allow an attacker with the right to modify the SNMP configuration to execute arbitrary code with root privileges.	2024-07-09	8.8	CVE-2024-39571
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application allows users to upload encrypted backup files. As part of this backup, files can be restored without correctly checking the path of the restored file. This could allow an attacker with access to the backup encryption key to upload malicious files, that could potentially lead to remote code execution.	2024-07-09	8.8	CVE-2024-39865
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application allows users to upload encrypted backup files. This could allow an attacker with access to the backup encryption key and with the right to upload backup files to create a user with administrative privileges.	2024-07-09	8.8	CVE-2024-39866

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected devices do not properly validate the authentication when performing certain actions in the web interface allowing an unauthenticated attacker to access and edit device configuration information of devices for which they have no privileges.	2024-07-09	7.6	CVE-2024-39867
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected devices do not properly validate the authentication when performing certain actions in the web interface allowing an unauthenticated attacker to access and edit VxLAN configuration information of networks for which they have no privileges.	2024-07-09	7.6	CVE-2024-39868
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application does not properly implement brute force protection against user credentials in its web API. This could allow an attacker to learn user credentials that are vulnerable to brute force attacks.	2024-07-09	7.5	CVE-2024-39873
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application does not properly implement brute force protection against user credentials in its Client Communication component. This could allow an attacker to learn user credentials that are vulnerable to brute force attacks.	2024-07-09	7.5	CVE-2024-39874
Smartypants--SP Project & Document Manager	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Smartypants SP Project & Document Manager allows Path Traversal.This issue affects SP Project & Document Manager: from n/a through 4.71.	2024-07-09	7.5	CVE-2024-37224
smub--User Feedback Create Interactive Feedback Form, User Surveys, and Polls in Seconds	The User Feedback - Create Interactive Feedback Form, User Surveys, and Polls in Seconds plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the name parameter in all versions up to, and including, 1.0.15 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in feedback form responses that will execute whenever a high-privileged user tries to view them.	2024-07-12	7.2	CVE-2024-5902
SpreadsheetConverter--Import Spreadsheets from Microsoft Excel	Unrestricted Upload of File with Dangerous Type vulnerability in SpreadsheetConverter Import Spreadsheets from Microsoft Excel allows Code Injection.This issue affects Import Spreadsheets from Microsoft Excel: from n/a through 10.1.4.	2024-07-12	9.1	CVE-2024-38734
Spring by VMware Tanzu--Spring Cloud Function Framework	In Spring Cloud Function framework, versions 4.1.x prior to 4.1.2, 4.0.x prior to 4.0.8 an application is vulnerable to a DOS attack when attempting to compose functions with non-existing functions. Specifically, an application is vulnerable when all of the following are true: User is using Spring Cloud Function Web module Affected Spring Products and Versions Spring Cloud Function Framework 4.1.0 to 4.1.2 4.0.0 to 4.0.8 References https://spring.io/security/cve-2022-22979 Â https://checkmarx.com/blog/spring-function-cloud-dos-cve-2022-22979-and-unintended-function-invocation/ Â History 2020-01-16: Initial vulnerability report published.	2024-07-09	8.2	CVE-2024-22271
StylemixThemes--Masterstudy Elementor Widgets	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in StylemixThemes Masterstudy Elementor Widgets, StylemixThemes Consulting Elementor Widgets.This issue affects Masterstudy Elementor Widgets: from n/a through 1.2.2; Consulting Elementor Widgets: from n/a through 1.3.0.	2024-07-09	8.5	CVE-2024-37090
subratamal--Wallet for WooCommerce	The Wallet for WooCommerce plugin for WordPress is vulnerable to SQL Injection via the 'search[value]' parameter in all versions up to, and including, 1.5.4 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 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.	2024-07-12	8.8	CVE-2024-6353
Tencent--RapidJSON	Tencent RapidJSON is vulnerable to privilege escalation due to an integer underflow in the `GenericReader::ParseNumber()` function of `include/rapidjson/reader.h` when parsing JSON text from a stream. An attacker needs to send the victim a crafted file which needs to be opened; this triggers the integer underflow vulnerability (when the file is parsed), leading to elevation of privilege.	2024-07-09	7.8	CVE-2024-38517

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Tencent--RapidJSON	Tencent RapidJSON is vulnerable to privilege escalation due to an integer overflow in the `GenericReader::ParseNumber()` function of `include/rapidjson/reader.h` when parsing JSON text from a stream. An attacker needs to send the victim a crafted file which needs to be opened; this triggers the integer overflow vulnerability (when the file is parsed), leading to elevation of privilege.	2024-07-09	7.8	CVE-2024-39684
tenda --ac8v4_firmware	Vulnerability in Tenda AC8v4 .V16.03.34.09 due to sscanf and the last digit of s8 being overwritten with \x0. After executing set_client_qos, control over the gp register can be obtained.	2024-07-09	9.8	CVE-2023-48194
themeenergy--BookYourTravel	Improper Privilege Management vulnerability in themeenergy BookYourTravel allows Privilege Escalation.This issue affects BookYourTravel: from n/a through 8.18.17.	2024-07-09	8.8	CVE-2024-37952
Themeum--Tutor LMS	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Tutor LMS.This issue affects Tutor LMS: from n/a through 2.7.1.	2024-07-09	7.6	CVE-2024-37256
Themewinter--WPCafe	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Themewinter WPCafe allows Path Traversal.This issue affects WPCafe: from n/a through 2.2.27.	2024-07-09	8.5	CVE-2024-37513
Unknown--ContentLock	The ContentLock WordPress plugin through 1.0.3 does not have CSRF check in place when deleting groups or emails, which could allow attackers to make a logged in admin remove them via a CSRF attack	2024-07-12	8.8	CVE-2024-6024
Unknown--SEOPress	The SEOPress WordPress plugin before 7.9 does not properly protect some of its REST API routes, which combined with another Object Injection vulnerability can allow unauthenticated attackers to unserialize malicious gadget chains, compromising the site if a suitable chain is present.	2024-07-09	9.8	CVE-2024-5488
unlimited-elements --unlimited_elements_for_elementor_\(free_widgets\,_addons\,_templates\)	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to time-based SQL Injection via the 'addons_order' parameter in all versions up to, and including, 1.5.112 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 and granted plugin setting edit permissions by an administrator, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-07-09	8.8	CVE-2024-6166
vercel--next.js	Next.js is a React framework. A Denial of Service (DoS) condition was identified in Next.js. Exploitation of the bug can trigger a crash, affecting the availability of the server. his vulnerability was resolved in Next.js 13.5 and later.	2024-07-10	7.5	CVE-2024-39693
vmware --aria_automation	VMware Aria Automation does not apply correct input validation which allows for SQL-injection in the product.Â An authenticated malicious user could enter specially crafted SQL queries and perform unauthorised read/write operations in the database.	2024-07-11	8.1	CVE-2024-22280
vnotex--vnote	VNote is a note-taking platform. Prior to 3.18.1, a code execution vulnerability existed in VNote, which allowed an attacker to execute arbitrary programs on the victim's system. A crafted URI can be used in a note to perform this attack using file:/// as a link. For example, file:///C:/WINDOWS/system32/cmd.exe. This allows attackers to execute arbitrary programs by embedding a reference to a local executable file such as file:///C:/WINDOWS/system32/cmd.exe and file:///C:/WINDOWS/system32/calc.exe. This vulnerability can be exploited by creating and sharing specially crafted notes. An attacker could send a crafted note file and perform further attacks. This vulnerability is fixed in 3.18.1.	2024-07-11	8.8	CVE-2024-39904
WatchGuard--Fireware OS	A buffer overflow in WatchGuard Fireware OS could may allow an authenticated remote attacker with privileged management access to execute arbitrary code with system privileges on the firewall. This issue affects Fireware OS: from 11.9.6 through 12.10.3.	2024-07-09	7.2	CVE-2024-5974 5d1c2695-1a31-4499-88ae-e847036fd7e3
WatchGuard--Mobile VPN with SSL Client	A local privilege escalation vlnerability in the WatchGuard Mobile VPN with SSL client on Windows enables a local user to execute arbitrary commands with elevated privileged.	2024-07-09	7.8	CVE-2024-4944 5d1c2695-1a31-4499-88ae-e847036fd7e3
Webmin--Webmin	Improper handling of insufficient permissions or privileges vulnerability exists in ajaxterm module of Webmin prior to 2.003. If this vulnerability is exploited, a console session may be hijacked by an unauthorized user. As a result, data within a system may be referred, a webpage may be altered, or a server may be permanently halted.	2024-07-10	8.8	CVE-2024-36451
webnus --modern_events_calendar	The Modern Events Calendar plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the set_featured_image function in all versions up to, and including, 7.11.0. This makes it possible for authenticated attackers, with subscriber access and above, to upload arbitrary files on the	2024-07-09	8.8	CVE-2024-5441

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	affected site's server which may make remote code execution possible. The plugin allows administrators (via its settings) to extend the ability to submit events to unauthenticated users, which would allow unauthenticated attackers to exploit this vulnerability.			
wedevs -- wp_erp	The WP ERP plugin for WordPress is vulnerable to SQL Injection via the 'vendor_id' parameter in all versions up to, and including, 1.13.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Accounting Manager access (erp_ac_view_sales_summary capability) and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2024-07-11	8.8	CVE-2024-6666
whisperfish--rust-phonenumber	phonenumber is a library for parsing, formatting and validating international phone numbers. Since 0.3.4, the phonenumber parsing code may panic due to a panic-guarded out-of-bounds access on the phonenumber string. In a typical deployment of rust-phonenumber, this may get triggered by feeding a maliciously crafted phonenumber, e.g. over the network, specifically strings of the form `+dwPAA;phone-context=AA`, where the "number" part potentially parses as a number larger than 2^56. This vulnerability is fixed in 0.3.6.	2024-07-09	8.6	CVE-2024-39697
widgetti--solara	Solara is a pure Python, React-style framework for scaling Jupyter and web apps. A Local File Inclusion (LFI) vulnerability was identified in widgetti/solara, in version <1.35.1, which was fixed in version 1.35.1. This vulnerability arises from the application's failure to properly validate URI fragments for directory traversal sequences such as '../' when serving static files. An attacker can exploit this flaw by manipulating the fragment part of the URI to read arbitrary files on the local file system.	2024-07-12	8.6	CVE-2024-39903
woobewoo--Product Table by WBW	The Product Table by WBW plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 2.0.1 via the 'saveCustomTitle' function. This is due to missing authorization and lack of sanitization of appended data in the languages/customTitle.php file. This makes it possible for unauthenticated attackers to execute code on the server.	2024-07-09	9.8	CVE-2024-6365
WPJohnny, zerOneIT--Comment Reply Email	Cross-Site Request Forgery (CSRF) vulnerability in WPJohnny, zerOneIT Comment Reply Email allows Cross-Site Scripting (XSS).This issue affects Comment Reply Email: from n/a through 1.3.	2024-07-12	7.1	CVE-2024-35773
wpvibes--Form Vibes Database Manager for Forms	The Form Vibes plugin for WordPress is vulnerable to SQL Injection via the 'fv_export_data' parameter in all versions up to, and including, 1.4.10 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.	2024-07-12	8.8	CVE-2024-5325
WPZita--Zita Elementor Site Library	Unrestricted Upload of File with Dangerous Type vulnerability in WPZita Zita Elementor Site Library allows Upload a Web Shell to a Web Server.This issue affects Zita Elementor Site Library: from n/a through 1.6.1.	2024-07-09	9.9	CVE-2024-37420
zealopensource--Generate PDF using Contact Form 7	The Generate PDF using Contact Form 7 plugin for WordPress is vulnerable to Cross-Site Request Forgery to Arbitrary File Upload in versions up to, and including, 4.0.6. This is due to missing nonce validation and missing file type validation in the 'wp_cf7_pdf_dashboard_html_page' function. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-07-09	8.8	CVE-2024-6316
zealopensource--Generate PDF using Contact Form 7	The Generate PDF using Contact Form 7 plugin for WordPress is vulnerable to Cross-Site Request Forgery to Arbitrary File Upload in versions up to, and including, 4.0.6. This is due to missing nonce validation and the plugin not properly validating a file or its path prior to deleting it in the 'wp_cf7_pdf_dashboard_html_page' function. 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 via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-07-09	8.8	CVE-2024-6317
ZealousWeb--Generate PDF using Contact	Unrestricted Upload of File with Dangerous Type vulnerability in ZealousWeb Generate PDF using Contact Form 7.This issue affects Generate PDF using Contact Form 7: from n/a through 4.0.6.	2024-07-09	9.1	CVE-2024-37555

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Form 7				
Zoho Marketing Automation--Zoho Marketing Automation	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Zoho Marketing Automation.This issue affects Zoho Marketing Automation: from n/a through 1.2.7.	2024-07-09	8.5	CVE-2024-37225
202ecommerce--paypal	In the module "PayPal Official" for PrestaShop 7+ releases prior to version 6.4.2 and for PrestaShop 1.6 releases prior to version 3.18.1, a malicious customer can confirm an order even if payment is finally declined by PayPal. A logical weakness during the capture of a payment in case of disabled webhooks can be exploited to create an accepted order. This could allow a threat actor to confirm an order with a fraudulent payment support. Versions 6.4.2 and 3.18.1 contain a patch for the issue. Additionally, users enable webhooks and check they are callable.	2024-07-26	7.5	CVE-2024-41670
ABB--Advant MOD 300 AdvaBuild	AdvaBuild uses a command queue to launch certain operations. An attacker who gains access to the command queue can use it to launch an attack by running any executable on the AdvaBuild node. The executables that can be run are not limited to AdvaBuild specific executables.Ã, Improper Privilege Management vulnerability in ABB Advant MOD 300 AdvaBuild.This issue affects Advant MOD 300 AdvaBuild: from 3.0 through 3.7 SP2.	2024-07-23	8.8	CVE-2020-11640
ABB--Advant MOD 300 AdvaBuild	An attacker could exploit the vulnerability by injecting garbage data or specially crafted data. Depending on the data injected each process might be affected differently. The process could crash or cause communication issues on the affected node, effectively causing a denial-of-service attack. The attacker could tamper with the data transmitted, causing the product to store wrong information or act on wrong data or display wrong information. This issue affects Advant MOD 300 AdvaBuild: from 3.0 through 3.7 SP2. For an attack to be successful, the attacker must have local access to a node in the system and be able to start a specially crafted application that disrupts the communication. An attacker who successfully exploited the vulnerability would be able to manipulate the data in such way as allowing reads and writes to the controllers or cause Windows processes in 800xA for MOD 300 and AdvaBuild to crash.	2024-07-23	7.8	CVE-2020-11639
Absolute Security--Secure Access	There is an elevation of privilege vulnerability in server and client components of Absolute Secure Access prior to version 13.07. Attackers with local access and valid desktop user credentials can elevate their privilege to system level by passing invalid address data to the vulnerable component. This could be used to manipulate process tokens to elevate the privilege of a normal process to System. The scope is changed, the impact to system confidentiality and integrity is high, the impact to the availability of the effected component is none.	2024-07-25	8.4	CVE-2024-40872
Acronis -- Acronis Cyber Infrastructure	Remote command execution due to use of default passwords. The following products are affected: Acronis Cyber Infrastructure (ACI) before build 5.0.1-61, Acronis Cyber Infrastructure (ACI) before build 5.1.1-71, Acronis Cyber Infrastructure (ACI) before build 5.2.1-69, Acronis Cyber Infrastructure (ACI) before build 5.3.1-53, Acronis Cyber Infrastructure (ACI) before build 5.4.4-132.	2024-07-24	9.8	CVE-2023-45249
Adrian Tobey--FormLift for Infusionsoft Web Forms	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Adrian Tobey FormLift for Infusionsoft Web Forms allows Blind SQL Injection.This issue affects FormLift for Infusionsoft Web Forms: from n/a through 7.5.17.	2024-07-22	9.3	CVE-2024-38773
Ankitects--Anki	An arbitrary script execution vulnerability exists in the MPV functionality of Ankitects Anki 24.04. A specially crafted flashcard can lead to a arbitrary code execution. An attacker can send malicious flashcard to trigger this vulnerability.	2024-07-22	9.6	CVE-2024-26020
Ankitects--Anki	An reflected XSS vulnerability exists in the handling of invalid paths in the Flask server in Ankitects Anki 24.04. A specially crafted flashcard can lead to JavaScript code execution and result in an arbitrary file read. An attacker can share a malicious flashcard to trigger this vulnerability.	2024-07-22	7.4	CVE-2024-32484
argoproj--argo-cd	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. This report details a security vulnerability in Argo CD, where an unauthenticated attacker can send a specially crafted large JSON payload to the /api/webhook endpoint, causing excessive memory allocation that leads to service disruption by triggering an Out Of Memory (OOM) kill. The issue poses a high risk to the availability of Argo CD deployments. This vulnerability is fixed in 2.11.6, 2.10.15, and 2.9.20.	2024-07-22	7.5	CVE-2024-40634

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Berqier Ltd--BerqWP	Server-Side Request Forgery (SSRF) vulnerability in Berqier Ltd BerqWP.This issue affects BerqWP: from n/a through 1.7.5.	2024-07-22	7.2	CVE-2024-37942
Bi Admin 2020--UiPress lite	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BÃ¡Â»Å¸i Admin 2020 UiPress lite allows SQL Injection.This issue affects UiPress lite: from n/a through 3.4.06.	2024-07-22	7.6	CVE-2024-38788
Canonical Ltd.--Ubuntu Desktop Provision	An issue was discovered in provd before version 0.1.5 with a setuid binary, which allows a local attacker to escalate their privilege.	2024-07-23	8.8	CVE-2024-6714
cBioPortal--cbioportal	The cBioPortal for Cancer Genomics provides visualization, analysis, and download of large-scale cancer genomics data sets. When running a publicly exposed proxy endpoint without authentication, cBioPortal could allow someone to perform a Server Side Request Forgery (SSRF) attack. Logged in users could do the same on private instances. A fix has been released in version 6.0.12. As a workaround, one might be able to disable `/proxy` endpoint entirely via, for example, nginx.	2024-07-23	8.3	CVE-2024-41668
ChurchCRM--CRM	ChurchCRM is an open-source church management system. Versions of the application prior to 5.9.2 are vulnerable to an authenticated SQL injection due to an improper sanitization of user input. Authentication is required, but no elevated privileges are necessary. This allows attackers to inject SQL statements directly into the database query due to inadequate sanitization of the EID parameter in in a GET request to `/GetText.php`. Version 5.9.2 patches the issue.	2024-07-26	8.8	CVE-2024-39304
ckp267--MaxiBlocks: 2200+ Patterns, 190 Pages, 14.2K Icons & 100 Styles	The MaxiBlocks: 2200+ Patterns, 190 Pages, 14.2K Icons & 100 Styles plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the maxi_remove_custom_image_size and maxi_add_custom_image_size functions in all versions up to, and including, 1.9.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	2024-07-23	8.1	CVE-2024-6885
danocmx--node-tf2-item-format	TF2 Item Format helps users format TF2 items to the community standards. Versions of `tf2-item-format` since at least `4.2.6` and prior to `5.9.14` are vulnerable to a Regular Expression Denial of Service (ReDoS) attack when parsing crafted user input. This vulnerability can be exploited by an attacker to perform DoS attacks on any service that uses any `tf2-item-format` to parse user input. Version `5.9.14` contains a fix for the issue.	2024-07-23	7.5	CVE-2024-41655
davidanderson--Redux Framework	The Redux Framework plugin for WordPress is vulnerable to unauthenticated JSON file uploads due to missing authorization and capability checks on the Redux_Color_Scheme_Import function in versions 4.4.12 to 4.4.17. This makes it possible for unauthenticated attackers to upload JSON files, which can be used to conduct stored cross-site scripting attacks and, in some rare cases, when the wp_filesystem fails to initialize - to Remote Code Execution.	2024-07-23	7.2	CVE-2024-6828
Designinvento--DirectoryPress	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Designinvento DirectoryPress allows SQL Injection.This issue affects DirectoryPress: from n/a through 3.6.10.	2024-07-22	8.5	CVE-2024-38755
dnsjava--dnsjava	dnsjava is an implementation of DNS in Java. Records in DNS replies are not checked for their relevance to the query, allowing an attacker to respond with RRs from different zones. This vulnerability is fixed in 3.6.0.	2024-07-22	8.9	CVE-2024-25638
duckdb--duckdb	DuckDB is a SQL database management system. In versions 1.0.0 and prior, content in filesystem is accessible for reading using `sniff_csv`, even with `enable_external_access=false`. This vulnerability provides an attacker with access to filesystem even when access is expected to be disabled and other similar functions do NOT provide access. There seem to be two vectors to this vulnerability. First, access to files that should otherwise not be allowed. Second, the content from a file can be read (e.g. `/etc/hosts`, `proc/self/environ`, etc) even though that doesn't seem to be the intent of the sniff_csv function. A fix for this issue is available in commit c9b7c98aa0e1cd7363fe8bb8543a95f38e980d8a and is expected to be part of version 1.1.0.	2024-07-24	7.5	CVE-2024-41672
F-logic--DataCube3	A vulnerability was found in F-logic DataCube3 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file	2024-07-24	7.3	CVE-2024-7066

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/admin/config_time_sync.php of the component HTTP POST Request Handler. The manipulation of the argument ntp_server leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272347.			
FishAudio--Bert-VITS2	Bert-VITS2 is the VITS2 Backbone with multilingual bert. User input supplied to the data_dir variable is used directly in a command executed with subprocess.run(cmd, shell=True) in the resample function, which leads to arbitrary command execution. This affects fishaudio/Bert-VITS2 2.3 and earlier.	2024-07-22	9.8	CVE-2024-39685
FishAudio--Bert-VITS2	Bert-VITS2 is the VITS2 Backbone with multilingual bert. User input supplied to the data_dir variable is used directly in a command executed with subprocess.run(cmd, shell=True) in the bert_gen function, which leads to arbitrary command execution. This affects fishaudio/Bert-VITS2 2.3 and earlier.	2024-07-22	9.8	CVE-2024-39686
ForIP Tecnologia--Administrao PABX	A vulnerability, which was classified as critical, has been found in ForIP Tecnologia AdministraÃƒÂ§ÃƒÂ£o PABX 1.x. This issue affects some unknown processing of the file /login of the component Authentication Form. The manipulation of the argument usuario leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272423. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-25	7.3	CVE-2024-7101
getsentry--sentry	Sentry is an error tracking and performance monitoring platform. Starting in version 10.0.0 and prior to version 24.7.1, an unsanitized payload sent by an Integration platform integration allows storing arbitrary HTML tags on the Sentry side with the subsequent rendering them on the Issues page. Self-hosted Sentry users may be impacted in case of untrustworthy Integration platform integrations sending external issues from their side to Sentry. A patch has been released in Sentry 24.7.1. For Sentry SaaS customers, no action is needed. This has been patched on July 23, and even prior to the fix, the exploitation was not possible due to the strict Content Security Policy deployed on sentry.io site. For self-hosted users, the maintainers of Sentry strongly recommend upgrading Sentry to the latest version. If it is not possible, one could enable CSP on one's self-hosted installation with `CSP_REPORT_ONLY = False` (enforcing mode). This will mitigate the risk of cross-site scripting.	2024-07-23	7.1	CVE-2024-41656
GitLab--GitLab	A cross site scripting vulnerability exists in GitLab CE/EE affecting all versions from 16.6 prior to 17.0.5, 17.1 prior to 17.1.3, 17.2 prior to 17.2.1 allowing an attacker to execute arbitrary scripts under the context of the current logged in user.	2024-07-25	7.7	CVE-2024-7047
HashiCorp--Nomad	HashiCorp Nomad and Nomad Enterprise 1.6.12 up to 1.7.9, and 1.8.1 archive unpacking during migration is vulnerable to path escaping of the allocation directory. This vulnerability, CVE-2024-6717, is fixed in Nomad 1.6.13, 1.7.10, and 1.8.2.	2024-07-23	7.7	CVE-2024-6717 security@hashicorp.com
Hewlett Packard Enterprise (HPE)--HPE Aruba Networking EdgeConnect SD-WAN	A vulnerability in the web-based management interface of HPE Aruba Networking EdgeConnect SD-WAN gateway could allow an authenticated remote attacker to conduct a server-side prototype pollution attack. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise.	2024-07-24	7.2	CVE-2024-33519
Hewlett Packard Enterprise (HPE)--HPE Aruba Networking EdgeConnect SD-WAN	A vulnerability exists in the HPE Aruba Networking EdgeConnect SD-WAN gateway's Command Line Interface that allows remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of this vulnerability will result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise	2024-07-24	7.2	CVE-2024-41133
Hewlett Packard Enterprise (HPE)--HPE Aruba Networking EdgeConnect SD-WAN	A vulnerability exists in the HPE Aruba Networking EdgeConnect SD-WAN gateway's Command Line Interface that allows remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of this vulnerability will result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise	2024-07-24	7.2	CVE-2024-41134
Hewlett Packard Enterprise (HPE)--HPE Aruba	A vulnerability exists in the HPE Aruba Networking EdgeConnect SD-WAN gateway's Command Line Interface that allows remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of this	2024-07-24	7.2	CVE-2024-41135

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Networking EdgeConnect SD-WAN	vulnerability will result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise			
Hewlett Packard Enterprise -- HPE Aruba Networking EdgeConnect SD-WAN Orchestrator	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	2024-07-24	9	CVE-2024-41914
Hewlett Packard Enterprise -- HPE Aruba Networking EdgeConnect SD-WAN Orchestrator	A vulnerability in the web-based management interface of EdgeConnect SD-WAN Orchestrator could allow an authenticated remote attacker to conduct a server-side prototype pollution attack. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary commands on the underlying operating system leading to complete system compromise.	2024-07-24	8.8	CVE-2024-22443
Hewlett Packard Enterprise -- HPE Aruba Networking EdgeConnect SD-WAN Orchestrator	An authenticated command injection vulnerability exists in the HPE Aruba Networking EdgeConnect SD-WAN gateways Command Line Interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	2024-07-24	8.8	CVE-2024-41136
Huawei -- HarmonyOS	Memory request logic vulnerability in the memory module. Impact: Successful exploitation of this vulnerability will affect integrity and availability.	2024-07-25	7.1	CVE-2024-39672 psirt@huawei.com
Huawei -- HarmonyOS	Vulnerability of serialisation/deserialisation mismatch in the iAware module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-07-25	7.1	CVE-2024-39673 psirt@huawei.com
ISC--BIND 9	A malicious client can send many DNS messages over TCP, potentially causing the server to become unstable while the attack is in progress. The server may recover after the attack ceases. Use of ACLs will not mitigate the attack. This issue affects BIND 9 versions 9.18.1 through 9.18.27, 9.19.0 through 9.19.24, and 9.18.11-S1 through 9.18.27-S1.	2024-07-23	7.5	CVE-2024-0760
ISC--BIND 9	Resolver caches and authoritative zone databases that hold significant numbers of RRs for the same hostname (of any RTYPE) can suffer from degraded performance as content is being added or updated, and also when handling client queries for this name. This issue affects BIND 9 versions 9.11.0 through 9.11.37, 9.16.0 through 9.16.50, 9.18.0 through 9.18.27, 9.19.0 through 9.19.24, 9.11.4-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.50-S1, and 9.18.11-S1 through 9.18.27-S1.	2024-07-23	7.5	CVE-2024-1737
ISC--BIND 9	If a server hosts a zone containing a "KEY" Resource Record, or a resolver DNSSEC-validates a "KEY" Resource Record from a DNSSEC-signed domain in cache, a client can exhaust resolver CPU resources by sending a stream of SIG(0) signed requests. This issue affects BIND 9 versions 9.0.0 through 9.11.37, 9.16.0 through 9.16.50, 9.18.0 through 9.18.27, 9.19.0 through 9.19.24, 9.9.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.49-S1, and 9.18.11-S1 through 9.18.27-S1.	2024-07-23	7.5	CVE-2024-1975
ISC--BIND 9	Client queries that trigger serving stale data and that also require lookups in local authoritative zone data may result in an assertion failure. This issue affects BIND 9 versions 9.16.13 through 9.16.50, 9.18.0 through 9.18.27, 9.19.0 through 9.19.24, 9.11.33-S1 through 9.11.37-S1, 9.16.13-S1 through 9.16.50-S1, and 9.18.11-S1 through 9.18.27-S1.	2024-07-23	7.5	CVE-2024-4076
itsourcecode -- Online Blood Bank Management System	A vulnerability was found in itsourcecode Online Blood Bank Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file login.php of the component Login. The manipulation of the argument user/pass leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272120.	2024-07-22	9.8	CVE-2024-6966
itsourcecode -- Online Blood Bank Management System	A vulnerability classified as critical has been found in itsourcecode Tailoring Management System 1.0. Affected is an unknown function of the file /staffcatadd.php. The manipulation of the argument title leads to sql injection. It is	2024-07-22	9.8	CVE-2024-6970

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272124.			
itsourcecode -- Online Blood Bank Management System	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file expcatadd.php. The manipulation of the argument title leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-272366 is the identifier assigned to this vulnerability.	2024-07-24	9.8	CVE-2024-7081
JetBrains--TeamCity	In JetBrains TeamCity before 2024.07 access tokens could continue working after deletion or expiration	2024-07-22	7.4	CVE-2024-41827
kirilkirkov -- Ecommerce-Laravel-Bootstrap	A vulnerability was found in kirilkirkov Ecommerce-Laravel-Bootstrap up to 1f1097a3448ce8ec53e034ea0f70b8e2a0e64a87. It has been rated as critical. Affected by this issue is the function getCartProductsIds of the file app/Cart.php. The manipulation of the argument laraCart leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The name of the patch is a02111a674ab49f65018b31da3011b1e396f59b1. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-272348.	2024-07-24	8.8	CVE-2024-7067
Lenovo--XClarity Controller	A privilege escalation vulnerability was discovered in the web interface or SSH captive command shell interface of XCC that could allow an authenticated XCC user with elevated privileges to perform command injection via a specially crafted request.	2024-07-26	7.2	CVE-2024-38508
Lenovo--XClarity Controller	A privilege escalation vulnerability was discovered in XCC that could allow an authenticated XCC user with elevated privileges to execute arbitrary code via a specially crafted IPMI command.	2024-07-26	7.2	CVE-2024-38509
Lenovo--XClarity Controller	A privilege escalation vulnerability was discovered in the SSH captive command shell interface that could allow an authenticated XCC user with elevated privileges to perform command injection via specially crafted file uploads.	2024-07-26	7.2	CVE-2024-38510
Lenovo--XClarity Controller	A privilege escalation vulnerability was discovered in an upload processing functionality of XCC that could allow an authenticated XCC user with elevated privileges to perform command injection via specially crafted file uploads.	2024-07-26	7.2	CVE-2024-38511
Lenovo--XClarity Controller	A privilege escalation vulnerability was discovered in XCC that could allow an authenticated XCC user with elevated privileges to perform command injection via specially crafted IPMI commands.	2024-07-26	7.2	CVE-2024-38512
ManageEngine--Exchange Reporter Plus	Zohocorp ManageEngine Exchange Reporter Plus versions 5717 and below are vulnerable to the authenticated SQL injection in the reports module.	2024-07-26	8.3	CVE-2024-38871
ManageEngine--Exchange Reporter Plus	Zohocorp ManageEngine Exchange Reporter Plus versions 5717 and below are vulnerable to the authenticated SQL injection in the monitoring module.	2024-07-26	8.3	CVE-2024-38872
Microsoft--GroupMe	An improper access control vulnerability in GroupMe allows an a unauthenticated attacker to elevate privileges over a network by convincing a user to click on a malicious link.	2024-07-23	9.6	CVE-2024-38164
Microsoft--GroupMe	An improper restriction of excessive authentication attempts in GroupMe allows a unauthenticated attacker to elevate privileges over a network.	2024-07-23	8.1	CVE-2024-38176
mnetadmanager--Media.net Ads Manager	The Media.net Ads Manager plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation and missing capability check in the 'sendMail' function in all versions up to, and including, 2.10.13. This makes it possible for authenticated attackers, with subscriber-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible. The vulnerability is only exploitable if anyone has ever logged in through the API.	2024-07-27	8.8	CVE-2024-6431
moby--moby	Moby is an open-source project created by Docker for software containerization. A security vulnerability has been detected in certain versions of Docker Engine, which could allow an attacker to bypass authorization plugins (AuthZ) under specific circumstances. The base likelihood of this being exploited is low. Using a specially-crafted API request, an Engine API client could make the daemon forward the request or response to an authorization plugin without the body. In certain circumstances, the authorization plugin may allow a request which it would have	2024-07-24	9.9	CVE-2024-41110

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	otherwise denied if the body had been forwarded to it. A security issue was discovered In 2018, where an attacker could bypass AuthZ plugins using a specially crafted API request. This could lead to unauthorized actions, including privilege escalation. Although this issue was fixed in Docker Engine v18.09.1 in January 2019, the fix was not carried forward to later major versions, resulting in a regression. Anyone who depends on authorization plugins that introspect the request and/or response body to make access control decisions is potentially impacted. Docker EE v19.03.x and all versions of Mirantis Container Runtime are not vulnerable. docker-ce v27.1.1 containes patches to fix the vulnerability. Patches have also been merged into the master, 19.0, 20.0, 23.0, 24.0, 25.0, 26.0, and 26.1 release branches. If one is unable to upgrade immediately, avoid using AuthZ plugins and/or restrict access to the Docker API to trusted parties, following the principle of least privilege.			
N/A - - MasterStudy LMS WordPress Plugin	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.3.24 does not prevent students from creating instructor accounts, which could be used to get access to functionalities they shouldn't have.	2024-07-22	8.8	CVE-2024-5973
N/A - - MasterStudy LMS WordPress Plugin	The PZ Frontend Manager WordPress plugin before 1.0.6 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	2024-07-22	8.8	CVE-2024-6244
N/A -- N/A	ProtonVPN before 3.2.10 on Windows mishandles the drive installer path, which should use this: '"' + ExpandConstant('{autopf}\Proton\Drive') + '"' in Setup/setup.iss.	2024-07-22	9.8	CVE-2024-37391
N/A -- N/A	The snapshot_path parameter in the /api/get-browser-snapshot endpoint in stitionai devika v1 is susceptible to a path traversal attack. An attacker can manipulate the snapshot_path parameter to traverse directories and access sensitive files on the server. This can potentially lead to unauthorized access to critical system files and compromise the confidentiality and integrity of the system.	2024-07-24	9.1	CVE-2024-40422
N/A -- N/A	TOTOLINK A6000R V1.0.1-B20201211.2000 was discovered to contain a command injection vulnerability via the cmd parameter in the webcmd function.	2024-07-23	9.8	CVE-2024-41319
N/A -- N/A	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the PPPOEPassword parameter at ip/goform/QuickIndex.	2024-07-24	9.8	CVE-2024-41459
N/A -- N/A	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the entrys parameter at ip/goform/RouteStatic.	2024-07-24	9.8	CVE-2024-41460
N/A -- N/A	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the list1 parameter at ip/goform/DhcpListClient.	2024-07-24	9.8	CVE-2024-41461
N/A -- N/A	CampCodes Supplier Management System v1.0 is vulnerable to SQL injection via Supply_Management_System/admin/view_order_items.php?id= .	2024-07-24	9.8	CVE-2024-41551
N/A -- N/A	LibreChat through 0.7.4-rc1 has incorrect access control for message updates. (Work on a fixed version release has started in PR 3363.)	2024-07-22	9.8	CVE-2024-41703
N/A -- N/A	LibreChat through 0.7.4-rc1 does not validate the normalized pathnames of images. (Work on a fixed version release has started in PR 3363.)	2024-07-22	9.8	CVE-2024-41704
N/A -- N/A	AdTran SRG 834-5 HDC17600021F1 devices (with SmartOS 11.1.1.1 and fixed in Version 12.1.3.1) have SSH enabled by default, accessible both over the LAN and the Internet. During a window of time when the device is being set up, it uses a default username and password combination of admin/admin with root-level privileges. An attacker can exploit this window to gain unauthorized root access by either modifying the existing admin account or creating a new account with equivalent privileges. This vulnerability allows attackers to execute arbitrary commands.	2024-07-24	8.8	CVE-2024-31970

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
N/A -- N/A	Adtran 834-5 11.1.0.101-202106231430, and fixed as of SmartOS Version 12.5.5.1, devices allow OS Command Injection via shell metacharacters to the Ping or Traceroute utility.	2024-07-24	8.8	CVE-2024-31977
N/A -- N/A	Insecure permissions in logging-operator v4.6.0 allows attackers to access sensitive data and escalate privileges by obtaining the service account's token.	2024-07-24	8.8	CVE-2024-36541
N/A -- N/A	AdTran 834-5 HDC17600021F1 (SmartOS 11.1.1.1) devices enable the SSH service by default and have a hidden, undocumented, hard-coded support account whose password is based on the devices MAC address. All of the devices internet interfaces share a similar MAC address that only varies in their final octet. This allows network-adjacent attackers to derive the support user's SSH password by decrementing the final octet of the connected gateway address or via the BSSID. An attacker can then execute arbitrary OS commands with root-level privileges.	2024-07-24	7.2	CVE-2024-39345
N/A -- N/A	go-chart v2.1.1 was discovered to contain an infinite loop via the drawCanvas() function.	2024-07-23	7.5	CVE-2024-40060
N/A -- N/A	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the page parameter at ip/goform/DhcpListClient.	2024-07-24	7.5	CVE-2024-41462
N/A -- N/A	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the entrys parameter at ip/goform/addressNat.	2024-07-24	7.5	CVE-2024-41463
N/A -- N/A	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the mitInterface parameter in ip/goform/RouteStatic	2024-07-24	7.5	CVE-2024-41464
N/A -- N/A	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the funcpara1 parameter at ip/goform/setcfm.	2024-07-24	7.5	CVE-2024-41465
N/A -- N/A	Tenda FH1201 v1.2.0.14 was discovered to contain a stack-based buffer overflow vulnerability via the page parameter at ip/goform/NatStaticSetting.	2024-07-24	7.5	CVE-2024-41466
N/A -- N/A	A stored XSS issue was discovered in Archer Platform 6.8 before 2024.06. A remote authenticated malicious Archer user could potentially exploit this to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application. 6.14.P4 (6.14.0.4) and 6.13 P4 (6.13.0.4) are also fixed releases. This vulnerability is similar to, but not identical to, CVE-2023-30639.	2024-07-25	7.1	CVE-2024-41705
N/A -- N/A	A stored XSS issue was discovered in Archer Platform 6 before version 2024.06. A remote authenticated malicious Archer user could potentially exploit this to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application. 6.14 P4 (6.14.0.4) is also a fixed release.	2024-07-25	7.3	CVE-2024-41706
n/a--SuperAGI	All versions of `SuperAGI` are vulnerable to Arbitrary Code Execution due to unsafe use of the 'eval' function. An attacker could induce the LLM output to exploit this vulnerability and gain arbitrary code execution on the SuperAGI application server.	2024-07-22	9.8	CVE-2024-21552
NI--IO Trace Tool	A stack-based buffer overflow vulnerability due to a missing bounds check in the NI I/O Trace Tool may result in arbitrary code execution. Successful exploitation requires an attacker to provide a user with a specially crafted nitrace file. The NI I/O Trace tool is installed as part of the NI System Configuration utilities included with many NI software products.? Refer to the NI Security Advisory for identifying the version of NI IO Trace.exe installed. The NI I/O Trace tool was also previously released as NI Spy.	2024-07-23	7.8	CVE-2024-5602 security@ni.com
NI--LabVIEW	An out of bounds read due to a missing bounds check in LabVIEW may disclose information or result in arbitrary code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	2024-07-23	7.8	CVE-2024-4079 security@ni.com
NI--LabVIEW	A memory corruption issue due to an improper length check in LabVIEW tdcore.dll may disclose information or result in arbitrary code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects LabVIEW 2024 Q1 and prior versions.	2024-07-23	7.8	CVE-2024-4080 security@ni.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
NI--LabVIEW	A memory corruption issue due to an improper length check in NI LabVIEW may disclose information or result in arbitrary code execution. Successful exploitation requires an attacker to provide a user with a specially crafted VI. This vulnerability affects NI LabVIEW 2024 Q1 and prior versions.	2024-07-23	7.8	CVE-2024-4081 security@ni.com
NI--SystemLink Server	An out-of-date version of Redis shipped with NI SystemLink Server is susceptible to multiple vulnerabilities, including CVE-2022-24834. This affects NI SystemLink Server 2024 Q1 and prior versions. It also affects NI FlexLogger 2023 Q2 and prior versions which installed this shared service.	2024-07-22	7.8	CVE-2024-6121 security@ni.com
NI--VeriStand	AÃ, deserialization of untrusted dataÃ, vulnerabilityÃ, exists in NI VeriStand DataLogging Server that may result in remote code execution. Successful exploitation requires an attacker to send a specially crafted message. These vulnerabilities affect NI VeriStand 2024 Q2 and prior versions.	2024-07-22	9.8	CVE-2024-6793 security@ni.com
NI--VeriStand	A deserialization of untrusted data vulnerability exists in NI VeriStand Waveform Streaming Server that may result in remote code execution. Successful exploitation requires an attacker to send a specially crafted message. These vulnerabilities affect NI VeriStand 2024 Q2 and prior versions.	2024-07-22	9.8	CVE-2024-6794 security@ni.com
NI--VeriStand	The NI VeriStand Gateway is missing authorization checks when an actor attempts to access Project resources. These missing checks may result in remote code execution. This affects NI VeriStand 2024 Q2 and prior versions.	2024-07-22	9.8	CVE-2024-6806 security@ni.com
NI--VeriStand	A deserialization of untrusted data vulnerability exists in NI VeriStand that may result in remote code execution. Successful exploitation requires an attacker to get a user to open a specially crafted project file. This vulnerability affects VeriStand 2024 Q2 and prior versions.	2024-07-22	7.8	CVE-2024-6675 security@ni.com
NI--VeriStand	A directory path traversal vulnerability exists when loading a vsmodel file in NI VeriStand that may result in remote code execution. Successful exploitation requires an attacker to get a user to open a specially crafted .vsmodel file. This vulnerability affects VeriStand 2024 Q2 and prior versions.	2024-07-22	7.8	CVE-2024-6791 security@ni.com
NI--VeriStand	The NI VeriStand Gateway is missing authorization checks when an actor attempts to access File Transfer resources. These missing checks may result in information disclosure or remote code execution. This affects NI VeriStand 2024 Q2 and prior versions.	2024-07-22	7.5	CVE-2024-6805 security@ni.com
Nimble Commander--Nimble Commander	Nimble Commander suffers from a privilege escalation vulnerability due to the server (info.filesmanager.Files.PrivilegedIOHelperV2) performing improper/insufficient validation of a client's authorization before executing an operation. Consequently, it is possible to execute system-level commands as the root user, such as changing permissions and ownership, obtaining a handle (file descriptor) of an arbitrary file, and terminating processes, among other operations.	2024-07-26	8.8	CVE-2024-7062 41c37e40-543d-43a2-b660-2fee83ea851a
Okta--Okta Browser Plugin	Okta Browser Plugin versions 6.5.0 through 6.31.0 (Chrome/Edge/Firefox/Safari) are vulnerable to cross-site scripting. This issue occurs when the plugin prompts the user to save these credentials within Okta Personal. A fix was implemented to properly escape these fields, addressing the vulnerability. Importantly, if Okta Personal is not added to the plugin to enable multi-account view, the Workforce Identity Cloud plugin is not affected by this issue. The vulnerability is fixed in Okta Browser Plugin version 6.32.0 for Chrome/Edge/Safari/Firefox.	2024-07-23	7.1	CVE-2024-0981 psirt@okta.com
opengeos--streamlit-geospatial	streamlit-geospatial is a streamlit multipage app for geospatial applications. Prior to commit c4f81d9616d40c60584e36abb15300853a66e489, the palette variable in `pages/1_Ã°Å¸â€œÂ·_Timelapse.py` takes user input, which is later used in the `eval()` function on line 380, leading to remote code execution. Commit c4f81d9616d40c60584e36abb15300853a66e489 fixes this issue.	2024-07-26	9.8	CVE-2024-41112
opengeos--streamlit-geospatial	streamlit-geospatial is a streamlit multipage app for geospatial applications. Prior to commit c4f81d9616d40c60584e36abb15300853a66e489, the `vis_params` variable on line 383 or line 390 in `pages/1_Ã°Å¸â€œÂ·_Timelapse.py` takes user input, which is later used in the `eval()` function on line 395, leading to remote code execution. Commit c4f81d9616d40c60584e36abb15300853a66e489 fixes this issue.	2024-07-26	9.8	CVE-2024-41113
opengeos--streamlit-geospatial	streamlit-geospatial is a streamlit multipage app for geospatial applications. Prior to commit c4f81d9616d40c60584e36abb15300853a66e489, the `palette` variable on line 430 in `pages/1_Ã°Å¸â€œÂ·_Timelapse.py` takes user input, which is later used in the `eval()` function on line 435, leading to remote code execution. Commit c4f81d9616d40c60584e36abb15300853a66e489 fixes this issue.	2024-07-26	9.8	CVE-2024-41114
opengeos--streamlit-	streamlit-geospatial is a streamlit multipage app for geospatial applications. Prior to commit c4f81d9616d40c60584e36abb15300853a66e489, the `palette` variable	2024-07-26	9.8	CVE-2024-41115

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
geospatial	on line 488 in `pages/1_Ã°Å¸â€œÂ·_Timelapse.py` takes user input, which is later used in the `eval()` function on line 493, leading to remote code execution. Commit c4f81d9616d40c60584e36abb15300853a66e489 fixes this issue.			
opengeos--streamlit-geospatial	streamlit-geospatial is a streamlit multipage app for geospatial applications. Prior to commit c4f81d9616d40c60584e36abb15300853a66e489, the `vis_params` variable on line 1254 in `pages/1_Ã°Å¸â€œÂ·_Timelapse.py` takes user input, which is later used in the `eval()` function on line 1345, leading to remote code execution. Commit c4f81d9616d40c60584e36abb15300853a66e489 fixes this issue.	2024-07-26	9.8	CVE-2024-41116
opengeos--streamlit-geospatial	streamlit-geospatial is a streamlit multipage app for geospatial applications. Prior to commit c4f81d9616d40c60584e36abb15300853a66e489, the `vis_params` variable on line 115 in `pages/10_Ã°Å¸Å’Â_Earth_Engine_Datasets.py` takes user input, which is later used in the `eval()` function on line 126, leading to remote code execution. Commit c4f81d9616d40c60584e36abb15300853a66e489 fixes this issue.	2024-07-26	9.8	CVE-2024-41117
opengeos--streamlit-geospatial	streamlit-geospatial is a streamlit multipage app for geospatial applications. Prior to commit c4f81d9616d40c60584e36abb15300853a66e489, the `vis_params` variable on line 80 in `8_Ã°Å¸Â Å“Ã¯Â¸Â_Raster_Data_Visualization.py` takes user input, which is later used in the `eval()` function on line 86, leading to remote code execution. Commit c4f81d9616d40c60584e36abb15300853a66e489 fixes this issue.	2024-07-26	9.8	CVE-2024-41119
opengeos--streamlit-geospatial	streamlit-geospatial is a streamlit multipage app for geospatial applications. Prior to commit c4f81d9616d40c60584e36abb15300853a66e489, the `url` variable on line 63 of `pages/9_Ã°Å¸â€Â²_Vector_Data_Visualization.py` takes user input, which is later passed to the `gpd.read_file` method. `gpd.read_file` method creates a request to arbitrary destinations, leading to blind server-side request forgery. Commit c4f81d9616d40c60584e36abb15300853a66e489 fixes this issue.	2024-07-26	9.8	CVE-2024-41120
opengeos--streamlit-geospatial	streamlit-geospatial is a streamlit multipage app for geospatial applications. Prior to commit c4f81d9616d40c60584e36abb15300853a66e489, the `url` variable on line 47 of `pages/7_Ã°Å¸â€œÂ¦_Web_Map_Service.py` takes user input, which is passed to `get_layers` function, in which `url` is used with `get_wms_layer` method. `get_wms_layer` method creates a request to arbitrary destinations, leading to blind server-side request forgery. Commit c4f81d9616d40c60584e36abb15300853a66e489 fixes this issue.	2024-07-26	7.5	CVE-2024-41118
OpenIdentityPlatform--OpenAM	OpenAM is an open access management solution. In versions 15.0.3 and prior, the `getCustomLoginUrlTemplate` method in RealmOAuth2ProviderSettings.java is vulnerable to template injection due to its usage of user input. Although the developer intended to implement a custom URL for handling login to override the default PingOne Advanced Identity Cloud login page,they did not restrict the `CustomLoginUrlTemplate`, allowing it to be set freely. Commit fcb8432aa77d5b2e147624fe954cb150c568e0b8 introduces `TemplateClassResolver.SAFER_RESOLVER` to disable the resolution of commonly exploited classes in FreeMarker template injection. As of time of publication, this fix is expected to be part of version 15.0.4.	2024-07-24	8.8	CVE-2024-41667
openobserve--openobserve	The OpenObserve open-source observability platform provides the ability to filter logs in a dashboard by the values uploaded in a given log. However, all versions of the platform through 0.9.1 do not sanitize user input in the filter selection menu, which may result in complete account takeover. It has been noted that the front-end uses `DOMPurify` or Vue templating to escape cross-site scripting (XSS) extensively, however certain areas of the front end lack this XSS protection. When combining the missing protection with the insecure authentication handling that the front-end uses, a malicious user may be able to take over any victim's account provided they meet the exploitation steps. As of time of publication, no patched version is available.	2024-07-25	8.8	CVE-2024-41808
openobserve--openobserve	OpenObserve is an open-source observability platform. Starting in version 0.4.4 and prior to version 0.10.0, OpenObserve contains a cross-site scripting vulnerability in line 32 of `openobserve/web/src/views/MemberSubscription.vue`. Version 0.10.0 sanitizes incoming html.	2024-07-25	7.2	CVE-2024-41809
Progress Software Corporation - - Telerik Reporting	In ProgressÃ‚Â® TelerikÃ‚Â® Reporting versions prior to 18.1.24.709, a code execution attack is possible through object injection via an insecure type resolution vulnerability.	2024-07-24	9.8	CVE-2024-6096 security@progress.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Progress Software Corporation - - Telerik Reporting	In ProgressÃ‚Â® TelerikÃ‚Â® Report Server versions prior to 2024 Q2 (10.1.24.709), a remote code execution attack is possible through an insecure deserialization vulnerability.	2024-07-24	9.8	CVE-2024-6327 security@progress.com security@progress.com
Seraphinite Solutions--Seraphinite Post .DOCX Source	Server-Side Request Forgery (SSRF) vulnerability in Seraphinite Solutions Seraphinite Post .DOCX Source.This issue affects Seraphinite Post .DOCX Source: from n/a through 2.16.9.	2024-07-22	7.2	CVE-2024-38728
Siemens--CPCI85 Central Processing/Communication	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V5.40), SICORE Base system (All versions < V1.4.0). The password of administrative accounts of the affected applications can be reset without requiring the knowledge of the current password, given the auto login is enabled. This could allow an unauthorized attacker to obtain administrative access of the affected applications.	2024-07-22	9.8	CVE-2024-37998
SixLabors--ImageSharp	ImageSharp is a 2D graphics API. An Out-of-bounds Write vulnerability has been found in the ImageSharp gif decoder, allowing attackers to cause a crash using a specially crafted gif. This can potentially lead to denial of service. All users are advised to upgrade to v3.1.5 or v2.1.9.	2024-07-22	7.5	CVE-2024-41131
Softaculous--Webuzo	Softaculous Webuzo contains an authentication bypass vulnerability through the password reset functionality. Remote, anonymous attackers can exploit this vulnerability to gain full server access as the root user.	2024-07-25	9.8	CVE-2024-24621
Softaculous--Webuzo	Softaculous Webuzo contains a command injection in the password reset functionality. A remote, authenticated attacker can exploit this vulnerability to gain code execution on the system.	2024-07-25	8.8	CVE-2024-24622
Softaculous--Webuzo	Softaculous Webuzo contains a command injection vulnerability in the FTP management functionality. A remote, authenticated attacker can exploit this vulnerability to gain code execution on the system.	2024-07-25	8.8	CVE-2024-24623
SourceCodester -- Clinics Patient Management System	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /print_patients_visits.php. The manipulation of the argument from/to leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-272122 is the identifier assigned to this vulnerability.	2024-07-22	7.5	CVE-2024-6968
SourceCodester -- 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/get_patient_history.php. The manipulation of the argument patient_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272123.	2024-07-22	7.5	CVE-2024-6969
SourceCodester - - Employee and Visitor Gate Pass Logging System	A vulnerability was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. It has been classified as critical. This affects an unknown part of the file /employee_gatepass/admin/?page=employee/manage_employee. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272121 was assigned to this vulnerability.	2024-07-22	7.5	CVE-2024-6967
SourceCodester - - Employee and Visitor Gate Pass Logging System	A vulnerability, which was classified as critical, has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. This issue affects some unknown processing of the file /employee_gatepass/classes/Master.php?f=delete_department. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272351.	2024-07-24	7.5	CVE-2024-7069
SourceCodester - - Insurance Management System	A vulnerability was found in SourceCodester Insurance Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /E-Insurance/. The manipulation leads to direct request. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272365 was assigned to this vulnerability.	2024-07-24	7.5	CVE-2024-7080

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spiffy Plugins--Spiffy Calendar	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Spiffy Plugins Spiffy Calendar allows SQL Injection.This issue affects Spiffy Calendar: from n/a through 4.9.11.	2024-07-22	7.6	CVE-2024-38692
Spring--Spring Cloud Data Flow	In Spring Cloud Data Flow versions prior to 2.11.4,Ã, Ã, a malicious user who has access to the Skipper server api can use a crafted upload request to write an arbitrary file to any location on the file system which could lead to compromising the server	2024-07-25	9.8	CVE-2024-37084
starship--starship	Starship is a cross-shell prompt. Starting in version 1.0.0 and prior to version 1.20.0, undocumented and unpredictable shell expansion and/or quoting rules make it easily to accidentally cause shell injection when using custom commands with starship in bash. This issue only affects users with custom commands, so the scope is limited, and without knowledge of others' commands, it could be hard to successfully target someone. Version 1.20.0 fixes the vulnerability.	2024-07-26	7.4	CVE-2024-41815
tenda --O3	A vulnerability classified as critical was found in Tenda O3 1.0.0.10. This vulnerability affects the function formQosSet. The manipulation of the argument remark/ipRange/upSpeed/downSpeed/enable leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272116. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-22	8.8	CVE-2024-6962
tenda --O3	A vulnerability, which was classified as critical, has been found in Tenda O3 1.0.0.10. This issue affects the function formexeCommand. The manipulation of the argument cmdinput leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272117 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-22	8.8	CVE-2024-6963
tenda --O3	A vulnerability, which was classified as critical, was found in Tenda O3 1.0.0.10. Affected is the function fromDhcpSetSer. The manipulation of the argument dhcpEn/startIP/endIP/preDNS/altDNS/mask/gateway leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-272118 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-22	8.8	CVE-2024-6964
tenda --O3	A vulnerability has been found in Tenda O3 1.0.0.10 and classified as critical. Affected by this vulnerability is the function fromVirtualSet. The manipulation of the argument ip/localPort/publicPort/app leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272119. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-22	8.8	CVE-2024-6965
Tenda--O3	A vulnerability was found in Tenda O3 1.0.0.10(2478). It has been declared as critical. This vulnerability affects the function fromMacFilterSet of the file /goform/setMacFilter. The manipulation of the argument remark leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-272554 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-27	8.8	CVE-2024-7151
Tenda--O3	A vulnerability was found in Tenda O3 1.0.0.10(2478). It has been rated as critical. This issue affects the function fromSafeSetMacFilter of the file /goform/setMacFilterList. The manipulation of the argument 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. The associated identifier of this vulnerability is VDB-272555. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-27	8.8	CVE-2024-7152
thimpress--LearnPress WordPress LMS Plugin	The LearnPress - WordPress LMS Plugin plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 4.2.6.8.2 via the 'render_content_block_template' function. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.	2024-07-25	8.8	CVE-2024-6589

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
TxtDot--txtdot	txtdot is an HTTP proxy that parses only text, links, and pictures from pages, removing ads and heavy scripts. Prior to version 1.7.0, a Server-Side Request Forgery (SSRF) vulnerability in the `/get` route of txtdot allows remote attackers to use the server as a proxy to send HTTP GET requests to arbitrary targets and retrieve information in the internal network. Version 1.7.0 prevents displaying the response of forged requests, but the requests can still be sent. For complete mitigation, a firewall between txtdot and other internal network resources should be set.	2024-07-26	7.5	CVE-2024-41812
TxtDot--txtdot	txtdot is an HTTP proxy that parses only text, links, and pictures from pages, removing ads and heavy scripts. Starting in version 1.4.0 and prior to version 1.6.1, a Server-Side Request Forgery (SSRF) vulnerability in the `/proxy` route of txtdot allows remote attackers to use the server as a proxy to send HTTP GET requests to arbitrary targets and retrieve information in the internal network. Version 1.6.1 patches the issue.	2024-07-26	7.5	CVE-2024-41813
UkrSolution--Barcode Scanner with Inventory & Order Manager	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in UkrSolution Barcode Scanner with Inventory & Order Manager allows SQL Injection.This issue affects Barcode Scanner with Inventory & Order Manager: from n/a through 1.6.1.	2024-07-22	8.5	CVE-2024-38708
Uncanny Owl--Uncanny Toolkit Pro for LearnDash	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Uncanny Owl Uncanny Toolkit Pro for LearnDash allows Reflected XSS.This issue affects Uncanny Toolkit Pro for LearnDash: from n/a before 4.1.4.1.	2024-07-22	7.1	CVE-2024-37436
vnotex--vnote	VNote is a note-taking platform. A Cross-Site Scripting (XSS) vulnerability has been identified in the Markdown rendering functionality of versions 3.18.1 and prior of the VNote note-taking application. This vulnerability allows the injection and execution of arbitrary JavaScript code through which remote code execution can be achieved. A patch for this issue is available at commit f1af78573a0ef51d6ef6a0bc4080cddc8f30a545. Other mitigation strategies include implementing rigorous input sanitization for all Markdown content and utilizing a secure Markdown parser that appropriately escapes or strips potentially dangerous content.	2024-07-24	8.6	CVE-2024-41662
wptexture--Flipbox Builder	The Flipbox Builder plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.5 via deserialization of untrusted input in the flipbox_builder_Flipbox_ShortCode function. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2024-07-27	8.8	CVE-2024-6152
WPWeb--Social Auto Poster	The Social Auto Poster plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'wpw_auto_poster_get_image_path' function in all versions up to, and including, 5.3.14. This makes it possible for authenticated attackers, with Contributor-level and above permissions, to upload arbitrary files on the affected site's server which may make remote code execution possible. An attacker can use CVE-2024-6754 to exploit with subscriber-level access.	2024-07-24	8.8	CVE-2024-6756
WPWeb--Social Auto Poster	The Social Auto Poster plugin for WordPress is vulnerable to unauthorized access, modification, and loss of data due to a missing capability check on multiple functions in all versions up to, and including, 5.3.14. This makes it possible for unauthenticated attackers to add, modify, or delete post meta and plugin options.	2024-07-24	7.3	CVE-2024-6750
WPWeb--Social Auto Poster	The Social Auto Poster plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mapTypes' parameter in the 'wpw_auto_poster_map_wordpress_post_type' AJAX function in all versions up to, and including, 5.3.14 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.	2024-07-24	7.2	CVE-2024-6753
WPWeb--WooCommerce - PDF Vouchers	The WooCommerce - PDF Vouchers plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 4.9.3. This is due to insufficient verification on the user being supplied during a QR code login through the plugin. This makes it possible for unauthenticated attackers to log in as any existing Voucher Vendor user on the site, if they have access to the user id.	2024-07-24	7.3	CVE-2024-7027
yogeshojha--rengine	reNgine is an automated reconnaissance framework for web applications. In versions 1.2.0 through 2.1.1, an authenticated command injection vulnerability in the WAF detection tool allows an authenticated attacker to remotely execute arbitrary commands as root user. The URL query parameter `url` is passed to	2024-07-23	8.8	CVE-2024-41661

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`subprocess.check_output` without any sanitization, resulting in a command injection vulnerability. This API endpoint is accessible by authenticated users with any use role. Because the process runs as `root`, an attacker has root access. Commit edd3c85ee16f93804ad38dac5602549d2d30a93e contains a patch for the issue.			
Admidio--admidio	Admidio is a free, open source user management system for websites of organizations and groups. In Admidio before version 4.3.9, there is an SQL Injection in the `/adm_program/modules/ecards/ecard_send.php` source file of the Admidio Application. The SQL Injection results in a compromise of the application's database. The value of `ecard_recipients `POST parameter is being directly concatenated with the SQL query in the source code causing the SQL Injection. The SQL Injection can be exploited by a member user, using blind condition-based, time-based, and Out of band interaction SQL Injection payloads. This vulnerability is fixed in 4.3.9.	2024-07-29	9.9	CVE-2024-37906
Admidio--admidio	Admidio is a free, open source user management system for websites of organizations and groups. In Admidio before version 4.3.10, there is a Remote Code Execution Vulnerability in the Message module of the Admidio Application, where it is possible to upload a PHP file in the attachment. The uploaded file can be accessed publicly through the URL `{admidio_base_url}/adm_my_files/messages_attachments/{file_name}`. The vulnerability is caused due to the lack of file extension verification, allowing malicious files to be uploaded to the server and public availability of the uploaded file. This vulnerability is fixed in 4.3.10.	2024-07-29	9	CVE-2024-38529
Adobe--InDesign Desktop	InDesign Desktop versions ID18.5.2, ID19.3 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.	2024-08-02	7.8	CVE-2024-39392
anji-plus--AJ-Report	anji-plus AJ-Report is affected by an authentication bypass vulnerability. A remote and unauthenticated attacker can append ";swagger-ui" to HTTP requests to bypass authentication and execute arbitrary Java on the victim server.	2024-08-02	9.8	CVE-2024-7314
Apache Software Foundation--Apache Linkis Basic management services	In Apache Linkis <= 1.5.0, Privilege Escalation in Basic management services where the attacking user is a trusted account allows access to Linkis's Token information. Users are advised to upgrade to version 1.6.0, which fixes this issue.	2024-08-02	8.8	CVE-2024-27181
Apache Software Foundation--Apache SeaTunnel Web	Web Authentication vulnerability in Apache SeaTunnel. Since the jwt key is hardcoded in the application, an attacker can forge any token to log in any user. Attacker can get secret key in /seatunnel-server/seatunnel-app/src/main/resources/application.yml and then create a token. This issue affects Apache SeaTunnel: 1.0.0. Users are recommended to upgrade to version 1.0.1, which fixes the issue.	2024-07-30	9.1	CVE-2023-48396
Apple--iOS and iPadOS	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.6.8, macOS Sonoma 14.5, macOS Monterey 12.7.6, watchOS 10.5, visionOS 1.3, tvOS 17.5, iOS 17.5 and iPadOS 17.5. An app may be able to execute arbitrary code with kernel privileges.	2024-07-29	7.8	CVE-2024-27826
Apple--iOS and iPadOS	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 16.7.9 and iPadOS 16.7.9, macOS Ventura 13.6.8, iOS 17.6 and iPadOS	2024-07-29	7.8	CVE-2024-40784

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	17.6, watchOS 10.6, tvOS 17.6, visionOS 1.3, macOS Sonoma 14.6. Processing a maliciously crafted file may lead to unexpected app termination.			
Apple--iOS and iPadOS	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 10.6, macOS Sonoma 14.6, iOS 17.6 and iPadOS 17.6, tvOS 17.6. An app may be able to bypass Privacy preferences.	2024-07-29	7.7	CVE-2024-40805
Apple--iOS and iPadOS	This issue was addressed through improved state management. This issue is fixed in watchOS 10.6, macOS Sonoma 14.6, iOS 17.6 and iPadOS 17.6, tvOS 17.6. An app may be able to bypass Privacy preferences.	2024-07-29	7.7	CVE-2024-40824
Apple--iOS and iPadOS	The issue was addressed with improved checks. This issue is fixed in watchOS 10.6, iOS 17.6 and iPadOS 17.6, iOS 16.7.9 and iPadOS 16.7.9, macOS Ventura 13.6.8. An attacker may be able to view restricted content from the lock screen.	2024-07-29	7.5	CVE-2024-40829
Apple--iOS and iPadOS	A logic issue was addressed with improved checks. This issue is fixed in watchOS 10.6, macOS Sonoma 14.6, iOS 17.6 and iPadOS 17.6, iOS 16.7.9 and iPadOS 16.7.9. A shortcut may be able to use sensitive data with certain actions without prompting the user.	2024-07-29	7.5	CVE-2024-40836
Apple--macOS	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14. A sandboxed process may be able to circumvent sandbox restrictions.	2024-07-29	8.6	CVE-2023-42918
Apple--macOS	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.6, macOS Monterey 12.7.6, macOS Ventura 13.6.8. A local attacker may be able to elevate their privileges.	2024-07-29	8.4	CVE-2024-40781

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Apple--macOS	An input validation issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.6, macOS Monterey 12.7.6, macOS Ventura 13.6.8. An app may be able to modify protected parts of the file system.	2024-07-29	8.4	CVE-2024-40800
Apple--macOS	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.6. An app may be able to modify protected parts of the file system.	2024-07-29	8.4	CVE-2024-40811
Apple--macOS	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sonoma 14.6, macOS Monterey 12.7.6, macOS Ventura 13.6.8. Third party app extensions may not receive the correct sandbox restrictions.	2024-07-29	8.4	CVE-2024-40821
Apple--macOS	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.6, macOS Monterey 12.7.6, macOS Ventura 13.6.8. A malicious app may be able to gain root privileges.	2024-07-29	8.4	CVE-2024-40828
Apple--macOS	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Ventura 13.4. An app may be able to gain elevated privileges.	2024-07-29	7.8	CVE-2023-42958
Apple--macOS	A race condition was addressed with improved state handling. This issue is fixed in macOS Sonoma 14. An app may be able to execute arbitrary code with kernel privileges.	2024-07-29	7	CVE-2023-42959
Apple--macOS	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sonoma 14.4. An unprivileged app may be able to log keystrokes in other apps including those using secure input mode.	2024-07-29	7.5	CVE-2024-27886
Apple--macOS	A permissions issue was addressed by removing vulnerable code and adding additional checks. This issue is fixed in macOS Sonoma 14.4. An app may be able to modify protected parts of the file system.	2024-07-29	7.1	CVE-2024-27888
Apple--macOS	The issue was addressed with improved restriction of data container access. This issue is fixed in macOS Sonoma 14.6, macOS Monterey 12.7.6, macOS Ventura 13.6.8. A malicious application may be able to bypass Privacy preferences.	2024-07-29	7.1	CVE-2024-40783
Apple--macOS	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.6, macOS Monterey 12.7.6, macOS Ventura 13.6.8. A local attacker may be able to elevate their privileges.	2024-07-29	7.8	CVE-2024-40802
Apple--macOS	A downgrade issue was addressed with additional code-signing restrictions. This issue is fixed in macOS Sonoma 14.6. An app may be able to bypass Privacy preferences.	2024-07-29	7.1	CVE-2024-40814
Apple--Safari	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 16.7.9 and iPadOS 16.7.9, Safari 17.6, iOS 17.6 and iPadOS 17.6,	2024-07-29	9.8	CVE-2024-40782

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	watchOS 10.6, tvOS 17.6, visionOS 1.3, macOS Sonoma 14.6. Processing maliciously crafted web content may lead to an unexpected process crash.			
AVTech--AVM1203 (IP Camera)	Commands can be injected over the network and executed without authentication.	2024-08-02	8.8	CVE-2024-7029
Bylancer--Quicklancer	A vulnerability was found in Bylancer Quicklancer 2.4. It has been rated as critical. This issue affects some unknown processing of the file /listing of the component GET Parameter Handler. The manipulation of the argument range2 leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272609 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	7.3	CVE-2024-7188
Canonical Ltd.--Juju	An issue was discovered in Juju that resulted in the leak of the sensitive context ID, which allows a local unprivileged attacker to access other sensitive data or relation accessible to the local charm.	2024-07-29	8.8	CVE-2024-6984
Cato Networks--SDP Client	Cato Networks Windows SDP Client Local Privilege Escalation via self-upgradeThis issue affects SDP Client: before 5.10.34.	2024-07-31	8.8	CVE-2024-6974
Cato Networks--SDP Client	Cato Networks Windows SDP Client Local Privilege Escalation via openssl configuration file. This issue affects SDP Client before 5.10.34.	2024-07-31	8.8	CVE-2024-6975
Cato Networks--SDP Client	Remote Code Execution in Cato Windows SDP client via crafted URLs. This issue affects Windows SDP Client before 5.10.34.	2024-07-31	7.5	CVE-2024-6973
CHANGING Information Technology--TCBServiSign Windows Version	The specific API in TCBServiSign Windows Version from CHANGING Information Technology does not properly validate server-side input. When a user visits a spoofed website, unauthenticated remote attackers can modify the `HKEY_CURRENT_USER` registry to execute arbitrary commands.	2024-08-02	8.8	CVE-2024-40720
CHANGING Information Technology--TCBServiSign Windows Version	The specific API in TCBServiSign Windows Version from CHANGING Information Technology does not properly validate server-side input. When a user visits a spoofed website, unauthenticated remote attackers can cause the TCBServiSign to load a DLL from an arbitrary path.	2024-08-02	8.8	CVE-2024-40721
charmbracelet--soft-serve	Soft Serve is a self-hostable Git server for the command line. Prior to 0.7.5, it is possible for a user who can commit files to a repository hosted by Soft Serve to execute arbitrary code via environment manipulation and Git. The issue is that Soft Serve passes all environment variables given by the client to git subprocesses. This includes environment variables that control program execution, such as LD_PRELOAD. This vulnerability is fixed in 0.7.5.	2024-08-01	8.1	CVE-2024-41956
ClickHouse--ClickHouse	It is possible to crash or redirect the execution flow of the ClickHouse server process from an unauthenticated vector by sending a specially crafted request to the ClickHouse server native interface. This redirection is limited to what is available within a 256-byte range of memory at the time of execution, and no known remote code execution (RCE) code has been produced or exploited. Fixes have been merged to all currently supported version of ClickHouse. If you are maintaining your own forked version of ClickHouse or using an older version and cannot upgrade, the fix for this vulnerability can be found in this commit https://github.com/ClickHouse/ClickHouse/pull/64024 .	2024-08-01	8.1	CVE-2024-6873 cb7ba516-3b07-4c98-b0c2-715220f1a8f6

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects--Online Bus Reservation Site	A vulnerability was found in code-projects Online Bus Reservation Site 1.0. It has been rated as critical. This issue affects some unknown processing of the file register.php. The manipulation of the argument Email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273203.	2024-07-31	7.3	CVE-2024-7311
CodeSolz--Better Find and Replace	Deserialization of Untrusted Data vulnerability in CodeSolz Better Find and Replace.This issue affects Better Find and Replace: from n/a through 1.6.1.	2024-08-01	8.3	CVE-2024-39636
Contest Gallery--Contest Gallery	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Contest Gallery allows Stored XSS.This issue affects Contest Gallery: from n/a through 23.1.2.	2024-08-01	7.1	CVE-2024-39631
CridioStudio--ListingPro	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in CridioStudio ListingPro allows PHP Local File Inclusion.This issue affects ListingPro: from n/a through 2.9.3.	2024-08-01	9	CVE-2024-39619
CridioStudio--ListingPro	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in CridioStudio ListingPro allows PHP Local File Inclusion.This issue affects ListingPro: from n/a through 2.9.3.	2024-08-01	8	CVE-2024-39621
CridioStudio--ListingPro	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in CridioStudio ListingPro allows PHP Local File Inclusion.This issue affects ListingPro: from n/a through 2.9.3.	2024-08-01	8.5	CVE-2024-39624
Cybonet--PineApp Mail Relay	Cybonet - CWE-22: Improper Limitation of a Pathname to a Restricted Directory	2024-07-30	7.5	CVE-2024-41695
Dahua--IPC-HX8XXX and NVR4XXX	A vulnerability has been found in Dahua products.Attackers can send carefully crafted data packets to the interface with vulnerabilities, causing the device to crash.	2024-07-31	7.5	CVE-2024-39944
Dahua--NVR4XXX and IPC-HX8XXX	A vulnerability has been found in Dahua products. Attackers can send carefully crafted data packets to the interface with vulnerabilities to initiate device initialization.	2024-07-31	8.6	CVE-2024-39950
Dahua--NVR4XXX	A vulnerability has been found in Dahua products. Attackers can send carefully crafted data packets to the interface with vulnerabilities, causing the device to crash.	2024-07-31	7.5	CVE-2024-39948
Dahua--NVR4XXX	A vulnerability has been found in Dahua products. Attackers can send carefully crafted data packets to the interface with vulnerabilities, causing the device to crash.	2024-07-31	7.5	CVE-2024-39949
deepset-ai--haystack	Haystack is an end-to-end LLM framework that allows you to build applications powered by LLMs, Transformer models, vector search and more. Haystack clients that let their users create and run Pipelines from scratch are vulnerable to remote code executions. Certain Components in Haystack use Jinja2 templates, if anyone can create and render that template on the client machine they run any code. The vulnerability has been fixed with Haystack `2.3.1`.	2024-07-31	7.5	CVE-2024-41950
Dell--Dell Peripheral Manager	Dell Peripheral Manager, versions prior to 1.7.6, contain an uncontrolled search path element vulnerability. An attacker could potentially exploit this vulnerability through preloading malicious DLL or symbolic link exploitation, leading to arbitrary code execution and escalation of privilege	2024-07-31	7.3	CVE-2024-32857
Dell--Dell Peripheral Manager	Dell Peripheral Manager, versions prior to 1.7.6, contain an uncontrolled search path element vulnerability. An attacker could potentially exploit this vulnerability through preloading malicious DLL or symbolic link exploitation, leading to arbitrary code execution and escalation of privilege	2024-07-31	7.8	CVE-2024-37127
Dell--Dell Peripheral Manager	Dell Peripheral Manager, versions prior to 1.7.6, contain an uncontrolled search path element vulnerability. An attacker could potentially exploit this vulnerability through preloading malicious DLL or symbolic link exploitation, leading to arbitrary code execution and escalation of privilege	2024-07-31	7.3	CVE-2024-37142
Delphix--Delphix Engine	Versions of Delphix Engine prior to Release 25.0.0.0 contain a flaw which results in Remote Code Execution (RCE).	2024-07-29	8.8	CVE-2024-6726
Dylan James--Zephyr Project Manager	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Dylan James Zephyr Project Manager.This issue affects Zephyr Project Manager: from n/a through 3.3.99.	2024-08-01	7.5	CVE-2024-38761

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
EC-CUBE CO.,LTD.--EC-CUBE 4 series	Acceptance of extraneous untrusted data with trusted data vulnerability exists in EC-CUBE 4 series. If this vulnerability is exploited, an attacker who obtained the administrative privilege may install an arbitrary PHP package. If the obsolete versions of PHP packages are installed, the product may be affected by some known vulnerabilities.	2024-07-30	7.2	CVE-2024-41924
enchant97--note-mark	Note Mark is a web-based Markdown notes app. A stored cross-site scripting (XSS) vulnerability in Note Mark allows attackers to execute arbitrary web scripts via a crafted payload injected into the URL value of a link in the markdown content. This vulnerability is fixed in 0.13.1.	2024-07-29	8.7	CVE-2024-41819
Epsiloncool--WP Fast Total Search	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Epsiloncool WP Fast Total Search allows Stored XSS.This issue affects WP Fast Total Search: from n/a through 1.68.232.	2024-08-01	7.1	CVE-2024-39663
FOGProject--fogproject	FOG is a cloning/imaging/rescue suite/inventory management system. FOG Server 1.5.10.41.2 can leak AD username and password when registering a computer. This vulnerability is fixed in 1.5.10.41.3 and 1.6.0-beta.1395.	2024-08-02	9.3	CVE-2024-42348
FOGProject--fogproject	FOG is a cloning/imaging/rescue suite/inventory management system. An improperly restricted file upload feature allows authenticated users to execute arbitrary code on the fogproject server. The Rebranding feature has a check on the client banner image requiring it to be 650 pixels wide and 120 pixels high. Apart from that, there are no checks on things like file extensions. This can be abused by appending a PHP webshell to the end of the image and changing the extension to anything the PHP web server will parse. This vulnerability is fixed in 1.5.10.41.	2024-07-31	8.8	CVE-2024-40645
FOGProject--fogproject	FOG is a free open-source cloning/imaging/rescue suite/inventory management system. The hostinfo page has missing/improper access control since only the host's mac address is required to obtain the configuration information. This data can only be retrieved if a task is pending on that host. Otherwise, an error message containing "Invalid tasking!" will be returned. The domainpassword in the hostinfo dump is hidden even to authenticated users, as it is displayed as a row of asterisks when navigating to the host's Active Directory settings. This vulnerability is fixed in 1.5.10.41.	2024-07-31	7.5	CVE-2024-41108
Google--Chrome	Uninitialized Use in Dawn in Google Chrome on Android prior to 127.0.6533.88 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Critical)	2024-08-01	8.8	CVE-2024-6990
Google--Chrome	Insufficient data validation in Dawn in Google Chrome on Android prior to 127.0.6533.88 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2024-08-01	8.8	CVE-2024-7256
Hewlett Packard Enterprise (HPE)--ClearPass Policy Manager (CPPM)	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit this vulnerability to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster.	2024-07-30	7.2	CVE-2024-41915
IdeaBox--PowerPack for Beaver Builder	Improper Privilege Management vulnerability in IdeaBox PowerPack for Beaver Builder allows Privilege Escalation.This issue affects PowerPack for Beaver Builder: from n/a through 2.33.0.	2024-08-01	8.8	CVE-2024-39633
IdeaBox--PowerPack Pro for Elementor	Improper Privilege Management vulnerability in IdeaBox PowerPack Pro for Elementor allows Privilege Escalation.This issue affects PowerPack Pro for Elementor: from n/a through 2.10.14.	2024-08-01	8.8	CVE-2024-39634
ImageMagick--ImageMagick	ImageMagick is a free and open-source software suite, used for editing and manipulating digital images. The `AppImage` version `ImageMagick` might use an empty path when setting `MAGICK_CONFIGURE_PATH` and `LD_LIBRARY_PATH` environment variables while executing, which might lead to arbitrary code execution by loading malicious configuration files or shared libraries in the current working directory while executing `ImageMagick`. The vulnerability is fixed in 7.11-36.	2024-07-29	7	CVE-2024-41817
IObit--Driver Booster	A vulnerability was found in IObit Driver Booster 11.0.0.0. It has been rated as critical. Affected by this issue is some unknown functionality in the library VCL120.BPL of the component BPL Handler. The manipulation leads to uncontrolled search path. Attacking locally is a requirement. The identifier of this vulnerability is VDB-273248. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-31	7.8	CVE-2024-7325

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IObit--DualSafe Password Manager	A vulnerability classified as critical has been found in IObit DualSafe Password Manager 1.4.0.3. This affects an unknown part in the library RTL120.BPL of the component BPL Handler. The manipulation leads to uncontrolled search path. It is possible to launch the attack on the local host. The identifier VDB-273249 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-31	7.8	CVE-2024-7326
IObit--iTop Data Recovery Pro	A vulnerability was found in IObit iTop Data Recovery Pro 4.4.0.687. It has been declared as critical. Affected by this vulnerability is an unknown functionality in the library madbasic_.bpl of the component BPL Handler. The manipulation leads to uncontrolled search path. Local access is required to approach this attack. The associated identifier of this vulnerability is VDB-273247. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-31	7.8	CVE-2024-7324
itsourcecode--Online Blood Bank Management System	A vulnerability classified as critical has been found in itsourcecode Online Blood Bank Management System 1.0. This affects an unknown part of the file /admin/index.php of the component Admin Login. The manipulation of the argument user leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273231.	2024-07-31	7.3	CVE-2024-7320
itsourcecode--Ticket Reservation System	A vulnerability classified as critical was found in itsourcecode Ticket Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file login.php of the component Login Page. 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. The identifier VDB-273529 was assigned to this vulnerability.	2024-08-03	7.3	CVE-2024-7444
jetmonsters--JetFormBuilder Dynamic Blocks Form Builder	The JetFormBuilder plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 3.3.4.1. This is due to improper restriction on user meta fields. This makes it possible for authenticated attackers, with administrator-level and above permissions, to register as super-admins on the sites configured as multi-sites.	2024-08-03	7.2	CVE-2024-7291
Kofi Mokome--Message Filter for Contact Form 7	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kofi Mokome Message Filter for Contact Form 7 allows Reflected XSS.This issue affects Message Filter for Contact Form 7: from n/a through 1.6.1.1.	2024-08-01	7.1	CVE-2024-39647
Kunal Nagar--Custom 404 Pro	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kunal Nagar Custom 404 Pro allows Reflected XSS.This issue affects Custom 404 Pro: from n/a through 3.11.1.	2024-08-01	7.1	CVE-2024-39646
Lenovo--Driver Manager	A path hijacking vulnerability was reported in Lenovo Driver Manager prior to version 3.1.1307.1308 that could allow a local user to execute code with elevated privileges.	2024-07-31	7.8	CVE-2023-1577
Lenovo--PC Manager	A vulnerability was reported in Lenovo PC Manager prior to version 2.8.90.11211 that could allow a local attacker to escalate privileges.	2024-07-31	7.8	CVE-2019-6197
Lenovo--PC Manager	A vulnerability was reported in Lenovo PC Manager prior to version 2.8.90.11211 that could allow a local attacker to escalate privileges.	2024-07-31	7.8	CVE-2019-6198
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix may_goto with negative offset. Zac's syzbot crafted a bpf prog that exposed two bugs in may_goto. The 1st bug is the way may_goto is patched. When offset is negative it should be patched differently. The 2nd bug is in the verifier: when current state may_goto_depth is equal to visited state may_goto_depth it means there is an actual infinite loop. It's not correct to prune exploration of the program at this point. Note, that this check doesn't limit the program to only one may_goto insn, since 2nd and any further may_goto will increment may_goto_depth only in the queued state pushed for future exploration. The current state will have may_goto_depth == 0 regardless of number of may_goto insns and the verifier has to explore the program until bpf_exit.	2024-07-29	7.8	CVE-2024-42072
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: mpi3mr: Sanitise num_phys Information is stored in mr_sas_port->phy_mask, values larger then size of this field shouldn't be allowed.	2024-07-30	7.8	CVE-2024-42159
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: f2fs: check validation of fault attrs in f2fs_build_fault_attr() - It missed to check validation of fault attrs in parse_options(), let's fix to add check condition in	2024-07-30	7.8	CVE-2024-42160

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	f2fs_build_fault_attr(). - Use f2fs_build_fault_attr() in __sbi_store() to clean up code.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: dsa: mv88e6xxx: Correct check for empty list Since commit a3c53be55c95 ("net: dsa: mv88e6xxx: Support multiple MDIO busses") mv88e6xxx_default_mdio_bus() has checked that the return value of list_first_entry() is non-NULL. This appears to be intended to guard against the list chip->mdios being empty. However, it is not the correct check as the implementation of list_first_entry is not designed to return NULL for empty lists. Instead, use list_first_entry_or_null() which does return NULL if the list is empty. Flagged by Smatch. Compile tested only.	2024-07-30	7.8	CVE-2024-42224
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: replace skb_put with skb_put_zero Avoid potentially reusing uninitialized data	2024-07-30	7.5	CVE-2024-42225
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Using uninitialized value *size when calling amdgpu_vce_cs_reloc Initialize the size before calling amdgpu_vce_cs_reloc, such as case 0x03000001. V2: To really improve the handling we would actually need to have a separate value of 0xffffffff.(Christian)	2024-07-30	7	CVE-2024-42228
looks_awesome--WordPress Menu Plugin Superfly Responsive Menu	The WordPress Menu Plugin - Superfly Responsive Menu plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.0.29. This is due to missing or incorrect nonce validation on the ajax_handle_delete_icons() function. This makes it possible for unauthenticated attackers to delete arbitrary files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Please not the CSRF was patched in 5.0.28, however, adequate directory traversal protection wasn't introduced until 5.0.30.	2024-08-02	8.8	CVE-2024-3238
MakeStories Team--MakeStories (for Google Web Stories)	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in MakeStories Team MakeStories (for Google Web Stories) allows Path Traversal, Server Side Request Forgery.This issue affects MakeStories (for Google Web Stories): from n/a through 3.0.3.	2024-08-01	7.1	CVE-2024-38746
ManageEngine--OpManager	Zohocorp ManageEngine OpManager, OpManager Plus, OpManager MSP and RMM versions 128317 and below are vulnerable to authenticated SQL injection in the URL monitoring.	2024-07-29	8.3	CVE-2024-6748
Martin Gibson--WP GoToWebinar	Cross-Site Request Forgery (CSRF) vulnerability in Martin Gibson WP GoToWebinar allows Cross-Site Scripting (XSS).This issue affects WP GoToWebinar: from n/a through 15.7.	2024-08-02	7.1	CVE-2024-38776
Matrix--Tafnit v8	Matrix Tafnit v8 - CWE-552: Files or Directories Accessible to External Parties	2024-07-30	7.5	CVE-2024-38429
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0, 9.5.x <= 9.5.6, 9.7.x <= 9.7.5 and 9.8.x <= 9.8.1 fail to properly validate that the channel that comes from the sync message is a shared channel, when shared channels are enabled, which allows a malicious remote to add users to arbitrary teams and channels	2024-08-01	8.7	CVE-2024-39274
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0, 9.5.x <= 9.5.6, 9.7.x <= 9.7.5 and 9.8.x <= 9.8.1 fail to disallow unsolicited invites to expose access to local channels, when shared channels are enabled, which allows a malicious remote to send an invite with the ID of an existing local channel, and that local channel will then become shared without the consent of the local admin.	2024-08-01	8.7	CVE-2024-39777
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0, 9.5.x <= 9.5.6, 9.7.x <= 9.7.5, 9.8.x <= 9.8.1 fail to disallow the modification of local users when syncing users in shared channels. which allows a malicious remote to overwrite an existing local user.	2024-08-01	7.4	CVE-2024-36492
Microsoft--Dynamics 365 Field Service (on-premises) v7 series	Weak authentication in Microsoft Dynamics 365 allows an unauthenticated attacker to elevate privileges over a network.	2024-07-31	9	CVE-2024-38182

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
monkeytypegame--monkeytype	Monkeytype is a minimalistic and customizable typing test. Monkeytype is vulnerable to Poisoned Pipeline Execution through Code Injection in its ci-failure-comment.yml GitHub Workflow, enabling attackers to gain pull-requests write access. The ci-failure-comment.yml workflow is triggered when the Monkey CI workflow completes. When it runs, it will download an artifact uploaded by the triggering workflow and assign the contents of ./pr_num/pr_num.txt artifact to the steps.pr_num_reader.outputs.content WorkFlow variable. It is not validated that the variable is actually a number and later it is interpolated into a JS script allowing an attacker to change the code to be executed. This issue leads to pull-requests write access. This vulnerability is fixed in 24.30.0.	2024-08-02	8.3	CVE-2024-41127
Motorola--Q14 Mesh Router Firmware	An authentication bypass vulnerability could allow an attacker to access API functions without authentication.	2024-07-31	7.3	CVE-2022-4001
Motorola--Q14 Mesh Router Firmware	A command injection vulnerability could allow an authenticated user to execute operating system commands as root via a specially crafted API request.	2024-07-31	7.2	CVE-2022-4002
n/a--n/a	An issue was discovered in Italtel i-MCS NFV 12.1.0-20211215. There is Incorrect Access Control.	2024-07-29	9.1	CVE-2024-28805
n/a--n/a	Prototype pollution in allpro form-manager 0.7.4 allows attackers to run arbitrary code and cause other impacts via the functions setDefaults, mergeBranch, and Object.setObjectValue.	2024-07-30	9.8	CVE-2024-36572
n/a--n/a	SQL Injection vulnerability in Lost and Found Information System 1.0 allows a remote attacker to escalate privileges via the id parameter to php-lfis/admin/categories/manage_category.php.	2024-07-29	9.8	CVE-2024-37858
n/a--n/a	An issue in Horizon Business Services Inc. Caterease 16.0.1.1663 through 24.0.1.2405 and possibly later versions, allows a remote attacker to perform command line execution through SQL Injection due to improper neutralization of special elements used in an OS command.	2024-08-02	9.8	CVE-2024-38882
n/a--n/a	An issue in Horizon Business Services Inc. Caterease 16.0.1.1663 through 24.0.1.2405 and possibly later versions, allows a remote attacker to perform a Drop Encryption Level attack due to the selection of a less-secure algorithm during negotiation.	2024-08-02	9.1	CVE-2024-38883
n/a--n/a	Studio 42 elFinder 2.1.64 is vulnerable to Incorrect Access Control. Copying files with an unauthorized extension between server directories allows an arbitrary attacker to expose secrets, perform RCE, etc.	2024-07-30	9.8	CVE-2024-38909
n/a--n/a	Prototype Pollution in alykoshin mini-deep-assign v0.0.8 allows an attacker to execute arbitrary code or cause a Denial of Service (DoS) and cause other impacts via the _assign() method at (/lib/index.js:91)	2024-07-30	9.8	CVE-2024-38983
n/a--n/a	Prototype Pollution in lukebond json-override 0.2.0 allows attackers to to execute arbitrary code or cause a Denial of Service (DoS) via the __proto__ property.	2024-07-30	9.8	CVE-2024-38984
n/a--n/a	Prototype Pollution in 75lb deep-merge 1.1.1 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) and cause other impacts via merge methods of lodash to merge objects.	2024-07-30	9.8	CVE-2024-38986
n/a--n/a	chase-moskal snapstate v0.0.9 was discovered to contain a prototype pollution via the function attemptNestedProperty. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-30	9.8	CVE-2024-39010
n/a--n/a	Prototype Pollution in chargeover redoc v2.0.9-rc.69 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) and cause other impacts via the function mergeObjects.	2024-07-30	9.8	CVE-2024-39011
n/a--n/a	Use of insecure hashing algorithm in the Gravatar's service in Navidrome v0.52.3 allows attackers to manipulate a user's account information.	2024-08-01	9.1	CVE-2024-41259
n/a--n/a	D-Link DIR-820LW REVB FIRMWARE PATCH 2.03.B01_TC contains hardcoded credentials in the Telnet service, enabling attackers to log in remotely to the Telnet service and perform arbitrary commands.	2024-07-30	9.8	CVE-2024-41610

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	In D-Link DIR-860L REVA FIRMWARE PATCH 1.10..B04, the Telnet service contains hardcoded credentials, enabling attackers to log in remotely to the Telnet service and perform arbitrary commands.	2024-07-30	9.8	CVE-2024-41611
n/a--n/a	SQL Injection vulnerability in Lost and Found Information System 1.0 allows a remote attacker to escalate privileges via id parameter to php-lfis/admin/categories/view_category.php.	2024-07-29	8.8	CVE-2024-37857
n/a--n/a	An issue in Horizon Business Services Inc. Caterease 16.0.1.1663 through 24.0.1.2405 and possibly later versions, allows a local attacker to perform a Password Brute Forcing attack due to improper restriction of excessive authentication attempts.	2024-08-02	8.4	CVE-2024-38888
n/a--n/a	An issue in Horizon Business Services Inc. Caterease Software 16.0.1.1663 through 24.0.1.2405 and possibly later versions allows a local attacker to perform an Authentication Bypass by Capture-replay attack due to insufficient protection against capture-replay attacks.	2024-08-02	8.4	CVE-2024-38890
n/a--n/a	An issue in beego v.2.2.0 and before allows a remote attacker to escalate privileges via the getCacheFileName function in file.go file	2024-07-31	8.8	CVE-2024-40465
n/a--n/a	RaspAP before 3.1.5 allows an attacker to escalate privileges: the www-data user has write access to the restapi.service file and also possesses Sudo privileges to execute several critical commands without a password.	2024-07-29	8.3	CVE-2024-41637
n/a--n/a	os/linux/elf.rb in Homebrew brew before 4.2.20 uses ldd to load ELF files obtained from untrusted sources, which allows attackers to achieve code execution via an ELF file with a custom .interp section. NOTE: this code execution would occur during an un-sandboxed binary relocation phase, which occurs before a user would expect execution of downloaded package content. (237d1e783f7ee261beaba7d3f6bde22da7148b0a was the tested vulnerable version.)	2024-07-31	8.3	CVE-2024-42381
N/A--N/A	Langflow versions prior to 1.0.13 suffer from a Privilege Escalation vulnerability, allowing a remote and low privileged attacker to gain super admin privileges by performing a mass assignment request on the '/api/v1/users' endpoint.	2024-07-30	8.8	CVE-2024-7297 vulnreport@tenable.com
N/A--N/A	The Weave server API allows remote users to fetch files from a specific directory, but due to a lack of input validation, it is possible to traverse and leak arbitrary files remotely. In various common scenarios, this allows a low-privileged user to assume the role of the server admin.	2024-07-31	8.8	CVE-2024-7340
n/a--n/a	SQL injection vulnerability in AzureSoft MyHorus 4.3.5 allows authenticated users to execute arbitrary SQL commands via unspecified vectors.	2024-08-02	7.5	CVE-2024-28297
n/a--n/a	An issue was discovered in Italtel i-MCS NFV 12.1.0-20211215. Stored Cross-site scripting (XSS) can occur via POST.	2024-07-29	7.1	CVE-2024-28804
n/a--n/a	An issue was discovered in Italtel i-MCS NFV 12.1.0-20211215. Remote unauthenticated attackers can upload files at an arbitrary path.	2024-07-29	7.5	CVE-2024-28806
n/a--n/a	Buffer Overflow vulnerability in Tenda AC10 v4 US_AC10V4.0si_V16.03.10.20_cn allows a remote attacker to execute arbitrary code via the Virtual_Data_Check function in the bin/httpd component.	2024-07-29	7.5	CVE-2024-33365
n/a--n/a	An issue in Horizon Business Services Inc. Caterease 16.0.1.1663 through 24.0.1.2405 and possibly later versions, allows a remote attacker to perform a Rainbow Table Password cracking attack due to the use of one-way hashes without salts when storing user passwords.	2024-08-02	7.5	CVE-2024-38881
n/a--n/a	An issue in Horizon Business Services Inc. Caterease 16.0.1.1663 through 24.0.1.2405 and possibly later versions, allows a remote attacker to perform	2024-08-02	7.5	CVE-2024-38885

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthorized access using known operating system credentials due to hardcoded SQL user credentials in the client application.			
n/a--n/a	goframe v2.7.2 is configured to skip TLS certificate verification, possibly allowing attackers to execute a man-in-the-middle attack via the gclient component.	2024-07-31	7.1	CVE-2024-41253
n/a--n/a	filestash v0.4 is configured to skip TLS certificate verification when using the FTPS protocol, possibly allowing attackers to execute a man-in-the-middle attack via the Init function of index.go.	2024-07-31	7.5	CVE-2024-41255
n/a--n/a	mmudb v1.9.3 was discovered to use the HTTP protocol in the ShowMetricsRaw and ShowMetricsAsText functions, possibly allowing attackers to intercept communications via a man-in-the-middle attack.	2024-07-31	7.4	CVE-2024-41262
n/a--n/a	A TLS certificate verification issue discovered in cortex v0.42.1 allows attackers to obtain sensitive information via the makeOperatorRequest function.	2024-08-01	7.5	CVE-2024-41265
n/a--n/a	A Server-Side Request Forgery (SSRF) in the Plugins Page of WonderCMS v3.4.3 allows attackers to force the application to make arbitrary requests via injection of crafted URLs into the pluginThemeUrl parameter.	2024-07-30	7.1	CVE-2024-41305
n/a--n/a	Buffer Overflow vulnerability in host-host NEUQ_board v.1.0 allows a remote attacker to cause a denial of service via the password.h component.	2024-07-29	7.5	CVE-2024-41631
ninjateam--File Manager Pro Filester	The File Manager Pro - Filester plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'njt_fs_saveSettingRestrictions' function in all versions up to, and including, 1.8.2. This makes it possible for authenticated attackers, with a role that has been granted permissions by an Administrator, to update the plugin settings for user role restrictions, including allowing file types such as .php to be uploaded.	2024-08-03	7.5	CVE-2024-7031
openbmc--slpd-lite	slpd-lite is a unicast SLP UDP server. Any OpenBMC system that includes the slpd-lite package is impacted. Installing this package is the default when building OpenBMC. Nefarious users can send slp packets to the BMC using UDP port 427 to cause memory overflow issues within the slpd-lite daemon on the BMC. Patches will be available in the latest openbmc/slpd-lite repository.	2024-07-31	9.8	CVE-2024-41660
Philip Hazel--SDoP	SDoP versions prior to 1.11 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 XML file, arbitrary code may be executed on the user's environment.	2024-07-29	8.8	CVE-2024-41881
Plug&Track--Sensor Net Connect V2	A "CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')" allows malicious users to permanently inject arbitrary Javascript code.	2024-07-31	7.7	CVE-2024-31199
Plug&Track--Thermoscan IP	A "CWE-732: Incorrect Permission Assignment for Critical Resource" in the ThermoscanIP installation folder allows a local attacker to perform a Local Privilege Escalation.	2024-07-31	8.4	CVE-2024-31202
Point B Ltd--Getscreen Agent	A vulnerability was found in Point B Ltd Getscreen Agent 2.19.6 on Windows. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file getscreen.msi of the component Installation. The manipulation leads to creation of temporary file with insecure permissions. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-273337 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but was not able to provide a technical response in time.	2024-08-01	7.8	CVE-2024-7358
Priority--PRI WEB Portal Add-On for Priority ERP on prem	Priority PRI WEB Portal Add-On for Priority ERP on prem - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	2024-07-30	7.5	CVE-2024-41696
Progress--MOVEit Transfer	Improper Authentication vulnerability in Progress MOVEit Transfer (SFTP module) can lead to Privilege Escalation.This issue affects MOVEit Transfer: from 2023.0.0 before 2023.0.12, from 2023.1.0 before 2023.1.7, from 2024.0.0 before 2024.0.3.	2024-07-29	7.3	CVE-2024-6576 security@progress.com security@progress.com

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat OpenStack Platform 13 (Queens)	An incomplete fix for CVE-2023-1625 was found in openstack-heat. Sensitive information may possibly be disclosed through the OpenStack stack abandon command with the hidden feature set to True and the CVE-2023-1625 fix applied.	2024-08-02	7.4	CVE-2024-7319
Revmakx--Backup and Staging by WP Time Capsule	Improper Privilege Management vulnerability in Revmakx Backup and Staging by WP Time Capsule allows Privilege Escalation, Authentication Bypass.This issue affects Backup and Staging by WP Time Capsule: from n/a through 1.22.20.	2024-08-01	9.8	CVE-2024-38770
sapcc--elektra	Elektra is an opinionated Openstack Dashboard for Operators and Consumers of Openstack Services. A code injection vulnerability was found in the live search functionality of the Ruby on Rails based Elektra web application. An authenticated user can craft a search term containing Ruby code, which later flows into an `eval` sink which executes the code. Fixed in commit 8bce00be93b95a6512ff68fe86bf9554e486bc02.	2024-08-01	9.6	CVE-2024-41961
SiberianCMS--SiberianCMS v5.0.8	SiberianCMS - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	2024-07-30	9.8	CVE-2024-41702
Siemens--Omnivise T3000 Application Server	A vulnerability has been identified in Omnivise T3000 Application Server (All versions), Omnivise T3000 Domain Controller (All versions), Omnivise T3000 Network Intrusion Detection System (NIDS) (All versions), Omnivise T3000 Product Data Management (PDM) (All versions), Omnivise T3000 Security Server (All versions), Omnivise T3000 Terminal Server (All versions), Omnivise T3000 Thin Client (All versions), Omnivise T3000 Whitelisting Server (All versions). The affected devices stores initial system credentials without sufficient protection. An attacker with remote shell access or physical access could retrieve the credentials leading to confidentiality loss allowing the attacker to laterally move within the affected network.	2024-08-02	8.2	CVE-2024-38877
Siemens--Omnivise T3000 Application Server	A vulnerability has been identified in Omnivise T3000 Application Server (All versions >= R9.2), Omnivise T3000 Domain Controller (All versions >= R9.2), Omnivise T3000 Product Data Management (PDM) (All versions >= R9.2), Omnivise T3000 Terminal Server (All versions >= R9.2), Omnivise T3000 Thin Client (All versions >= R9.2), Omnivise T3000 Whitelisting Server (All versions >= R9.2). The affected application regularly executes user modifiable code as a privileged user. This could allow a local authenticated attacker to execute arbitrary code with elevated privileges.	2024-08-02	7.8	CVE-2024-38876
Siemens--Omnivise T3000 Application Server	A vulnerability has been identified in Omnivise T3000 Application Server (All versions). Affected devices allow authenticated users to export diagnostics data. The corresponding API endpoint is susceptible to path traversal and could allow an authenticated attacker to download arbitrary files from the file system.	2024-08-02	7.2	CVE-2024-38878
Siemens--Omnivise T3000 Application Server	A vulnerability has been identified in Omnivise T3000 Application Server (All versions). The affected system exposes the port of an internal application on the public network interface allowing an attacker to circumvent authentication and directly access the exposed application.	2024-08-02	7.5	CVE-2024-38879
Simopro Technology--WinMatrix3	The login functionality of WinMatrix3 Web package from Simopro Technology lacks proper validation of user input, allowing unauthenticated remote attackers to inject SQL commands to read, modify, and delete database contents.	2024-07-29	9.8	CVE-2024-7201
Simopro Technology--WinMatrix3	The query functionality of WinMatrix3 Web package from Simopro Technology lacks proper validation of user input, allowing unauthenticated remote attackers to inject SQL commands to read, modify, and delete database contents.	2024-07-29	9.8	CVE-2024-7202
Sky Co.,LTD.--SKYSEA Client View	Incorrect privilege assignment vulnerability exists in SKYSEA Client View Ver.6.010.06 to Ver.19.210.04e. If a user who can log in to the PC where the product's Windows client is installed places a specially crafted DLL file in a specific folder, arbitrary code may be executed with SYSTEM privilege.	2024-07-29	7.8	CVE-2024-41139
Sky Co.,LTD.--SKYSEA Client View	Path traversal vulnerability exists in SKYSEA Client View Ver.3.013.00 to Ver.19.210.04e. If this vulnerability is exploited, an arbitrary executable file may be executed by a user who can log in to the PC where the product's Windows client is installed.	2024-07-29	7.5	CVE-2024-41726
Softnext--SN OS 12.1	The web services of Softnext's products, Mail SQR Expert and Mail Archiving Expert do not properly validate user input, allowing unauthenticated remote attackers to inject arbitrary OS commands and execute them on the remote server.	2024-07-29	9.8	CVE-2024-5670

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SourceCodester--Complaints Report Management System	A vulnerability was found in SourceCodester Complaints Report Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/ajax.php?action=login. 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. The identifier VDB-272617 was assigned to this vulnerability.	2024-07-29	7.3	CVE-2024-7196
SourceCodester--Establishment Billing Management System	A vulnerability was found in SourceCodester Establishment Billing Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/ajax.php?action=login of the component Login. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273155.	2024-07-31	7.3	CVE-2024-7286
SourceCodester--Lot Reservation Management System	A vulnerability was found in SourceCodester Lot Reservation Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/ajax.php?action=login. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273148.	2024-07-31	7.3	CVE-2024-7279
SourceCodester--School Log Management System	A vulnerability classified as critical has been found in SourceCodester School Log Management System 1.0. Affected is an unknown function of the file /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. VDB-272790 is the identifier assigned to this vulnerability.	2024-07-30	7.3	CVE-2024-7219
SourceCodester--Simple Realtime Quiz System	A vulnerability was found in SourceCodester Simple Realtime Quiz System 1.0 and classified as critical. This issue affects some unknown processing of the file /ajax.php?action=login of the component Login. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273353 was assigned to this vulnerability.	2024-08-01	7.3	CVE-2024-7369
SourceCodester--Tracking Monitoring Management System	A vulnerability was found in SourceCodester Tracking Monitoring Management System 1.0. It has been classified as critical. This affects an unknown part of the file /ajax.php?action=login of the component 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. The identifier VDB-273345 was assigned to this vulnerability.	2024-08-01	7.3	CVE-2024-7366
tensorflow--tensorflow	TensorFlow is an end-to-end open source platform for machine learning. `array_ops.upper_bound` causes a segfault when not given a rank 2 tensor. The fix will be included in TensorFlow 2.13 and will also cherrypick this commit on TensorFlow 2.12.	2024-07-30	7.5	CVE-2023-33976
tgstation--tgstation-server	tgstation-server is a production scale tool for BYOND server management. Prior to 6.8.0, low permission users using the "Set .dme Path" privilege could potentially set malicious .dme files existing on the host machine to be compiled and executed. These .dme files could be uploaded via tgstation-server (requiring a separate, isolated privilege) or some other means. A server configured to execute in BYOND's trusted security level (requiring a third separate, isolated privilege OR being set by another user) could lead to this escalating into remote code execution via BYOND's shell() proc. The ability to execute this kind of attack is a known side effect of having privileged TGS users, but normally requires multiple privileges with known weaknesses. This vector is not intentional as it does not require control over the where deployment code is sourced from and _may_ not require remote write access to an instance's `Configuration` directory. This problem is fixed in versions 6.8.0 and above.	2024-07-29	8.4	CVE-2024-41799
TOTOLINK-- A3300R	A vulnerability was found in TOTOLINK A3300R 17.0.0cu.557_B20221024 and classified as critical. Affected by this issue is the function UploadCustomModule of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument File leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-273254 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-01	8.8	CVE-2024-7331
TOTOLINK--A3600R	A vulnerability, which was classified as critical, has been found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. Affected by this issue is the function loginauth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password/http_host leads to buffer overflow. The attack may be launched	2024-07-29	8.8	CVE-2024-7173

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remotely. VDB-272594 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
TOTOLINK--A3600R	A vulnerability, which was classified as critical, was found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. This affects the function setdeviceName of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument deviceMac/deviceName leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272595. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	8.8	CVE-2024-7174
TOTOLINK--A3600R	A vulnerability was found in TOTOLINK A3600R 4.1.2cu.5182_B20201102 and classified as critical. This issue affects the function setIpQosRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument comment leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272597 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	8.8	CVE-2024-7176
TOTOLINK--A3600R	A vulnerability was found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. It has been classified as critical. Affected is the function setLanguageCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument langType leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-272598 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	8.8	CVE-2024-7177
TOTOLINK--A3600R	A vulnerability was found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. It has been declared as critical. Affected by this vulnerability is the function setMacQos of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument priority/macAddress leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272599. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	8.8	CVE-2024-7178
TOTOLINK--A3600R	A vulnerability was found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. It has been rated as critical. Affected by this issue is the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument startTime/endTime leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272600. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	8.8	CVE-2024-7179
TOTOLINK--A3600R	A vulnerability classified as critical has been found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. This affects the function setPortForwardRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument comment leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272601 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	8.8	CVE-2024-7180
TOTOLINK--A3600R	A vulnerability, which was classified as critical, has been found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. This issue affects the function setUpgradeFW of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272603. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	8.8	CVE-2024-7182
TOTOLINK--A3600R	A vulnerability, which was classified as critical, was found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. Affected is the function setUploadSetting of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272604. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	8.8	CVE-2024-7183
TOTOLINK--A3600R	A vulnerability has been found in TOTOLINK A3600R 4.1.2cu.5182_B20201102 and classified as critical. Affected by this vulnerability is the function setUrlFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument url leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272605 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	8.8	CVE-2024-7184

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
TOTOLINK--A3600R	A vulnerability was found in TOTOLINK A3600R 4.1.2cu.5182_B20201102 and classified as critical. Affected by this issue is the function setWebWlanIdx of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument webWlanIdx leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-272606 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	8.8	CVE-2024-7185
TOTOLINK--A3600R	A vulnerability was found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. It has been classified as critical. This affects the function setWiFiAclAddConfig of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument comment leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272607. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	8.8	CVE-2024-7186
TOTOLINK--A3600R	A vulnerability was found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. It has been declared as critical. This vulnerability affects the function UploadCustomModule of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument File leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272608. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	8.8	CVE-2024-7187
TOTOLINK--A7000R	A vulnerability, which was classified as critical, has been found in TOTOLINK A7000R 9.1.0u.6268_B20220504. This issue affects the function loginauth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272783. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-30	8.8	CVE-2024-7212
TOTOLINK--A7000R	A vulnerability, which was classified as critical, was found in TOTOLINK A7000R 9.1.0u.6268_B20220504. Affected is the function setWizardCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ssid leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272784. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-30	8.8	CVE-2024-7213
TOTOLINK--CP450	A vulnerability was found in TOTOLINK CP450 4.1.0cu.747_B20191224. It has been classified as critical. This affects an unknown part of the file /web_cste/cgi-bin/product.ini of the component Telnet Service. The manipulation leads to use of hard-coded password. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273255. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-01	9.8	CVE-2024-7332
TOTOLINK--EX1200L	A vulnerability was found in TOTOLINK EX1200L 9.3.5u.6146_B20201023. It has been rated as critical. This issue affects the function UploadCustomModule of the file /cgi-bin/cstecgi.cgi. The manipulation leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273257 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-01	8.8	CVE-2024-7334
TOTOLINK--EX1200L	A vulnerability, which was classified as critical, has been found in TOTOLINK EX1200L 9.3.5u.6146_B20201023. Affected by this issue is the function loginauth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument http_host leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273260. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-01	8.8	CVE-2024-7337
TOTOLINK--EX1200L	A vulnerability, which was classified as critical, was found in TOTOLINK EX1200L 9.3.5u.6146_B20201023. This affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument week/sTime/eTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273261 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-01	8.8	CVE-2024-7338
TOTOLINK--EX200	A vulnerability classified as critical has been found in TOTOLINK EX200 4.0.3c.7646_B20201211. Affected is the function getSaveConfig of the file /cgi-bin/cstecgi.cgi?action=save&setting. The manipulation of the argument http_host	2024-08-01	8.8	CVE-2024-7335

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-273258 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
TOTOLINK--EX200	A vulnerability classified as critical was found in TOTOLINK EX200 4.0.3c.7646_B20201211. Affected by this vulnerability is the function loginauth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument http_host leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273259. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-01	8.8	CVE-2024-7336
TOTOLINK--N350RT	A vulnerability was found in TOTOLINK N350RT 9.3.5u.6139_B20201216. It has been declared as critical. This vulnerability affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument week/sTime/eTime leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273256. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-01	8.8	CVE-2024-7333
twisted--twisted	Twisted is an event-based framework for internet applications, supporting Python 3.6+. The HTTP 1.0 and 1.1 server provided by twisted.web could process pipelined HTTP requests out-of-order, possibly resulting in information disclosure. This vulnerability is fixed in 24.7.0rc1.	2024-07-29	8.3	CVE-2024-41671
Uncanny Owl--Tin Canny Reporting for LearnDash	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Uncanny Owl Tin Canny Reporting for LearnDash allows Reflected XSS.This issue affects Tin Canny Reporting for LearnDash: from n/a through 4.3.0.7.	2024-08-01	7.1	CVE-2024-39656
Unknown--Business Card	The Business Card WordPress plugin through 1.0.0 does not prevent high privilege users like administrators from uploading malicious PHP files, which could allow them to run arbitrary code on servers hosting their site, even in MultiSite configurations.	2024-07-30	7.2	CVE-2024-5807
Unknown--CZ Loan Management	The CZ Loan Management WordPress plugin through 1.1 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection	2024-07-30	9.1	CVE-2024-5975
Unknown--Ultimate Classified Listings	The Ultimate Classified Listings WordPress plugin before 1.3 does not validate the `ucl_page` and `layout` parameters allowing unauthenticated users to access PHP files on the server from the listings page	2024-07-29	7.5	CVE-2024-5882
Unknown--Ultimate Classified Listings	The Ultimate Classified Listings WordPress plugin before 1.4 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	2024-08-01	7.1	CVE-2024-6529
Unknown--User Profile Builder	The User Profile Builder WordPress plugin before 3.11.8 does not have proper authorisation, allowing unauthenticated users to upload media files via the async upload functionality of WP.	2024-07-29	9.1	CVE-2024-6366
Unknown--User Profile Builder	it's possible for an attacker to gain administrative access without having any kind of account on the targeted site and perform unauthorized actions. This is due to improper logic flow on the user registration process.	2024-07-31	9.8	CVE-2024-6695
Unknown--WooCommerce Customers Manager	The WooCommerce Customers Manager WordPress plugin before 30.1 does not have CSRF checks in some bulk actions, which could allow attackers to make logged in admins perform unwanted actions, such as deleting customers via CSRF attacks	2024-08-01	8.1	CVE-2024-3983
Unknown--WpStickyBar	The WpStickyBar WordPress plugin through 2.1.0 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection	2024-07-30	9.8	CVE-2024-5765
vikasratudi--Lifetime free Drag & Drop Contact Form Builder for WordPress VForm	The Lifetime free Drag & Drop Contact Form Builder for WordPress VForm plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 2.1.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-31	7.2	CVE-2024-6770

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WebAppick--CTX Feed	Improper Privilege Management vulnerability in WebAppick CTX Feed allows Privilege Escalation.This issue affects CTX Feed: from n/a through 6.5.6.	2024-08-01	7.2	CVE-2024-38775
WPForms, LLC.--WPForms User Registration	Improper Privilege Management vulnerability in WPForms, LLC. WPForms User Registration allows Privilege Escalation.This issue affects WPForms User Registration: from n/a through 2.1.0.	2024-08-01	8	CVE-2023-52209
wpmudev--Forminator Contact Form, Payment Form & Custom Form Builder	The Forminator plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.29.1 via class-forminator-addon-hubspot-wp-api.php. This makes it possible for unauthenticated attackers to extract the HubSpot integration developer API key and make unauthorized changes to the plugin's HubSpot integration or expose personally identifiable information from plugin users using the HubSpot integration.	2024-08-02	7.5	CVE-2024-7389
WPWeb Elite--WooCommerce PDF Vouchers	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPWeb Elite WooCommerce PDF Vouchers allows Reflected XSS.This issue affects WooCommerce PDF Vouchers: from n/a before 4.9.5.	2024-08-01	7.1	CVE-2024-39652
xibosignage--xibo-cms	Xibo is a content management system (CMS). An SQL injection vulnerability was discovered in the API routes inside the CMS responsible for Filtering DataSets. This allows an authenticated user to to obtain and modify arbitrary data from the Xibo database by injecting specially crafted values in to the APIs for importing JSON and importing a Layout containing DataSet data. Users should upgrade to version 3.3.12 or 4.0.14 which fix this issue	2024-07-30	8.1	CVE-2024-41802
xpeedstudio--FundEngine Donation and Crowdfunding Platform	The FundEngine plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.7.0. This is due to the plugin not properly verifying user meta updated through the update_user_meta function. This makes it possible for authenticated attackers, with subscriber-level access and above, to update their user meta which can be leveraged to update their capabilities to gain administrator access.	2024-08-01	8.8	CVE-2024-6698
xwiki--xwiki-platform	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit right on any page can perform arbitrary remote code execution by adding instances of `XWiki.SearchSuggestConfig` and `XWiki.SearchSuggestSourceClass` to their user profile or any other page. This compromises the confidentiality, integrity and availability of the whole XWiki installation. This vulnerability has been patched in XWiki 14.10.21, 15.5.5 and 15.10.2.	2024-07-31	9.9	CVE-2024-37901
xwiki--xwiki-platform	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. By creating a conflict when another user with more rights is currently editing a page, it is possible to execute JavaScript snippets on the side of the other user, which compromises the confidentiality, integrity and availability of the whole XWiki installation. This has been patched in XWiki 15.10.8 and 16.3.0RC1.	2024-07-31	9	CVE-2024-41947
yaycommerce--YayExtra WooCommerce Extra Product Options	The YayExtra - WooCommerce Extra Product Options plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the handle_upload_file function in all versions up to, and including, 1.3.7. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	2024-08-03	9.8	CVE-2024-7257

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
2code -- himer	The Himer WordPress theme before 2.1.1 does not sanitise and escape some of its Post settings, which could allow high privilege users such as Contributor to perform Stored Cross-Site Scripting attacks	2024-07-03	5.4	CVE-2024-2234

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
2code -- himer	The Himer WordPress theme before 2.1.1 does not have CSRF checks in some places, which could allow attackers to make users join private groups via a CSRF attack	2024-07-03	4.3	CVE-2024-2040
2code -- himer	The Himer WordPress theme before 2.1.1 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks. These include declining and accepting group invitations or leaving a group	2024-07-03	4.3	CVE-2024-2233
2code -- himer	The Himer WordPress theme before 2.1.1 does not have CSRF checks in some places, which could allow attackers to make users vote on any polls, including those they don't have access to via a CSRF attack	2024-07-03	4.3	CVE-2024-2235
2code -- wpqa_builder	The WPQA Builder WordPress plugin before 6.1.1 does not sanitise and escape some of its Slider settings, which could allow high privilege users such as contributor to perform Stored Cross-Site Scripting attacks	2024-07-03	5.4	CVE-2024-2375
aimeos--ai-admin-jsonadm	aimeos/ai-admin-jsonadm is the Aimeos e-commerce JSON API for administrative tasks. In versions prior to 2020.10.13, 2021.10.6, 2022.10.3, 2023.10.4, and 2024.4.2, improper access control allows editors to remove admin group and locale configuration in the Aimeos backend. Versions 2020.10.13, 2021.10.6, 2022.10.3, 2023.10.4, and 2024.4.2 contain a fix for the issue.	2024-07-02	5.5	CVE-2024-39322
aimeos--ai-controller-frontend	aimeos/ai-controller-frontend is the Aimeos frontend controller. Prior to versions 2024.04.2, 2023.10.9, 2022.10.8, 2021.10.8, and 2020.10.15, aimeos/ai-controller-frontend doesn't reset the payment status of a user's basket after the user completes a purchase. Versions 2024.04.2, 2023.10.9, 2022.10.8, 2021.10.8, and 2020.10.15 fix this issue.	2024-07-02	5.3	CVE-2024-39325
apollo13themes -- rife_elementor_extensions_\&_templates	The Rife Elementor Extensions & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tag' attribute within the plugin's Writing Effect Headline widget in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-02	5.4	CVE-2024-5504
Automattic--Newspack Ads	Cross Site Scripting (XSS) vulnerability in Automattic Newspack Ads allows Stored XSS.This issue affects Newspack Ads: from n/a through 1.47.1.	2024-07-04	6.5	CVE-2024-37474
Automattic--Newspack Campaigns	Cross Site Scripting (XSS) vulnerability in Automattic Newspack Campaigns allows Stored XSS.This issue affects Newspack Campaigns: from n/a through 2.31.1.	2024-07-04	6.5	CVE-2024-37476
Axelerant--Testimonials Widget	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Axelerant Testimonials Widget allows Stored XSS.This issue affects Testimonials Widget: from n/a through 4.0.4.	2024-07-06	6.5	CVE-2024-37553
biplob018--Image Hover Effects - Caption Hover with Carousel	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in biplob018 Image Hover Effects - Caption Hover with Carousel allows Stored XSS.This issue affects Image Hover Effects - Caption Hover with Carousel: from n/a through 3.0.2.	2024-07-06	6.5	CVE-2024-37546
boot_store_project -- boot_store	The Boot Store theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' parameter within the theme's Button shortcode in all versions up to, and including, 1.6.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and	2024-07-02	5.4	CVE-2024-5938

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
cedcommerce -- one_click_order_re-order	The One Click Order Re-Order plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ced_ocor_save_general_setting' function in all versions up to, and including, 1.1.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change the plugin settings, including adding stored cross-site scripting.	2024-07-04	5.4	CVE-2024-5641
CHANGING--Mobile One Time Password	CHANGING Mobile One Time Password does not properly filter parameters for the file download functionality, allowing remote attackers with administrator privilege to read arbitrary file on the system.	2024-07-01	4.9	CVE-2024-3122
Checkmk GmbH--Checkmk	Stored XSS in Checkmk before versions 2.3.0p8, 2.2.0p29, 2.1.0p45, and 2.0.0 (EOL) allows users to execute arbitrary scripts by injecting HTML elements	2024-07-03	6.5	CVE-2024-6052
Checkmk GmbH--Checkmk	Improper neutralization of input in Checkmk before versions 2.3.0p8, 2.2.0p28, 2.1.0p45, and 2.0.0 (EOL) allows attackers to craft malicious links that can facilitate phishing attacks.	2024-07-02	4.3	CVE-2024-38857
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root. Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials.	2024-07-01	6.7	CVE-2024-20399
CodeAstrology Team--UltraAddons Elementor Lite (Header & Footer Builder, Menu Builder, Cart Icon, Shortcode)	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CodeAstrology Team UltraAddons Elementor Lite (Header & Footer Builder, Menu Builder, Cart Icon, Shortcode).This issue affects UltraAddons Elementor Lite (Header & Footer Builder, Menu Builder, Cart Icon, Shortcode): from n/a through 1.1.6.	2024-07-06	6.5	CVE-2024-37554
coderberg -- residencecms	A stored cross-site scripting (XSS) vulnerability exists in ResidenceCMS 2.10.1 that allows a low-privilege user to create malicious property content with HTML inside which acts as a stored XSS payload.	2024-07-02	5.4	CVE-2024-39143
davidlingren -- media_library_assistant	The Media Library Assistant plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the order parameter in all versions up to, and including, 3.17 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.	2024-07-02	6.1	CVE-2024-5544
Delinea--Centrify PAS	Vulnerability in Delinea Centrify PAS v. 21.3 and possibly others. The application is prone to the path traversal vulnerability allowing listing of arbitrary directory outside the root directory of the web application. Versions 23.1-HF7 and on have the patch.	2024-07-02	5	CVE-2024-5866
dell -- powerscale_onefs	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privilege attacker could potentially exploit this vulnerability, leading to privilege escalation.	2024-07-02	6.7	CVE-2024-32854

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- powerscale_onefs	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to unauthorized gain of root-level access.	2024-07-02	6.7	CVE-2024-37126
dell -- powerscale_onefs	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an incorrect privilege assignment vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of service and Elevation of privileges.	2024-07-02	6.7	CVE-2024-37132
dell -- powerscale_onefs	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability, leading to unauthorized gain of root-level access.	2024-07-02	6.7	CVE-2024-37133
dell -- powerscale_onefs	Dell PowerScale OneFS versions 8.2.2.x through 9.8.0.0 contain an improper privilege management vulnerability. A local high privileged attacker could potentially exploit this vulnerability to gain root-level access.	2024-07-02	6.7	CVE-2024-37134
Dell--CPG BIOS	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability to modify a UEFI variable, leading to denial of service and escalation of privileges	2024-07-02	5.1	CVE-2024-0158
Delower--WP To Do	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Delower WP To Do allows Stored XSS.This issue affects WP To Do: from n/a through 1.3.0.	2024-07-06	6.5	CVE-2024-37539
discourse--discourse	Discourse is an open-source discussion platform. Prior to version 3.2.3 on the `stable` branch and version 3.3.0.beta4 on the `beta` and `tests-passed` branches, a malicious actor could get the FastImage library to redirect requests to an internal Discourse IP. This issue is patched in version 3.2.3 on the `stable` branch and version 3.3.0.beta4 on the `beta` and `tests-passed` branches. No known workarounds are available.	2024-07-03	6.4	CVE-2024-37157
discourse--discourse	Discourse is an open-source discussion platform. Prior to version 3.2.3 on the `stable` branch and version 3.3.0.beta3 on the `tests-passed` branch, an attacker can execute arbitrary JavaScript on users' browsers by posting a specific URL containing maliciously crafted meta tags. This issue only affects sites with Content Security Polic (CSP) disabled. The problem has been patched in version 3.2.3 on the `stable` branch and version 3.3.0.beta3 on the `tests-passed` branch. As a workaround, ensure CSP is enabled on the forum.	2024-07-03	4.2	CVE-2024-35234
discourse--discourse	Discourse is an open-source discussion platform. Prior to version 3.2.3 on the `stable` branch, version 3.3.0.beta3 on the `beta` branch, and version 3.3.0.beta4-dev on the `tests-passed` branch, a rogue staff user could suspend other staff users preventing them from logging in to the site. The issue is patched in version 3.2.3 on the `stable` branch, version 3.3.0.beta3 on the `beta` branch, and version 3.3.0.beta4-dev on the `tests-passed` branch. No known workarounds are available.	2024-07-03	4.9	CVE-2024-36113
dotcamp -- ultimate_blocks	The Ultimate Blocks - WordPress Blocks Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the title tag parameter in all versions up to, and including, 3.1.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access and higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-02	5.4	CVE-2024-3513
dotcamp -- ultimate_blocks	The Ultimate Blocks - WordPress Blocks Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's blocks in all versions up to, and including, 3.1.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with	2024-07-02	5.4	CVE-2024-4268

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
envoyproxy--envoy	Envoy is a cloud-native, open source edge and service proxy. Prior to versions 1.30.4, 1.29.7, 1.28.5, and 1.27.7. Envoy references already freed memory when route hash policy is configured with cookie attributes. Note that this vulnerability has been fixed in the open as the effect would be immediately apparent if it was configured. Memory allocated for holding attribute values is freed after configuration was parsed. During request processing Envoy will attempt to copy content of de-allocated memory into request cookie header. This can lead to arbitrary content of Envoy's memory to be sent to the upstream service or abnormal process termination. This vulnerability is fixed in Envoy versions v1.30.4, v1.29.7, v1.28.5, and v1.27.7. As a workaround, do not use cookie attributes in route action hash policy.	2024-07-01	6.5	CVE-2024-39305
ethyca--fides	Fides is an open-source privacy engineering platform, and `SERVER_SIDE_FIDES_API_URL` is a server-side configuration environment variable used by the Fides Privacy Center to communicate with the Fides webserver backend. The value of this variable is a URL which typically includes a private IP address, private domain name, and/or port. A vulnerability present starting in version 2.19.0 and prior to version 2.39.2rc0 allows an unauthenticated attacker to make a HTTP GET request from the Privacy Center that discloses the value of this server-side URL. This could result in disclosure of server-side configuration giving an attacker information on server-side ports, private IP addresses, and/or private domain names. The vulnerability has been patched in Fides version 2.39.2rc0. No known workarounds are available.	2024-07-03	5.3	CVE-2024-31223
flowiseai -- flowise	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, a reflected cross-site scripting vulnerability occurs in the `api/v1/chatflows/id` endpoint. If the default configuration is used (unauthenticated), an attacker may be able to craft a specially crafted URL that injects Javascript into the user sessions, allowing the attacker to steal information, create false popups, or even redirect the user to other websites without interaction. If the chatflow ID is not found, its value is reflected in the 404 page, which has type text/html. This allows an attacker to attach arbitrary scripts to the page, allowing an attacker to steal sensitive information. This XSS may be chained with the path injection to allow an attacker without direct access to Flowise to read arbitrary files from the Flowise server. As of time of publication, no known patches are available.	2024-07-01	6.1	CVE-2024-36422
FlowiseAI--Flowise	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, a reflected cross-site scripting vulnerability occurs in the `/api/v1/public-chatflows/id` endpoint. If the default configuration is used (unauthenticated), an attacker may be able to craft a specially crafted URL that injects Javascript into the user sessions, allowing the attacker to steal information, create false popups, or even redirect the user to other websites without interaction. If the chatflow ID is not found, its value is reflected in the 404 page, which has type text/html. This allows an attacker to attach arbitrary scripts to the page, allowing an attacker to steal sensitive information. This XSS may be chained with the path injection to allow an attacker without direct access to Flowise to read arbitrary files from the Flowise server. As of time of publication, no known patches are available.	2024-07-01	6.1	CVE-2024-36423
FlowiseAI--Flowise	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, a reflected cross-site scripting vulnerability occurs in the `/api/v1/chatflows-streaming/id` endpoint. If the default configuration is	2024-07-01	6.1	CVE-2024-37145

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	used (unauthenticated), an attacker may be able to craft a specially crafted URL that injects Javascript into the user sessions, allowing the attacker to steal information, create false popups, or even redirect the user to other websites without interaction. If the chatflow ID is not found, its value is reflected in the 404 page, which has type text/html. This allows an attacker to attach arbitrary scripts to the page, allowing an attacker to steal sensitive information. This XSS may be chained with the path injection to allow an attacker without direct access to Flowise to read arbitrary files from the Flowise server. As of time of publication, no known patches are available.			
FlowiseAI--Flowise	Flowise is a drag & drop user interface to build a customized large language model flow. In version 1.4.3 of Flowise, a reflected cross-site scripting vulnerability occurs in the `/api/v1/credentials/id` endpoint. If the default configuration is used (unauthenticated), an attacker may be able to craft a specially crafted URL that injects Javascript into the user sessions, allowing the attacker to steal information, create false popups, or even redirect the user to other websites without interaction. If the chatflow ID is not found, its value is reflected in the 404 page, which has type text/html. This allows an attacker to attach arbitrary scripts to the page, allowing an attacker to steal sensitive information. This XSS may be chained with the path injection to allow an attacker without direct access to Flowise to read arbitrary files from the Flowise server. As of time of publication, no known patches are available.	2024-07-01	6.1	CVE-2024-37146
geoserver -- geoserver	GeoServer is an open source server that allows users to share and edit geospatial data. Starting in version 2.10.0 and prior to versions 2.24.4 and 2.25.1, GeoServer's Server Status page and REST API lists all environment variables and Java properties to any GeoServer user with administrative rights as part of those modules' status message. These variables/properties can also contain sensitive information, such as database passwords or API keys/tokens. Additionally, many community-developed GeoServer container images `export` other credentials from their start-up scripts as environment variables to the GeoServer (`java`) process. The precise scope of the issue depends on which container image is used and how it is configured. The `about status` API endpoint which powers the Server Status page is only available to administrators.Depending on the operating environment, administrators might have legitimate access to credentials in other ways, but this issue defeats more sophisticated controls (like break-glass access to secrets or role accounts).By default, GeoServer only allows same-origin authenticated API access. This limits the scope for a third-party attacker to use an administrator's credentials to gain access to credentials. The researchers who found the vulnerability were unable to determine any other conditions under which the GeoServer REST API may be available more broadly. Users should update container images to use GeoServer 2.24.4 or 2.25.1 to get the bug fix. As a workaround, leave environment variables and Java system properties hidden by default. Those who provide the option to re-enable it should communicate the impact and risks so that users can make an informed choice.	2024-07-01	4.9	CVE-2024-34696
HCL Software--Nomad server on Domino	HCL Nomad server on Domino fails to properly handle users configured with limited Domino access resulting in a possible denial of service vulnerability.	2024-07-05	5.3	CVE-2024-23588
Hitachi--Hitachi Ops Center Common Services	Incorrect Default Permissions, Improper Preservation of Permissions vulnerability in Hitachi Ops Center Common Services allows File Manipulation.This issue affects Hitachi Ops Center Common Services: before 11.0.2-00.	2024-07-02	5.1	CVE-2024-2819
hitout -- carsale	A vulnerability has been found in Hitout Carsale 1.0 and classified as critical. This vulnerability affects unknown code of the file OrderController.java. The manipulation of the argument orderBy leads to sql injection. The attack can be	2024-07-02	6.5	CVE-2024-6438

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	initiated remotely. The exploit has been disclosed to the public and may be used. VDB-270166 is the identifier assigned to this vulnerability.			
ICONICS--GENESIS64	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in the licensing feature of ICONICS GENESIS64 versions 10.97 to 10.97.2, Mitsubishi Electric GENESIS64 versions 10.97 to 10.97.2 and Mitsubishi Electric MC Works64 all versions allows a local attacker to execute a malicious code with administrative privileges by tampering with a specific file that is not protected by the system.	2024-07-04	6.7	CVE-2024-1574
ICONICS--GENESIS64	Improper Authentication vulnerability in the mobile monitoring feature of ICONICS GENESIS64 versions 10.97 to 10.97.2, Mitsubishi Electric GENESIS64 versions 10.97 to 10.97.2 and Mitsubishi Electric MC Works64 all versions allows a remote unauthenticated attacker to bypass proper authentication and log in to the system when all of the following conditions are met: * Active Directory is used in the security setting. * "Automatic log in" option is enabled in the security setting. * The IcoAnyGlass IIS Application Pool is running under an Active Directory Domain Account. * The IcoAnyGlass IIS Application Pool account is included in GENESIS64TM and MC Works64 Security and has permission to log in.	2024-07-04	5.9	CVE-2024-1573
itsourcecode--Farm Management System	A vulnerability was found in itsourcecode Farm Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /quarantine.php?id=3. The manipulation of the argument pigno/breed/reason leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-270241 was assigned to this vulnerability. NOTE: Original submission mentioned parameter pigno only but the VulDB data analysis team determined two additional parameters to be affected as well.	2024-07-02	6.3	CVE-2024-6453
JetBrains--TeamCity	In JetBrains TeamCity before 2024.03.3 application token could be exposed in EC2 Cloud Profile settings	2024-07-01	5	CVE-2024-39879
JetBrains--TeamCity	In JetBrains TeamCity before 2024.03.3 private key could be exposed via testing GitHub App Connection	2024-07-01	4.1	CVE-2024-39878
Johnson Controls--American Dynamics Illustra Essentials Gen 4	Under certain circumstances the Linux users credentials may be recovered by an authenticated user.	2024-07-02	6.8	CVE-2024-32756
Johnson Controls--American Dynamics Illustra Essentials Gen 4	Under certain circumstances unnecessary user details are provided within system logs	2024-07-02	6.8	CVE-2024-32757
Johnson Controls--American Dynamics Illustra Essentials Gen 4	Under certain circumstances the web interface users credentials may be recovered by an authenticated user.	2024-07-02	6.8	CVE-2024-32932
jungo -- windriver	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error.	2024-07-02	5.5	CVE-2023-51777
jungo -- windriver	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.1.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	2024-07-02	5.5	CVE-2023-51778

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jungo -- windriver	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error.	2024-07-02	5.5	CVE-2024-22102
jungo -- windriver	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.6.0 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	2024-07-02	5.5	CVE-2024-22103
jungo -- windriver	Out-of-Bounds Write vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error and Denial of Service (DoS).	2024-07-02	5.5	CVE-2024-22104
jungo -- windriver	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.5.1 allows local attackers to cause a Windows blue screen error.	2024-07-02	5.5	CVE-2024-22105
jungo -- windriver	Denial of Service (DoS) vulnerability in Jungo WinDriver before 12.7.0 allows local attackers to cause a Windows blue screen error.	2024-07-02	5.5	CVE-2024-25087
kiloview -- p1_firmware	A 'Cross-site Scripting' (XSS) vulnerability, characterized by improper input neutralization during web page generation, has been discovered. This vulnerability allows for Stored XSS attacks to occur. Multiple areas within the administration interface of the webserver lack adequate input validation, resulting in multiple instances of Stored XSS vulnerabilities.	2024-07-02	5.4	CVE-2023-41922
Kiloview--P1/P2	The server supports at least one cipher suite which is on the NCSC-NL list of cipher suites to be phased out, increasing the risk of cryptographic weaknesses.	2024-07-02	5.3	CVE-2023-41927
Kiloview--P1/P2	The device is observed to accept deprecated TLS protocols, increasing the risk of cryptographic weaknesses.	2024-07-02	5.3	CVE-2023-41928
KisaragiEffective--toy-blog	toy-blog is a headless content management system implementation. Starting in version 0.5.4 and prior to version 0.6.1, articles with private visibility can be read if the reader does not set credentials for the request. Users should upgrade to 0.6.1 or later to receive a patch. No known workarounds are available.	2024-07-01	6.5	CVE-2024-39313
KisaragiEffective--toy-blog	toy-blog is a headless content management system implementation. Starting in version 0.4.3 and prior to version 0.5.0, the administrative password was leaked through the command line parameter. The problem was patched in version 0.5.0. As a workaround, pass `--read-bearer-token-from-stdin` to the launch arguments and feed the token from the standard input in version 0.4.14 or later. Earlier versions do not have this workaround.	2024-07-01	4.7	CVE-2024-39314
leap13 -- premium_addons_for_elementor	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown widget in all versions up to, and including, 4.10.35 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-03	5.4	CVE-2024-6340
leap13 -- premium_addons_for_elementor	The Premium Addons for Elementor plugin for WordPress is vulnerable to Regular Expression Denial of Service (ReDoS) in all versions up to, and including, 4.10.35. This is due to processing user-supplied input as a regular expression. This makes it possible for authenticated attackers, with Author-level access and above, to create and query a malicious post title, resulting in slowing server resources.	2024-07-04	4.3	CVE-2024-6434
linlinjava--litemall	A vulnerability classified as critical was found in linlinjava litemall up to 1.8.0. Affected by this vulnerability is an unknown functionality of the file AdminGoodscontroller.java. The manipulation of the argument goodsId/goodsSn/name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-270235.	2024-07-02	6.3	CVE-2024-6452

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Livemesh--Livemesh Addons for Elementor	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Livemesh Livemesh Addons for Elementor.This issue affects Livemesh Addons for Elementor: from n/a through 8.3.7.	2024-07-06	6.5	CVE-2024-37547
livemeshelementor -- addons_for_elementor	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 8.3.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-04	5.4	CVE-2024-2926
livemeshelementor -- addons_for_elementor	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Marquee Text Widget, Testimonials Widget, and Testimonial Slider widgets in all versions up to, and including, 8.3.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-04	5.4	CVE-2024-3638
livemeshelementor -- addons_for_elementor	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Posts Grid widget in all versions up to, and including, 8.3.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-04	5.4	CVE-2024-3639
matrix-org--matrix-appservice-irc	matrix-appservice-irc is a Node.js IRC bridge for the Matrix messaging protocol. The fix for GHSA-wm4w-7h2q-3pf7 / CVE-2024-32000 included in matrix-appservice-irc 2.0.0 relied on the Matrix homeserver-provided timestamp to determine whether a user has access to the event they're replying to when determining whether or not to include a truncated version of the original event in the IRC message. Since this value is controlled by external entities, a malicious Matrix homeserver joined to a room in which a matrix-appservice-irc bridge instance (before version 2.0.1) is present can fabricate the timestamp with the intent of tricking the bridge into leaking room messages the homeserver should not have access to. matrix-appservice-irc 2.0.1 drops the reliance on `origin_server_ts` when determining whether or not an event should be visible to a user, instead tracking the event timestamps internally. As a workaround, it's possible to limit the amount of information leaked by setting a reply template that doesn't contain the original message.	2024-07-05	4.3	CVE-2024-39691
mattermost -- mattermost	Mattermost versions 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2, 9.5.x <= 9.5.5 fail to prevent specifying a RemoteId when creating a new user which allows an attacker to specify both a remoteId and the user ID, resulting in creating a user with a user-defined user ID. This can cause some broken functionality in User Management such administrative actions against the user not working.	2024-07-03	6.5	CVE-2024-6428
mattermost -- mattermost	Mattermost versions 9.5.x <= 9.5.5 and 9.8.0,Â when using shared channels with multiple remote servers connected,Â fail to check that the remote server A requesting the server B to update the profile picture of a user is the remote that actually has the user as a local one .Â This allows a malicious remote A to change the profile images of users that belong to another remote server C that is connected to the server A.	2024-07-03	5.3	CVE-2024-36257
mattermost -- mattermost	Mattermost versions 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2 and 9.5.x <= 9.5.5 fail toÂ prevent users from specifying a RemoteId for their posts which allows an attacker to specify both a remoteId and the post ID, resulting in creating a post	2024-07-03	5.4	CVE-2024-39361

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	with a user-defined post ID. This can cause some broken functionality in the channel or thread with user-defined posts			
mattermost -- mattermost	Mattermost versions 9.5.x <= 9.5.5 and 9.8.0Â fail to properly sanitize the recipients of a webhook event which allows an attacker monitoring webhook events to retrieve the channel IDs of archived or restored channels.	2024-07-03	5.3	CVE-2024-39807
mattermost -- mattermost	Mattermost versions 9.8.x <= 9.8.0, 9.7.x <= 9.7.4, 9.6.x <= 9.6.2 and 9.5.x <= 9.5.5, when shared channels are enabled, fail to use constant time comparison for remote cluster tokens which allows an attacker to retrieve the remote cluster token via a timing attack during remote cluster token comparison.	2024-07-03	5.9	CVE-2024-39830
mongodb -- mongodb	A command for refining a collection shard key is missing an authorization check. This may cause the command to run directly on a shard, leading to either degradation of query performance, or to revealing chunk boundaries through timing side channels. This affects MongoDB Server v5.0 versions, prior to 5.0.22, MongoDB Server v6.0 versions, prior to 6.0.11 and MongoDB Server v7.0 versions prior to 7.0.3.	2024-07-01	6.5	CVE-2024-6375
MongoDB Inc-- libbson	The bson_string_append function in MongoDB C Driver may be vulnerable to a buffer overflow where the function might attempt to allocate too small of buffer and may lead to memory corruption of neighbouring heap memory. This issue affects libbson versions prior to 1.27.1	2024-07-03	5.3	CVE-2024-6383
MongoDB Inc-- libbson	The bson_strfreev function in the MongoDB C driver library may be susceptible to an integer overflow where the function will try to free memory at a negative offset. This may result in memory corruption. This issue affected libbson versions prior to 1.26.2	2024-07-02	4	CVE-2024-6381
MongoDB Inc-- MongoDB Rust Driver	Incorrect handling of certain string inputs may result in MongoDB Rust driver constructing unintended server commands. This may cause unexpected application behavior including data modification. This issue affects MongoDB Rust Driver 2.0 versions prior to 2.8.2	2024-07-02	6.4	CVE-2024-6382
n/a--n/a	FFmpeg 7.0 is vulnerable to Buffer Overflow. There is a SEGV at libavcodec/hevcdec.c:2947:22 in hevc_frame_end.	2024-07-01	6.6	CVE-2024-32228
n/a--n/a	Tada5hi sp-common v0.5.4 was discovered to contain a prototype pollution via the function mergeDeep. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	6.3	CVE-2024-38990
n/a--n/a	adolph_dudu ratio-swiper v0.0.2 was discovered to contain a prototype pollution via the function extendDefaults. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	6.5	CVE-2024-38997
n/a--n/a	adolph_dudu ratio-swiper v0.0.2 was discovered to contain a prototype pollution via the function parse. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	6.5	CVE-2024-39000
n/a--n/a	adolph_dudu ratio-swiper 0.0.2 was discovered to contain a prototype pollution via the function parse. This vulnerability allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via injecting arbitrary properties.	2024-07-01	6.5	CVE-2024-39853
n/a--n/a	MachForm up to version 19 is affected by an authenticated stored cross-site scripting.	2024-07-01	5.4	CVE-2024-37764
n/a--n/a	In the Twilio Authy API, accessed by Authy Android before 25.1.0 and Authy iOS before 26.1.0, an unauthenticated endpoint provided access to certain phone-number data, as exploited in the wild in June 2024. Specifically, the endpoint accepted a stream of requests containing phone numbers, and responded with information about whether each phone number was registered with Authy. (Authy accounts were not compromised, however.)	2024-07-02	5.3	CVE-2024-39891

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--ORIPA	A vulnerability was found in ORIPA up to 1.72. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file src/main/java/oripa/persistence/doc/loader/LoaderXML.java. The manipulation leads to deserialization. The attack can be launched remotely. Upgrading to version 1.80 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-270169 was assigned to this vulnerability.	2024-07-02	6.3	CVE-2024-6441
n/a--ShopXO	A vulnerability was found in ShopXO up to 6.1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file extend/base/Uploader.php. The manipulation of the argument source leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-270367. NOTE: The original disclosure confuses CSRF with SSRF.	2024-07-05	5.5	CVE-2024-6524
N/A--VMware Cloud Director Availability	VMware Cloud Director Availability contains an HTML injection vulnerability. A malicious actor with network access to VMware Cloud Director Availability can craft malicious HTML tags to execute within replication tasks.	2024-07-04	6.4	CVE-2024-22277
NationalSecurityAgency--skills-service	SkillTree is a micro-learning gamification platform. Prior to version 2.12.6, the endpoint `/admin/projects/{projectname}/skills/{skillname}/video` (and probably others) is open to a cross-site request forgery (CSRF) vulnerability. Due to the endpoint being CSRFable e.g POST request, supports a content type that can be exploited (multipart file upload), makes a state change and has no CSRF mitigations in place (samesite flag, CSRF token). It is possible to perform a CSRF attack against a logged in admin account, allowing an attacker that can target a logged in admin of Skills Service to modify the videos, captions, and text of the skill. Version 2.12.6 contains a patch for this issue.	2024-07-02	4.4	CVE-2024-39326
pomerium--pomerium	Pomerium is an identity and context-aware access proxy. Prior to version 0.26.1, the Pomerium user info page (at `/.pomerium`) unintentionally included serialized OAuth2 access and ID tokens from the logged-in user's session. These tokens are not intended to be exposed to end users. This issue may be more severe in the presence of a cross-site scripting vulnerability in an upstream application proxied through Pomerium. If an attacker could insert a malicious script onto a web page proxied through Pomerium, that script could access these tokens by making a request to the `/.pomerium` endpoint. Upstream applications that authenticate only the ID token may be vulnerable to user impersonation using a token obtained in this manner. Note that an OAuth2 access token or ID token by itself is not sufficient to hijack a user's Pomerium session. Upstream applications should not be vulnerable to user impersonation via these tokens provided the application verifies the Pomerium JWT for each request, the connection between Pomerium and the application is secured by mTLS, or the connection between Pomerium and the application is otherwise secured at the network layer. The issue is patched in Pomerium v0.26.1. No known workarounds are available.	2024-07-02	5.7	CVE-2024-39315
posimyth --the_plus_addons_for_elementor	The The Plus Addons for Elementor - Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Countdown' widget in all versions up to, and including, 5.6.1 due to insufficient input sanitization and output escaping on user supplied 'text_days' attribute. 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.	2024-07-03	5.4	CVE-2024-4482
qualcomm --315_5g_iot_modem_firmware	Transient DOS while loading the TA ELF file.	2024-07-01	5.5	CVE-2024-21462

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- fastconnect_6900_firmware	Information disclosure when ASLR relocates the IMEM and Secure DDR portions as one chunk in virtual address space.	2024-07-01	6.5	CVE-2024-21460
Qualcomm, Inc.--Snapdragon	Information Disclosure while parsing beacon frame in STA.	2024-07-01	6.5	CVE-2024-21456
rack--rack	Rack is a modular Ruby web server interface. Starting in version 3.1.0 and prior to version 3.1.5, Regular Expression Denial of Service (ReDoS) vulnerability exists in the `Rack::Request::Helpers` module when parsing HTTP Accept headers. This vulnerability can be exploited by an attacker sending specially crafted `Accept-Encoding` or `Accept-Language` headers, causing the server to spend excessive time processing the request and leading to a Denial of Service (DoS). The fix for CVE-2024-26146 was not applied to the main branch and thus while the issue was fixed for the Rack v3.0 release series, it was not fixed in the v3.1 release series until v3.1.5. Users of versions on the 3.1 branch should upgrade to version 3.1.5 to receive the fix.	2024-07-02	6.5	CVE-2024-39316
radiustheme -- the_post_grid	The The Post Grid - Shortcode, Gutenberg Blocks and Elementor Addon for Post Grid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the section title tag attribute in all versions up to, and including, 7.7.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-02	5.4	CVE-2024-1427
rankmath -- seo	The Rank Math SEO WordPress plugin before 1.0.219 does not sanitise and escape some of its settings, which could allow users with access to the General Settings (by default admin, however such access can be given to lower roles via the Role Manager feature of the Rank Math SEO WordPress plugin before 1.0.219) to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	2024-07-02	5.4	CVE-2024-4627
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in the virtio-net device in QEMU. When enabling the RSS feature on the virtio-net network card, the indirections_table data within RSS becomes controllable. Setting excessively large values may cause an index out-of-bounds issue, potentially resulting in heap overflow access. This flaw allows a privileged user in the guest to crash the QEMU process on the host.	2024-07-05	6	CVE-2024-6505
Robert Macchi--WP Scraper	Server-Side Request Forgery (SSRF) vulnerability in Robert Macchi WP Scraper.This issue affects WP Scraper: from n/a through 5.7.	2024-07-06	4.9	CVE-2024-37208
samsung -- android	Improper input validation in parsing application information from RTCP packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to execute arbitrary code with system privilege. User interaction is required for triggering this vulnerability.	2024-07-02	6.8	CVE-2024-34587
samsung -- android	Improper input validation?in parsing RTCP SR packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability.	2024-07-02	6.5	CVE-2024-34588
samsung -- android	Improper input validation in parsing RTCP RR packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability.	2024-07-02	6.5	CVE-2024-34589
samsung -- android	Improper access control in Dar service prior to SMR Jul-2024 Release 1 allows local attackers to bypass restriction for calling SDP features.	2024-07-02	5.5	CVE-2024-20895

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
samsung -- android	Use of implicit intent for sensitive communication in Configuration message prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information.	2024-07-02	5.5	CVE-2024-20896
samsung -- android	Use of implicit intent for sensitive communication in FCM function in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information.	2024-07-02	5.5	CVE-2024-20897
samsung -- android	Use of implicit intent for sensitive communication in SoftphoneClient in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information.	2024-07-02	5.5	CVE-2024-20898
samsung -- android	Use of implicit intent for sensitive communication in RCS function in IMS service prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information.	2024-07-02	5.5	CVE-2024-20899
samsung -- android	Exposure of sensitive information in proc file system prior to SMR Jul-2024 Release 1 allows local attackers to read kernel memory address.	2024-07-02	5.5	CVE-2024-34594
samsung -- android	Improper authentication in BLE prior to SMR Jul-2024 Release 1 allows adjacent attackers to pair with devices.	2024-07-02	4.3	CVE-2024-20889
samsung -- android	Improper handling of exceptional conditions in Secure Folder prior to SMR Jul-2024 Release 1 allows physical attackers to bypass authentication under certain condition. User interaction is required for triggering this vulnerability.	2024-07-02	4.3	CVE-2024-20894
samsung -- android	Improper input validationí˜»in parsing an item type from RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability.	2024-07-02	4.3	CVE-2024-34590
samsung -- android	Improper input validation in parsing an item data from RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability.	2024-07-02	4.3	CVE-2024-34591
samsung -- android	Improper input validation in parsing RTCP SDES packet in librtp.so prior to SMR Jul-2024 Release 1 allows remote attackers to trigger temporary denial of service. User interaction is required for triggering this vulnerability.	2024-07-02	4.3	CVE-2024-34592
samsung -- galaxystore	Improper verification of intent by broadcast receiver vulnerability in GalaxyStore prior to version 4.5.81.0 allows local attackers to launch unexported activities of GalaxyStore.	2024-07-02	5.3	CVE-2024-34601
shaonsina--Sina Extension for Elementor (Slider, Gallery, Form, Modal, Data Table, Tab, Particle, Free Elementor Widgets & Elementor Templates)	The Sina Extension for Elementor (Slider, Gallery, Form, Modal, Data Table, Tab, Particle, Free Elementor Widgets & Elementor Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'read_more_text' parameter in all versions up to, and including, 3.5.5 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.	2024-07-02	6.4	CVE-2024-5260
SourceCodester--Medicine Tracker System	A vulnerability classified as critical was found in SourceCodester Medicine Tracker System 1.0. This vulnerability affects unknown code of the file /classes/Master.php?f=save_medicine. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-270010 is the identifier assigned to this vulnerability.	2024-07-01	6.3	CVE-2024-6419
SourceCodester--Online Tours & Travels	A vulnerability classified as critical has been found in SourceCodester Online Tours & Travels Management 1.0. This affects an unknown part of the file sms_setting.php. The manipulation of the argument uname leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the	2024-07-03	6.3	CVE-2024-6471

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management	public and may be used. The associated identifier of this vulnerability is VDB-270279.			
spider-themes -- eazydocs	The EazyDocs WordPress plugin before 2.5.0 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)	2024-07-02	4.8	CVE-2024-3999
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, an authenticated user could run risky commands using the permissions of a higher-privileged user to bypass SPL safeguards for risky commands in the Analytics Workspace. The vulnerability requires the authenticated user to phish the victim by tricking them into initiating a request within their browser. The authenticated user should not be able to exploit the vulnerability at will.	2024-07-01	6.3	CVE-2024-36986
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.2.2403.100, an authenticated, low-privileged user that does not hold the admin or power Splunk roles could send a specially crafted HTTP POST request to the datamodel/web REST endpoint in Splunk Enterprise, potentially causing a denial of service.	2024-07-01	6.5	CVE-2024-36990
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, a low-privileged user that does not hold the admin or power Splunk roles could craft a malicious payload through a View that could result in execution of unauthorized JavaScript code in the browser of a user. The "url" parameter of the Dashboard element does not have proper input validation to reject invalid URLs, which could lead to a Persistent Cross-site Scripting (XSS) exploit.	2024-07-01	5.4	CVE-2024-36992
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, a low-privileged user that does not hold the admin or power Splunk roles could craft a malicious payload through a Splunk Web Bulletin Messages that could result in execution of unauthorized JavaScript code in the browser of a user.	2024-07-01	5.4	CVE-2024-36993
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, a low-privileged user that does not hold the admin or power Splunk roles could craft a malicious payload through a View and Splunk Web Bulletin Messages that could result in execution of unauthorized JavaScript code in the browser of a user.	2024-07-01	5.4	CVE-2024-36994
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200 and 9.1.2308.207, a low-privileged user that does not hold the admin or power Splunk roles could create experimental items.	2024-07-01	5.4	CVE-2024-36995
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.109, an attacker could determine whether or not another user exists on the instance by deciphering the error response that they would likely receive from the instance when they attempt to log in. This disclosure could then lead to additional brute-force password-guessing attacks. This vulnerability would require that the Splunk platform instance uses the Security Assertion Markup Language (SAML) authentication scheme.	2024-07-01	5.3	CVE-2024-36996
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 9.2.2, 9.1.5, and 9.0.10 and Splunk Cloud Platform versions below 9.1.2312.200, an authenticated, low-privileged user who does not hold the admin or power Splunk roles could upload a file with an arbitrary extension using the indexing/preview REST endpoint.	2024-07-01	4.3	CVE-2024-36987
StaxWP--Elementor Addons, Widgets and	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in StaxWP Elementor Addons, Widgets and Enhancements -	2024-07-06	6.5	CVE-2024-37541

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Enhancements Stax	Stax allows Stored XSS.This issue affects Elementor Addons, Widgets and Enhancements - Stax: from n/a through 1.4.4.1.			
stylemixthemes -- cost_calculator_builder	The Cost Calculator Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'textarea.description' parameter in all versions up to, and including, 3.2.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-02	4.8	CVE-2024-6011
stylemixthemes -- cost_calculator_builder	The Cost Calculator Builder plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'embed-create-page' and 'embed-insert-pages' functions in all versions up to, and including, 3.2.12. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create arbitrary posts and append arbitrary content to existing posts.	2024-07-02	4.3	CVE-2024-6012
stylemixthemes -- motors_-_car_dealer\,_classifieds_\&_listing	The Motors - Car Dealer, Classifieds & Listing plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the stm_edit_delete_user_car function in all versions up to, and including, 1.4.8. This makes it possible for unauthenticated attackers to unpublish arbitrary posts and pages.	2024-07-02	5.3	CVE-2024-5545
supsystic -- easy_google_maps	The Easy Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's file upload feature in all versions up to, and including, 1.11.15 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-02	5.4	CVE-2024-5219
syedbalkhi -- wp_lightbox_2	The WP Lightbox 2 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' parameter in all versions up to, and including, 3.0.6.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-03	5.4	CVE-2024-6263
thimpress -- learnpress	The LearnPress - WordPress LMS Plugin plugin for WordPress is vulnerable to unauthorized user registration due to a missing capability check on the 'register' function in all versions up to, and including, 4.2.6.8.1. This makes it possible for unauthenticated attackers to bypass disabled user registration to create a new account with the default role.	2024-07-02	5.3	CVE-2024-6088
thimpress -- learnpress	The LearnPress - WordPress LMS Plugin plugin for WordPress is vulnerable to unauthenticated bypass to user registration in versions up to, and including, 4.2.6.8.1. This is due to missing checks in the 'check_validate_fields' function in the checkout. This makes it possible for unauthenticated attackers to register as the default role on the site, even if registration is disabled.	2024-07-02	5.3	CVE-2024-6099
Unisoc (Shanghai) Technologies Co., Ltd.-- SC7731E/SC9832E/SC9863A/T310/T606/T612/T616/T610/T618	In faceid servive, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2024-07-01	5.1	CVE-2024-39429
Unisoc (Shanghai) Technologies Co., Ltd.-- SC7731E/SC9832E/	In faceid servive, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2024-07-01	5.1	CVE-2024-39430

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SC9863A/T310/T606/T612/T616/T610/T618				
Unisoc (Shanghai) Technologies Co., Ltd.--SC7731E/SC9832E/SC9863A/T310/T606/T612/T616/T610/T618/T760/T770/T820/S8000	In trusty service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2024-07-01	6.8	CVE-2024-39428
Unisoc (Shanghai) Technologies Co., Ltd.--SC7731E/SC9832E/SC9863A/T310/T606/T612/T616/T610/T618/T760/T770/T820/S8000	In trusty service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2024-07-01	5.1	CVE-2024-39427
voidcoders --void_contact_form_7_widget_for_elementor_page_builder	The Void Contact Form 7 Widget For Elementor Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cf7_redirect_page' attribute within the plugin's Void Contact From 7 widget in all versions up to, and including, 2.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-02	5.4	CVE-2024-5419
WeblateOrg--weblate	Weblate is a web based localization tool. Prior to version 5.6.2, Weblate didn't correctly validate filenames when restoring project backup. It may be possible to gain unauthorized access to files on the server using a crafted ZIP file. This issue has been addressed in Weblate 5.6.2. As a workaround, do not allow untrusted users to create projects.	2024-07-01	4.4	CVE-2024-39303
WpDevArt--Responsive Image Gallery, Gallery Album	Missing Authorization vulnerability in WpDevArt Responsive Image Gallery, Gallery Album.This issue affects Responsive Image Gallery, Gallery Album: from n/a through 2.0.3.	2024-07-06	5.4	CVE-2024-37542
wpexpertplugins --post_meta_data_manager	The Post Meta Data Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '$meta_key' parameter in all versions up to, and including, 1.2.3 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.	2024-07-02	5.4	CVE-2024-6264
XjSv--Basil	The Basil recipe theme for WordPress is vulnerable to Persistent Cross-Site Scripting (XSS) via the `post_title` parameter in versions up to, and including, 2.0.4 due to insufficient input sanitization and output escaping. This vulnerability allows authenticated attackers with contributor-level access and above to inject arbitrary web scripts in pages that will execute whenever a user accesses a compromised page. Because the of the default WordPress validation, it is not possible to insert the payload directly but if the Cooked plugin is installed, it is possible to create a recipe post type (cp_recipe) and inject the payload in the title field. Version 2.0.5 contains a patch for the issue.	2024-07-01	5.4	CVE-2024-39310

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
yeken -- snippet_shortcodes	The Snippet Shortcodes plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.1.4. This is due to missing or incorrect nonce validation when adding or editing shortcodes. This makes it possible for unauthenticated attackers to modify shortcodes via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-07-03	4.3	CVE-2024-4543
zephyrproject-rtos--Zephyr	A malicious BLE device can send a specific order of packet sequence to cause a DoS attack on the victim BLE device	2024-07-03	6.5	CVE-2024-3332
zitadel--zitadel	ZITADEL is an open-source identity infrastructure tool. ZITADEL provides users the ability to list all user sessions of the current user agent (browser). Starting in version 2.53.0 and prior to versions 2.53.8, 2.54.5, and 2.55.1, due to a missing check, user sessions without that information (e.g. when created though the session service) were incorrectly listed exposing potentially other user's sessions. Versions 2.55.1, 2.54.5, and 2.53.8 contain a fix for the issue. There is no workaround since a patch is already available.	2024-07-03	5.7	CVE-2024-39683
1E--1E Platform	The 1E Platform's component utilized the third-party Duende Identity Server, which suffered from an open redirect vulnerability, permitting an attacker to control the redirection path of end users. Note: 1E Platform's component utilizing the third-party Duende Identity Server has been updated with the patch that includes the fix.	2024-08-01	4.7	CVE-2024-7211
5 Star Plugins--Pretty Simple Popup Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in 5 Star Plugins Pretty Simple Popup Builder allows Stored XSS.This issue affects Pretty Simple Popup Builder: from n/a through 1.0.7.	2024-08-01	5.9	CVE-2024-39626
AccuPOS--AccuPOS	AccuPOS - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	2024-07-30	5.3	CVE-2024-41701
Adobe--Acrobat for Edge	Acrobat for Edge versions 126.0.2592.81 and earlier are affected by an out-of-bounds read vulnerability that could lead to arbitrary file system read access. An attacker could exploit this vulnerability to read contents from a location in memory past the buffer boundary, potentially leading to sensitive information disclosure. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-07-31	5.5	CVE-2024-39379
Adobe--InDesign Desktop	InDesign Desktop versions ID18.5.2, ID19.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-02	5.5	CVE-2024-39396
advancedcoding--Comments wpDiscuz	The Comments - wpDiscuz plugin for WordPress is vulnerable to HTML Injection in all versions up to, and including, 7.6.21. This is due to a lack of filtering of HTML tags in comments. This makes it possible for unauthenticated attackers to add HTML such as hyperlinks to comments when rich editing is disabled.	2024-08-02	5.3	CVE-2024-6704
Ai3--QbiBot	Ai3 QbiBot does not properly filter user input, allowing unauthenticated remote attackers to insert JavaScript code into the chat box. Once the recipient views the message, they will be subject to a Stored XSS attack.	2024-08-02	6.1	CVE-2024-7204

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Akana--Akana API Platform	In versions of Akana API Platform prior to 2024.1.0 a flaw resulting in XML External Entity (XXE) was discovered.	2024-07-30	6.3	CVE-2024-3930
Akana--Akana API Platform	In versions of Akana API Platform prior to 2024.1.0, SAML tokens can be replayed.	2024-07-30	5.4	CVE-2024-5249
AkshuDev--PheonixAppAPI	Pheonix App is a Python application designed to streamline various tasks, from managing files to playing mini-games. The issue is that the map of encoding/decoding languages are visible in code. The Problem was patched in 0.2.4.	2024-07-31	4.4	CVE-2024-41951
Apple--iOS and iPadOS	The issue was addressed with improved memory handling. This issue is fixed in iOS 17 and iPadOS 17, macOS Sonoma 14, watchOS 10, tvOS 17. An app may be able to execute arbitrary code with kernel privileges.	2024-07-29	6.6	CVE-2023-40396
Apple--macOS	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.6. An app with root privileges may be able to execute arbitrary code with kernel privileges.	2024-07-29	6.5	CVE-2024-27878
Apple--macOS	A logic issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.6. Enabling Lockdown Mode while setting up a Mac may cause FileVault to become unexpectedly disabled.	2024-07-29	5.3	CVE-2024-27862
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 'end_redirect_link' parameter in versions up to, and including, 5.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-02	6.4	CVE-2024-4643
BdThemes--Element Pack Elementor Addons	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BdThemes Element Pack Elementor Addons allows Stored XSS.This issue affects Element Pack Elementor Addons: from n/a through 5.6.11.	2024-08-01	6.5	CVE-2024-39667
BDThemes--Element Pack Pro - Addon for Elementor Page Builder WordPress Plugin	The Element Pack - Addon for Elementor Page Builder WordPress Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the widget wrapper link URL in all versions up to, and including, 7.9.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-01	6.4	CVE-2024-2455
boldthemes--Bold Page Builder	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's bt_bb_button shortcode in all versions up to, and including, 5.0.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-30	6.4	CVE-2024-7100

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Brainstorm Force--Spectra Pro	The Spectra Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via block ids in all versions up to, and including, 1.1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-02	6.4	CVE-2024-3827
Breakdance--Breakdance	The Breakdance plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the breakdance_css_file_paths_cache parameter in all versions up to, and including, 1.7.2 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.	2024-08-01	6.4	CVE-2024-5330
Breakdance--Breakdance	The Breakdance plugin for WordPress is vulnerable to unauthorized access of data in all versions up to, and including, 1.7.2. This makes it possible for authenticated attackers, with Contributor-level access and above, to export form submissions.	2024-08-01	4.3	CVE-2024-5331
Cato Networks--SDP Client	A vulnerability in Cato Networks SDP Client on Windows allows the insertion of sensitive information into the log file, which can lead to an account takeover. However, the attack requires bypassing protections on modifying the tunnel token on a the attacker's system.This issue affects SDP Client: before 5.10.34.	2024-07-31	6.5	CVE-2024-6977
Cato Networks--SDP Client	Cato Networks Windows SDP Client Local root certificates can be installed by low-privileged users.This issue affects SDP Client: before 5.10.28.	2024-07-31	5.6	CVE-2024-6978
CHANGING Information Technology--HWATAIServiSign Windows Version	The specific API in HWATAIServiSign Windows Version from CHANGING Information Technology does not properly validate the length of server-side inputs. When a user visits a spoofed website, unauthenticated remote attackers can cause a stack-based buffer overflow in the HWATAIServiSign, temporarily disrupting its service.	2024-08-02	4.3	CVE-2024-40723
CHANGING Information Technology--TCBServiSign Windows Version	The encryption strength of the authorization keys in CHANGING Information Technology TCBServiSign Windows Version is insufficient. When a remote attacker tricks a victim into visiting a malicious website, TCBServiSign will treat that website as a legitimate server and interact with it.	2024-08-02	6.5	CVE-2024-40719
CHANGING Information Technology--TCBServiSign Windows Version	The specific API in TCBServiSign Windows Version from CHANGING Information Technology does does not properly validate the length of server-side input. When a user visits a spoofed website, unauthenticated remote attackers can cause a stack-based buffer overflow in the TCBServiSign, temporarily disrupting its service.	2024-08-02	4.3	CVE-2024-40722
codename065--Download Manager	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpdm_all_packages' shortcode in all versions up to, and including, 3.2.97 due to insufficient input sanitization and output escaping on the 'cols' parameter. 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.	2024-07-31	6.4	CVE-2024-6208
Crocoblock--JetWidgets for Elementor and WooCommerce	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Crocoblock JetWidgets for Elementor and WooCommerce allows PHP Local File Inclusion.This issue affects JetWidgets for Elementor and WooCommerce: from n/a through 1.1.7.	2024-08-01	6.5	CVE-2024-38772

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cybonet--PineApp Mail Relay	Cybonet - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	2024-07-30	5.3	CVE-2024-41694
D-Link--DI-8100	A vulnerability, which was classified as critical, has been found in D-Link DI-8100 16.07. This issue affects the function msp_info_htm of the file msp_info.htm. The manipulation of the argument cmd leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273521 was assigned to this vulnerability.	2024-08-03	6.3	CVE-2024-7436
Dahua--NVR4XXX	A vulnerability has been found in Dahua products.After obtaining the administrator's username and password, the attacker can send a carefully crafted data packet to the interface with vulnerabilities, causing device initialization.	2024-07-31	6	CVE-2024-39946
Dahua--NVR4XXX	A vulnerability has been found in Dahua products.After obtaining the ordinary user's username and password, the attacker can send a carefully crafted data packet to the interface with vulnerabilities, causing the device to crash.	2024-07-31	6.5	CVE-2024-39947
Dahua--NVR4XXX	A vulnerability has been found in Dahua products. After obtaining the administrator's username and password, the attacker can send a carefully crafted data packet to the interface with vulnerabilities, causing the device to crash.	2024-07-31	4.9	CVE-2024-39945
Dell -- iDRAC Service Module	Dell iDRAC Service Module version 5.3.0.0 and prior, contain an Out of bound Read Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event.	2024-08-01	4.4	CVE-2024-25947
Dell -- iDRAC Service Module	Dell iDRAC Service Module version 5.3.0.0 and prior, contain a Out of bound Write Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event.	2024-08-01	4.4	CVE-2024-25948
Dell--CloudLink	CloudLink, versions 7.1.x and 8.x, contain an Improper check or handling of Exceptional Conditions Vulnerability in Cluster Component. A highly privileged malicious user with remote access could potentially exploit this vulnerability, leading to execute unauthorized actions and retrieve sensitive information from the database.	2024-08-02	6.6	CVE-2024-38482
Dell--Dell BSAFE Micro Edition Suite	Dell BSAFE Crypto-C Micro Edition 4.1.5 and Dell BSAFE Micro Edition Suite, versions 4.0 through 4.6.1 and version 5.0 contain a buffer over-read vulnerability.	2024-07-31	6.2	CVE-2023-28074
Dell--Dell Inventory Collector	Dell Inventory Collector, versions prior to 12.3.0.6 contains a Path Traversal vulnerability. A local authenticated malicious user could potentially exploit this vulnerability, leading to arbitrary code execution on the system.	2024-07-31	6.7	CVE-2024-37129
Dell--iDRAC Service Module	Dell iDRAC Service Module version 5.3.0.0 and prior, contain a Out of bound Read Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event.	2024-08-01	4.4	CVE-2024-38481
Dell--iDRAC Service Module	Dell iDRAC Service Module version 5.3.0.0 and prior contains Out of bound write Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service (partial) event.	2024-08-01	4.4	CVE-2024-38489
Dell--iDRAC Service Module	Dell iDRAC Service Module version 5.3.0.0 and prior, contain a Out of bound Write Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event.	2024-08-01	4.4	CVE-2024-38490

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dell--InsightIQ	Dell InsightIQ, Verion 5.0.0, contains a use of a broken or risky cryptographic algorithm vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to information disclosure.	2024-08-01	5.9	CVE-2024-28972
Delphix--Data Control Tower (DCT)	A flaw in versions of Delphix Data Control Tower (DCT) prior to 19.0.0 results in broken authentication through the enable-scale-testing functionality of the application.	2024-07-29	5.4	CVE-2024-6727
Digiwin--EasyFlow .NET	Digiwin EasyFlow .NET lacks proper access control for specific functionality, and the functionality do not adequately filter user input. A remote attacker with regular privilege can exploit this vulnerability to download arbitrary files from the remote server .	2024-08-02	6.5	CVE-2024-7323
discourse--discourse	Discourse is an open source discussion platform. Prior to 3.2.3 and 3.3.0.beta3, improperly sanitized Onebox data could lead to an XSS vulnerability in some situations. This vulnerability only affects Discourse instances which have disabled the default Content Security Policy. This vulnerability is fixed in 3.2.3 and 3.3.0.beta3.	2024-07-30	6.3	CVE-2024-37165
discourse--discourse	Discourse is an open source discussion platform. Prior to 3.2.5 and 3.3.0.beta5, the vulnerability allows an attacker to inject iframes from any domain, bypassing the intended restrictions enforced by the allowed_iframes setting. This vulnerability is fixed in 3.2.5 and 3.3.0.beta5.	2024-07-30	6.1	CVE-2024-39320
discourse--discourse	Discourse is an open source discussion platform. Prior to 3.2.5 and 3.3.0.beta5, crafting requests to submit very long tag group names can reduce the availability of a Discourse instance. This vulnerability is fixed in 3.2.5 and 3.3.0.beta5.	2024-07-30	4.9	CVE-2024-37299
doublesharp--Remote Content Shortcode	The Remote Content Shortcode plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.5 via the remote_content shortcode. This makes it possible for authenticated attackers, with contributor-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	2024-08-01	6.4	CVE-2024-2090
DuendeSoftware--IdentityServer	Duende IdentityServer is an OpenID Connect and OAuth 2.x framework for ASP.NET Core. It is possible for an attacker to craft malicious Urls that certain functions in IdentityServer will incorrectly treat as local and trusted. If such a Url is returned as a redirect, some browsers will follow it to a third-party, untrusted site. Note: by itself, this vulnerability does **not** allow an attacker to obtain user credentials, authorization codes, access tokens, refresh tokens, or identity tokens. An attacker could however exploit this vulnerability as part of a phishing attack designed to steal user credentials. This vulnerability is fixed in 7.0.6, 6.3.10, 6.2.5, 6.1.8, and 6.0.5. Duende.IdentityServer 5.1 and earlier and all versions of IdentityServer4 are no longer supported and will not be receiving updates. If upgrading is not possible, use `IUrlHelper.IsLocalUrl` from ASP.NET Core to validate return Urls in user interface code in the IdentityServer host.	2024-07-31	4.7	CVE-2024-39694
dylanjkotze--Zephyr Project Manager	The Zephyr Project Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'filename' parameter in all versions up to, and including, 3.3.100 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-03	6.4	CVE-2024-7356

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Elastic--APM Server	APM server logs contain document body from a partially failed bulk index request. For example, in case of unavailable_shards_exception for a specific document, since the ES response line contains the document body, and that APM server logs the ES response line on error, the document is effectively logged.	2024-08-03	5.7	CVE-2024-37286 bressers@elastic.co
Elastic--Elasticsearch	It was discovered by Elastic engineering that when elasticsearch-certutil CLI tool is used with the csr option in order to create a new Certificate Signing Requests, the associated private key that is generated is stored on disk unencrypted even if the --pass parameter is passed in the command invocation.	2024-07-31	4.9	CVE-2024-23444 bressers@elastic.co
Elastic--Kibana	An issue was discovered in Kibana where a user with Viewer role could cause a Kibana instance to crash by sending a large number of maliciously crafted requests to a specific endpoint.	2024-07-30	6.5	CVE-2024-37281 bressers@elastic.co
ELECOM CO.,LTD.--WRC-2533GS2V-B	Unrestricted upload of file with dangerous type vulnerability exists in ELECOM wireless LAN routers. A specially crafted file may be uploaded to the affected product by a logged-in user with an administrative privilege, resulting in an arbitrary OS command execution.	2024-08-01	6.8	CVE-2024-34021
ELECOM CO.,LTD.--WRC-X6000XS-G	OS command injection vulnerability exists in ELECOM wireless LAN routers. A specially crafted request may be sent to the affected product by a logged-in user with an administrative privilege to execute an arbitrary OS command.	2024-08-01	6.8	CVE-2024-39607
ExtendThemes--Kubio AI Page Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ExtendThemes Kubio AI Page Builder.This issue affects Kubio AI Page Builder: from n/a through 2.2.4.	2024-08-01	6.5	CVE-2024-39661
FFRI Security, Inc.--FFRI AMC	FFRI AMC versions 3.4.0 to 3.5.3 and some OEM products that implement/bundle FFRI AMC versions 3.4.0 to 3.5.3 allow a remote unauthenticated attacker to execute arbitrary OS commands when certain conditions are met in an environment where the notification program setting is enabled and the executable file path is set to a batch file (.bat) or command file (.cmd) extension.	2024-07-30	6.4	CVE-2024-40895
FOGProject--fogproject	FOG is a cloning/imaging/rescue suite/inventory management system. The application stores plaintext service account credentials in the "/opt/fog/.fogsettings" file. This file is by default readable by all users on the host. By exploiting these credentials, a malicious user could create new accounts for the web application and much more. The vulnerability is fixed in 1.5.10.41.	2024-07-31	5.3	CVE-2024-41954
FOGProject--fogproject	FOG is a cloning/imaging/rescue suite/inventory management system. FOG Server 1.5.10.41.4 and earlier can leak authorized and rejected logins via logs stored directly on the root of the web server. FOG Server creates 2 logs on the root of the web server (fog_login_accepted.log and fog_login_failed.log), exposing the name of the user account used to manage FOG, the IP address of the computer used to login and the User-Agent. This vulnerability is fixed in 1.5.10.47.	2024-08-02	5.3	CVE-2024-42349
gpriday--SiteOrigin Widgets Bundle	The SiteOrigin Widgets Bundle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Image Grid widget in all versions up to, and including, 1.62.2 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.	2024-07-30	6.4	CVE-2024-5901
harbor--harbor	Incorrect user permission validation in Harbor <v2.9.5 and Harbor <v2.10.3 allows authenticated users to modify configurations.	2024-08-02	5.4	CVE-2024-22278

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Hewlett Packard Enterprise (HPE)--ClearPass Policy Manager (CPPM)	A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further access to network services supported by ClearPass Policy Manager.	2024-07-30	6.8	CVE-2024-41916
Hewlett Packard Enterprise (HPE)--ClearPass Policy Manager (CPPM)	A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further access to network services supported by ClearPass Policy Manager	2024-07-30	5.8	CVE-2024-5486
ibexa--admin-ui	The Ibexa Admin UI Bundle contains all the necessary parts to run the Ibexa DXP Back Office interface. The file upload widget is vulnerable to XSS payloads in filenames. Access permission to upload files is required. As such, in most cases only authenticated editors and administrators will have the required permission. It is not persistent, i.e. the payload is only executed during the upload. In effect, an attacker will have to trick an editor/administrator into uploading a strangely named file.	2024-07-31	5.4	CVE-2024-39318
IBM--Aspera Orchestrator	IBM Aspera Orchestrator 4.0.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 260206.	2024-07-30	6.5	CVE-2023-38001
IBM--Aspera Orchestrator	IBM Aspera Orchestrator 4.0.1 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: 248477.	2024-07-30	5.5	CVE-2023-26288
IBM--Aspera Orchestrator	IBM Aspera Orchestrator 4.0.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 248478.	2024-07-30	5.4	CVE-2023-26289
IBM--Business Automation Workflow	IBM Business Automation Workflow 22.0.2, 23.0.1, 23.0.2, and 24.0.0 stores potentially sensitive information in log files under certain situations that could be read by an authenticated user. IBM X-Force ID: 284868.	2024-08-03	5.3	CVE-2024-38321
Imagely--NextGEN Gallery	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Imagely NextGEN Gallery allows Stored XSS.This issue affects NextGEN Gallery: from n/a through 3.59.3.	2024-08-01	5.9	CVE-2024-39627
itsourcecode--Alton Management System	A vulnerability classified as critical was found in itsourcecode Alton Management System 1.0. This vulnerability affects unknown code of the file search.php. The manipulation of the argument rcode leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273142 is the identifier assigned to this vulnerability.	2024-07-30	6.3	CVE-2024-7273
itsourcecode--Alton Management System	A vulnerability, which was classified as critical, has been found in itsourcecode Alton Management System 1.0. This issue affects some unknown processing of the file /reservation_status.php. The manipulation of the argument rcode leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273143.	2024-07-30	4.7	CVE-2024-7274
itsourcecode--Alton Management	A vulnerability, which was classified as critical, was found in itsourcecode Alton Management System 1.0. Affected is an unknown function of the file /admin/category_save.php. The manipulation of the argument category leads to sql injection. It is possible to launch the attack remotely. The exploit has been	2024-07-30	4.7	CVE-2024-7275

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
System	disclosed to the public and may be used. The identifier of this vulnerability is VDB-273144.			
itsourcecode--Alton Management System	A vulnerability has been found in itsourcecode Alton Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/member_save.php. The manipulation of the argument last/first leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273145 was assigned to this vulnerability.	2024-07-30	4.7	CVE-2024-7276
itsourcecode--Alton Management System	A vulnerability was found in itsourcecode Alton Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/menu.php of the component Add a Menu. The manipulation of the argument image leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-273146 is the identifier assigned to this vulnerability.	2024-07-31	4.7	CVE-2024-7277
itsourcecode--Alton Management System	A vulnerability was found in itsourcecode Alton Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/team_save.php. The manipulation of the argument team leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273147.	2024-07-31	4.7	CVE-2024-7278
itsourcecode--Online Blood Bank Management System	A vulnerability classified as problematic was found in itsourcecode Online Blood Bank Management System 1.0. This vulnerability affects unknown code of the file signup.php of the component User Registration Handler. The manipulation of the argument user leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273232.	2024-07-31	4.3	CVE-2024-7321
itsourcecode--Online Food Ordering System	A vulnerability classified as critical has been found in itsourcecode Online Food Ordering System 1.0. Affected is an unknown function of the file editproduct.php. The manipulation of the argument photo leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-272610 is the identifier assigned to this vulnerability.	2024-07-29	6.3	CVE-2024-7189
itsourcecode--Society Management System	A vulnerability classified as critical was found in itsourcecode Society Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/get_price.php. The manipulation of the argument expenses_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272611.	2024-07-29	6.3	CVE-2024-7190
itsourcecode--Society Management System	A vulnerability, which was classified as critical, has been found in itsourcecode Society Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/get_balance.php. The manipulation of the argument student_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272612.	2024-07-29	6.3	CVE-2024-7191
itsourcecode--Society Management System	A vulnerability, which was classified as critical, was found in itsourcecode Society Management System 1.0. This affects an unknown part of the file /admin/student.php. The manipulation of the argument 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. The identifier VDB-272613 was assigned to this vulnerability.	2024-07-29	6.3	CVE-2024-7192
itsourcecode--Society Management	A vulnerability was found in itsourcecode Society Management System 1.0 and classified as critical. This issue affects some unknown processing of the file check_student.php. The manipulation of the argument student_id leads to sql	2024-07-29	6.3	CVE-2024-7194

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
System	injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272615.			
itsourcecode--Society Management System	A vulnerability was found in itsourcecode Society Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/check_admin.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. The identifier of this vulnerability is VDB-272616.	2024-07-29	6.3	CVE-2024-7195
itsourcecode--Ticket Reservation System	A vulnerability, which was classified as critical, has been found in itsourcecode Ticket Reservation System 1.0. Affected by this issue is some unknown functionality of the file checkout_ticket_save.php. The manipulation of the argument data leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-273530 is the identifier assigned to this vulnerability.	2024-08-03	4.7	CVE-2024-7445
itsourcecode--Ticket Reservation System	A vulnerability, which was classified as critical, was found in itsourcecode Ticket Reservation System 1.0. This affects an unknown part of the file list_tickets.php. The manipulation of the argument prefSeat_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273531.	2024-08-03	4.7	CVE-2024-7446
Johnson Controls--exacqVision	Under certain circumstances the ExacqVision Web Services does not provide sufficient protection from untrusted domains.	2024-08-01	6.8	CVE-2024-32862
Johnson Controls--exacqVision	Under certain circumstances the exacqVision Web Services may be susceptible to Cross-Site Request Forgery (CSRF)	2024-08-01	6.8	CVE-2024-32863
Johnson Controls--exacqVision	Under certain circumstances exacqVision Web Services will not enforce secure web communications (HTTPS)	2024-08-01	6.4	CVE-2024-32864
Johnson Controls--exacqVision	Under certain circumstances the exacqVision Server will not properly validate TLS certificates provided by connected devices.	2024-08-01	6.4	CVE-2024-32865
Johnson Controls--exacqVision	Under certain circumstances the exacqVision Web Service can expose authentication token details within communications.	2024-08-01	5.7	CVE-2024-32931
Jordy Meow--AI Engine: ChatGPT Chatbot	Server-Side Request Forgery (SSRF) vulnerability in Jordy Meow AI Engine: ChatGPT Chatbot allows Server Side Request Forgery.This issue affects AI Engine: ChatGPT Chatbot: from n/a through 2.4.7.	2024-08-01	4.9	CVE-2024-38791
Jordy Meow--Photo Engine	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jordy Meow Photo Engine allows Stored XSS.This issue affects Photo Engine: from n/a through 6.3.1.	2024-08-01	5.9	CVE-2024-39660
kp4coder--Sync Post With Other	The Sync Post With Other Site plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'sps_add_update_post' function in all versions up to, and including, 1.6. This makes	2024-08-03	4.3	CVE-2024-6709

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Site	it possible for authenticated attackers, with Subscriber-level access and above, to create new draft posts and update existing posts.			
Lenovo--PC Manager	A vulnerability was reported in Lenovo PC Manager versions prior to 2.6.40.3154 that could allow an attacker to cause a system reboot.	2024-07-31	5.5	CVE-2017-3772
leogermani--Tainacan	The Tainacan plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'get_file' function in all versions up to, and including, 0.21.7. The function is also vulnerable to directory traversal. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	2024-07-31	6.5	CVE-2024-7135
Lester GaMerZ Chan--WP-PostRatings	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Lester 'GaMerZ' Chan WP-PostRatings allows Stored XSS.This issue affects WP-PostRatings: from n/a through 1.91.1.	2024-08-01	6.5	CVE-2024-39659
limpinho--CTT Expresso para WooCommerce	The CTT Expresso para WooCommerce plugin for WordPress is vulnerable to sensitive information exposure in all versions up to and including 3.2.12 via the /wp-content/uploads/cepw directory. The generated .pdf and log files are publicly accessible and contain sensitive information such as sender and receiver names, phone numbers, physical addresses, and email addresses	2024-08-01	5.3	CVE-2024-6687
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nfsd: initialise nfsd_info.mutex early. nfsd_info.mutex can be dereferenced by svc_pool_stats_start() immediately after the new netns is created. Currently this can trigger an oops. Move the initialisation earlier before it can possibly be dereferenced.	2024-07-29	5.5	CVE-2024-42078
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix NULL pointer dereference in gfs2_log_flush In gfs2_jindex_free(), set sdp->sd_jdesc to NULL under the log flush lock to provide exclusion against gfs2_log_flush(). In gfs2_log_flush(), check if sdp->sd_jdesc is non-NULL before dereferencing it. Otherwise, we could run into a NULL pointer dereference when outstanding glock work races with an unmount (glock_work_func -> run_queue -> do_xmote -> inode_go_sync -> gfs2_log_flush).	2024-07-29	5.5	CVE-2024-42079
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/restrack: Fix potential invalid address access struct rdma_restrack_entry's kern_name was set to KBUILD_MODNAME in ib_create_cq(), while if the module exited but forgot del this rdma_restrack_entry, it would cause a invalid address access in rdma_restrack_clean() when print the owner of this rdma_restrack_entry. These code is used to help find one forgotten PD release in one of the ULPs. But it is not needed anymore, so delete them.	2024-07-29	5.5	CVE-2024-42080
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/xe_devcoredump: Check NULL before assignments Assign 'xe_devcoredump_snapshot *' and 'xe_device *' only if 'coredump' is not NULL. v2 - Fix commit messages. v3 - Define variables before code.(Ashutosh/Jose) v4 - Drop return check for coredump_to_xe. (Jose/Rodrigo) v5 - Modify misleading commit message. (Matt)	2024-07-29	5.5	CVE-2024-42081
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xdp: Remove WARN() from __xdp_reg_mem_model() syzkaller reports a warning in __xdp_reg_mem_model(). The warning occurs only if __mem_id_init_hash_table() returns an error. It returns the error in two cases: 1. memory allocation fails; 2. rhashtable_init() fails when some fields of rhashtable_params struct are not initialized properly. The second case cannot happen since there is a static const rhashtable_params struct with valid fields. So, warning is only triggered when there is a problem with memory allocation. Thus, there is no sense in using WARN()	2024-07-29	5.5	CVE-2024-42082

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to handle this error and it can be safely removed. WARNING: CPU: 0 PID: 5065 at net/core/xdp.c:299 __xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 CPU: 0 PID: 5065 Comm: syz-executor883 Not tainted 6.8.0-syzkaller-05271-gf99c5f563c17 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:__xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 Call Trace: xdp_reg_mem_model+0x22/0x40 net/core/xdp.c:344 xdp_test_run_setup net/bpf/test_run.c:188 [inline] bpf_test_run_xdp_live+0x365/0x1e90 net/bpf/test_run.c:377 bpf_prog_test_run_xdp+0x813/0x11b0 net/bpf/test_run.c:1267 bpf_prog_test_run+0x33a/0x3b0 kernel/bpf/syscall.c:4240 __sys_bpf+0x48d/0x810 kernel/bpf/syscall.c:5649 __do_sys_bpf kernel/bpf/syscall.c:5738 [inline] __se_sys_bpf kernel/bpf/syscall.c:5736 [inline] __x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:5736 do_syscall_64+0xfb/0x240 entry_SYSCALL_64_after_hwframe+0x6d/0x75 Found by Linux Verification Center (linuxtesting.org) with syzkaller.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ionic: fix kernel panic due to multi-buffer handling Currently, the ionic_run_xdp() doesn't handle multi-buffer packets properly for XDP_TX and XDP_REDIRECT. When a jumbo frame is received, the ionic_run_xdp() first makes xdp frame with all necessary pages in the rx descriptor. And if the action is either XDP_TX or XDP_REDIRECT, it should unmap dma-mapping and reset page pointer to NULL for all pages, not only the first page. But it doesn't for SG pages. So, SG pages unexpectedly will be reused. It eventually causes kernel panic. Oops: general protection fault, probably for non-canonical address 0x504f4e4dbebc64ff: 0000 [#1] PREEMPT SMP NOPTI CPU: 3 PID: 0 Comm: swapper/3 Not tainted 6.10.0-rc3+ #25 RIP: 0010:xdp_return_frame+0x42/0x90 Code: 01 75 12 5b 4c 89 e6 5d 31 c9 41 5c 31 d2 41 5d e9 73 fd ff ff 44 8b 6b 20 0f b7 43 0a 49 81 ed 68 01 00 00 49 29 c5 49 01 fd <41> 80 7d0 RSP: 0018:ffff99d00122ce08 EFLAGS: 00010202 RAX: 0000000000005453 RBX: ffff8d325f904000 RCX: 0000000000000001 RDX: 00000000670e1000 RSI: 000000011f90d000 RDI: 504f4e4d4c4b4a49 RBP: ffff99d003907740 R08: 0000000000000000 R09: 0000000000000000 R10: 000000011f90d000 R11: 0000000000000000 R12: ffff8d325f904010 R13: 504f4e4dbebc64fd R14: ffff8d3242b070c8 R15: ffff99d0039077c0 FS: 0000000000000000(0000) GS:ffff8d399f780000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f41f6c85e38 CR3: 000000037ac30000 CR4: 00000000007506f0 PKRU: 55555554 Call Trace: <IRQ> ? die_addr+0x33/0x90 ? exc_general_protection+0x251/0x2f0 ? asm_exc_general_protection+0x22/0x30 ? xdp_return_frame+0x42/0x90 ionic_tx_clean+0x211/0x280 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] ionic_tx_cq_service+0xd3/0x210 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] ionic_txrx_napi+0x41/0x1b0 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] __napi_poll.constprop.0+0x29/0x1b0 net_rx_action+0x2c4/0x350 handle_softirqs+0xf4/0x320 irq_exit_rcu+0x78/0xa0 common_interrupt+0x77/0x90	2024-07-29	5.5	CVE-2024-42083
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: tda10048: Fix integer overflow state->xtal_hz can be up to 16M, so it can overflow a 32 bit integer when multiplied by pll_mfactor. Create a new 64 bit variable to hold the calculations.	2024-07-30	5.5	CVE-2024-42223

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: fix calc_available_free_space() for zoned mode calc_available_free_space() returns the total size of metadata (or system) block groups, which can be allocated from unallocated disk space. The logic is wrong on zoned mode in two places. First, the calculation of data_chunk_size is wrong. We always allocate one zone as one chunk, and no partial allocation of a zone. So, we should use zone_size (= data_sinfo->chunk_size) as it is. Second, the result "avail" may not be zone aligned. Since we always allocate one zone as one chunk on zoned mode, returning non-zone size aligned bytes will result in less pressure on the async metadata reclaim process. This is serious for the nearly full state with a large zone size device. Allowing over-commit too much will result in less async reclaim work and end up in ENOSPC. We can align down to the zone size to avoid that.	2024-07-30	5.5	CVE-2024-42231
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Skip pipe if the pipe idx not set properly [why] Driver crashes when pipe idx not set properly [how] Add code to skip the pipe that idx not set properly	2024-07-29	5.5	CVE-2024-42064
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Add a NULL check in xe_ttm_stolen_mgr_init Add an explicit check to ensure that the mgr is not NULL.	2024-07-29	5.5	CVE-2024-42065
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix potential integer overflow in page size calculation Explicitly cast tbo->page_alignment to u64 before bit-shifting to prevent overflow when assigning to min_page_size.	2024-07-29	5.5	CVE-2024-42066
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_rox() into account with bpf_jit_binary_lock_ro() set_memory_rox() can fail, leaving memory unprotected. Check return and bail out when bpf_jit_binary_lock_ro() returns an error.	2024-07-29	5.5	CVE-2024-42067
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_ro() into account with bpf_prog_lock_ro() set_memory_ro() can fail, leaving memory unprotected. Check its return and take it into account as an error.	2024-07-29	5.5	CVE-2024-42068
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: mana: Fix possible double free in error handling path When auxiliary_device_add() returns error and then calls auxiliary_device_uninit(), callback function adev_release calls kfree(madev). We shouldn't call kfree(madev) again in the error handling path. Set 'madev' to NULL.	2024-07-29	5.5	CVE-2024-42069
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fully validate NFT_DATA_VALUE on store to data registers register store validation for NFT_DATA_VALUE is conditional, however, the datatype is always either NFT_DATA_VALUE or NFT_DATA_VERDICT. This only requires a new helper function to infer the register type from the set datatype so this conditional check can be removed. Otherwise, pointer to chain object can be leaked through the registers.	2024-07-29	5.5	CVE-2024-42070

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ionic: use dev_consume_skb_any outside of napi If we're not in a NAPI softirq context, we need to be careful about how we call napi_consume_skb(), specifically we need to call it with budget==0 to signal to it that we're not in a safe context. This was found while running some configuration stress testing of traffic and a change queue config loop running, and this curious note popped out: [4371.402645] BUG: using smp_processor_id() in preemptible [00000000] code: ethtool/20545 [4371.402897] caller is napi_skb_cache_put+0x16/0x80 [4371.403120] CPU: 25 PID: 20545 Comm: ethtool Kdump: loaded Tainted: G OE 6.10.0-rc3-netnext+ #8 [4371.403302] Hardware name: HPE ProLiant DL360 Gen10/ProLiant DL360 Gen10, BIOS U32 01/23/2021 [4371.403460] Call Trace: [4371.403613] <TASK> [4371.403758] dump_stack_lvl+0x4f/0x70 [4371.403904] check_preemption_disabled+0xc1/0xe0 [4371.404051] napi_skb_cache_put+0x16/0x80 [4371.404199] ionic_tx_clean+0x18a/0x240 [ionic] [4371.404354] ionic_tx_cq_service+0xc4/0x200 [ionic] [4371.404505] ionic_tx_flush+0x15/0x70 [ionic] [4371.404653] ? ionic_lif_qcq_deinit.isra.23+0x5b/0x70 [ionic] [4371.404805] ionic_txrx_deinit+0x71/0x190 [ionic] [4371.404956] ionic_reconfigure_queues+0x5f5/0xff0 [ionic] [4371.405111] ionic_set_ringparam+0x2e8/0x3e0 [ionic] [4371.405265] ethnl_set_rings+0x1f1/0x300 [4371.405418] ethnl_default_set_doit+0xbb/0x160 [4371.405571] genl_family_rcv_msg_doit+0xff/0x130 [...] I found that ionic_tx_clean() calls napi_consume_skb() which calls napi_skb_cache_put(), but before that last call is the note /* Zero budget indicate non-NAPI context called us, like netpoll */ and DEBUG_NET_WARN_ON_ONCE(!in_softirq()); Those are pretty big hints that we're doing it wrong. We can pass a context hint down through the calls to let ionic_tx_clean() know what we're doing so it can call napi_consume_skb() correctly.	2024-07-29	5.5	CVE-2024-42071
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_buffers: Fix memory corruptions on Spectrum-4 systems The following two shared buffer operations make use of the Shared Buffer Status Register (SBSR): # devlink sb occupancy snapshot pci/0000:01:00.0 # devlink sb occupancy clearmax pci/0000:01:00.0 The register has two masks of 256 bits to denote on which ingress / egress ports the register should operate on. Spectrum-4 has more than 256 ports, so the register was extended by cited commit with a new 'port_page' field. However, when filling the register's payload, the driver specifies the ports as absolute numbers and not relative to the first port of the port page, resulting in memory corruptions [1]. Fix by specifying the ports relative to the first port of the port page. [1] BUG: KASAN: slab-use-after-free in mlxsw_sp_sb_occ_snapshot+0xb6d/0xbc0 Read of size 1 at addr ffff8881068cb00f by task devlink/1566 [...] Call Trace: <TASK> dump_stack_lvl+0xc6/0x120 print_report+0xce/0x670 kasan_report+0xd7/0x110 mlxsw_sp_sb_occ_snapshot+0xb6d/0xbc0 mlxsw_devlink_sb_occ_snapshot+0x75/0xb0 devlink_nl_sb_occ_snapshot_doit+0x1f9/0x2a0 genl_family_rcv_msg_doit+0x20c/0x300 genl_rcv_msg+0x567/0x800 netlink_rcv_skb+0x170/0x450 genl_rcv+0x2d/0x40 netlink_unicast+0x547/0x830 netlink_sendmsg+0x8d4/0xdb0 __sys_sendto+0x49b/0x510 __x64_sys_sendto+0xe5/0x1c0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f [...] Allocated by task 1: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 __kasan_kmalloc+0x8f/0xa0 copy_verifier_state+0xbc2/0xfb0 do_check_common+0x2c51/0xc7e0 bpf_check+0x5107/0x9960 bpf_prog_load+0xf0e/0x2690 __sys_bpf+0x1a61/0x49d0 __x64_sys_bpf+0x7d/0xc0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 1: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3b/0x60 poison_slab_object+0x109/0x170 __kasan_slab_free+0x14/0x30 kfree+0xca/0x2b0 free_verifier_state+0xce/0x270	2024-07-29	5.5	CVE-2024-42073

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	do_check_common+0x4828/0xc7e0 bpf_check+0x5107/0x9960 bpf_prog_load+0xf0e/0x2690 __sys_bpf+0x1a61/0x49d0 __x64_sys_bpf+0x7d/0xc0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd: acp: add a null check for chip_pdev structure When acp platform device creation is skipped, chip->chip_pdev value will remain NULL. Add NULL check for chip->chip_pdev structure in snd_acp_resume() function to avoid null pointer dereference.	2024-07-29	5.5	CVE-2024-42074
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix remap of arena. The bpf arena logic didn't account for mremap operation. Add a refcnt for multiple mmap events to prevent use-after-free in arena_vm_close.	2024-07-29	5.5	CVE-2024-42075
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: can: j1939: Initialize unused data in j1939_send_one() syzbot reported kernel-infoleak in raw_recvmsg() [1]. j1939_send_one() creates full frame including unused data, but it doesn't initialize it. This causes the kernel-infoleak issue. Fix this by initializing unused data. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in copy_to_user_iter lib/iov_iter.c:24 [inline] BUG: KMSAN: kernel-infoleak in iterate_ubuf include/linux/iov_iter.h:29 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance2 include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance include/linux/iov_iter.h:271 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 instrument_copy_to_user include/linux/instrumented.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline] iterate_ubuf include/linux/iov_iter.h:29 [inline] iterate_and_advance2 include/linux/iov_iter.h:245 [inline] iterate_and_advance include/linux/iov_iter.h:271 [inline] _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 copy_to_iter include/linux/uio.h:196 [inline] memcpy_to_msg include/linux/skbuff.h:4113 [inline] raw_recvmsg+0x2b8/0x9e0 net/can/raw.c:1008 sock_recvmsg_nosec net/socket.c:1046 [inline] sock_recvmsg+0x2c4/0x340 net/socket.c:1068 ____sys_recvmsg+0x18a/0x620 net/socket.c:2803 ___sys_recvmsg+0x223/0x840 net/socket.c:2845 do_recvmmsg+0x4fc/0xfd0 net/socket.c:2939 __sys_recvmmsg net/socket.c:3018 [inline] __do_sys_recvmmsg net/socket.c:3041 [inline] __se_sys_recvmmsg net/socket.c:3034 [inline] __x64_sys_recvmmsg+0x397/0x490 net/socket.c:3034 x64_sys_call+0xf6c/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:300 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3804 [inline] slab_alloc_node mm/slub.c:3845 [inline] kmem_cache_alloc_node+0x613/0xc50 mm/slub.c:3888 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:577 __alloc_skb+0x35b/0x7a0 net/core/skbuff.c:668 alloc_skb include/linux/skbuff.h:1313 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6504 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2795 sock_alloc_send_skb include/net/sock.h:1842 [inline] j1939_sk_alloc_skb net/can/j1939/socket.c:878 [inline] j1939_sk_send_loop net/can/j1939/socket.c:1142 [inline] j1939_sk_sendmsg+0xc0a/0x2730 net/can/j1939/socket.c:1277 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 ____sys_sendmsg+0x877/0xb60 net/socket.c:2584 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2638 __sys_sendmsg net/socket.c:2667 [inline] __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] __x64_sys_sendmsg+0x307/0x4a0 net/socket.c:2674 x64_sys_call+0xc4b/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0	2024-07-29	5.5	CVE-2024-42076

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Bytes 12-15 of 16 are uninitialized Memory access of size 16 starts at ffff888120969690 Data copied to user address 00000000200017c0 CPU: 1 PID: 5050 Comm: syz-executor198 Not tainted 6.9.0-rc5-syzkaller-00031-g71b1543c83d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix DIO failure due to insufficient transaction credits The code in ocfs2_dio_end_io_write() estimates number of necessary transaction credits using ocfs2_calc_extend_credits(). This however does not take into account that the IO could be arbitrarily large and can contain arbitrary number of extents. Extent tree manipulations do often extend the current transaction but not in all of the cases. For example if we have only single block extents in the tree, ocfs2_mark_extent_written() will end up calling ocfs2_replace_extent_rec() all the time and we will never extend the current transaction and eventually exhaust all the transaction credits if the IO contains many single block extents. Once that happens a WARN_ON(jbd2_handle_buffer_credits(handle) <= 0) is triggered in jbd2_journal_dirty_metadata() and subsequently OCFS2 aborts in response to this error. This was actually triggered by one of our customers on a heavily fragmented OCFS2 filesystem. To fix the issue make sure the transaction always has enough credits for one extent insert before each call of ocfs2_mark_extent_written(). Heming Zhao said: ------ PANIC: "Kernel panic - not syncing: OCFS2: (device dm-1): panic forced after error" PID: xxx TASK: xxxx CPU: 5 COMMAND: "SubmitThread-CA" #0 machine_kexec at ffffffff8c069932 #1 __crash_kexec at ffffffff8c1338fa #2 panic at ffffffff8c1d69b9 #3 ocfs2_handle_error at ffffffffc0c86c0c [ocfs2] #4 __ocfs2_abort at ffffffffc0c88387 [ocfs2] #5 ocfs2_journal_dirty at ffffffffc0c51e98 [ocfs2] #6 ocfs2_split_extent at ffffffffc0c27ea3 [ocfs2] #7 ocfs2_change_extent_flag at ffffffffc0c28053 [ocfs2] #8 ocfs2_mark_extent_written at ffffffffc0c28347 [ocfs2] #9 ocfs2_dio_end_io_write at ffffffffc0c2bef9 [ocfs2] #10 ocfs2_dio_end_io at ffffffffc0c2c0f5 [ocfs2] #11 dio_complete at ffffffff8c2b9fa7 #12 do_blockdev_direct_IO at ffffffff8c2bc09f #13 ocfs2_direct_IO at ffffffffc0c2b653 [ocfs2] #14 generic_file_direct_write at ffffffff8c1dcf14 #15 __generic_file_write_iter at ffffffff8c1dd07b #16 ocfs2_file_write_iter at ffffffffc0c49f1f [ocfs2] #17 aio_write at ffffffff8c2cc72e #18 kmem_cache_alloc at ffffffff8c248dde #19 do_io_submit at ffffffff8c2ccada #20 do_syscall_64 at ffffffff8c004984 #21 entry_SYSCALL_64_after_hwframe at ffffffff8c8000ba	2024-07-29	5.5	CVE-2024-42077
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Wipe copies of clear-key structures on failure Wipe all sensitive data from stack for all IOCTLs, which convert a clear-key into a protected- or secure-key.	2024-07-30	4.1	CVE-2024-42156
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Wipe sensitive data on failure Wipe sensitive data from stack also if the copy_to_user() fails.	2024-07-30	4.1	CVE-2024-42157
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Use kfree_sensitive() to fix Coccinelle warnings Replace memzero_explicit() and kfree() with kfree_sensitive() to fix warnings reported by Coccinelle: WARNING opportunity for kfree_sensitive/kvfree_sensitive (line 1506) WARNING opportunity	2024-07-30	4.1	CVE-2024-42158

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	for kfree_sensitive/kvfree_sensitive (line 1643) WARNING opportunity for kfree_sensitive/kvfree_sensitive (line 1770)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: usb: xhci: prevent potential failure in handle_tx_event() for Transfer events without TRB Some transfer events don't always point to a TRB, and consequently don't have a endpoint ring. In these cases, function handle_tx_event() should not proceed, because if 'ep->skip' is set, the pointer to the endpoint ring is used. To prevent a potential failure and make the code logical, return after checking the completion code for a Transfer event without TRBs.	2024-07-30	4.6	CVE-2024-42226
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix overlapping copy within dml_core_mode_programming [WHY] &mode_lib->mp.Watermark and &locals->Watermark are the same address. memcpy may lead to unexpected behavior. [HOW] memmove should be used.	2024-07-30	4.7	CVE-2024-42227
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: aead,cipher - zeroize key buffer after use I.G 9.7.B for FIPS 140-3 specifies that variables temporarily holding cryptographic information should be zeroized once they are no longer needed. Accomplish this by using kfree_sensitive for buffers that previously held the private key.	2024-07-30	4.1	CVE-2024-42229
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: Fix scv instruction crash with kexec kexec on pseries disables AIL (reloc_on_exc), required for scv instruction support, before other CPUs have been shut down. This means they can execute scv instructions after AIL is disabled, which causes an interrupt at an unexpected entry location that crashes the kernel. Change the kexec sequence to disable AIL after other CPUs have been brought down. As a refresher, the real-mode scv interrupt vector is 0x17000, and the fixed-location head code probably couldn't easily deal with implementing such high addresses so it was just decided not to support that interrupt at all.	2024-07-30	4.4	CVE-2024-42230
LiquidPoll--LiquidPoll Advanced Polls for Creators and Brands	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LiquidPoll LiquidPoll - Advanced Polls for Creators and Brands.This issue affects LiquidPoll - Advanced Polls for Creators and Brands: from n/a through 3.3.77.	2024-08-01	6.5	CVE-2024-39655
ManageEngine--Applications Manager	Zohocorp ManageEngine Applications Manager versions 170900 and below are vulnerable to the authenticated admin-only SQL Injection in the Create Monitor feature.	2024-08-01	4.7	CVE-2024-5678
Mashov--Mashov	Mashov - CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	2024-07-30	6.1	CVE-2024-41693
Matrix--Tafnit v8	Matrix - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2024-07-30	5.4	CVE-2024-38430
Matrix--Tafnit v8	Matrix Tafnit v8 - CWE-204: Observable Response Discrepancy	2024-07-30	5.3	CVE-2024-38431

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Matrix--Tafnit v8	Matrix Tafnit v8 - CWE-646: Reliance on File Name or Extension of Externally-Supplied File	2024-07-30	5.5	CVE-2024-38432
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0, 9.5.x <= 9.5.6, 9.7.x <= 9.7.5, 9.8.x <= 9.8.1 fail to properly safeguard an error handling which allows a malicious remote to permanently delete local data by abusing dangerous error handling, when share channels were enabled.	2024-08-01	6.8	CVE-2024-39832
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0, 9.5.x <= 9.5.6, 9.7.x <= 9.7.5, 9.8.x <= 9.8.1 fail to properly validate synced posts, when shared channels are enabled, which allows a malicious remote to create/update/delete arbitrary posts in arbitrary channels	2024-08-01	5.5	CVE-2024-41144
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0, 9.5.x <= 9.5.6, 9.7.x <= 9.7.5, 9.8.x <= 9.8.1 fail to disallow users to set their own remote username, when shared channels were enabled, which allows a user on a remote to set their remote username prop to an arbitrary string, which would be then synced to the local server as long as the user hadn't been synced before.	2024-08-01	4.3	CVE-2024-39839
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0, 9.5.x <= 9.5.6, 9.7.x <= 9.7.5 and 9.8.x <= 9.8.1 fail to disallow the modification of local channels by a remote, when shared channels are enabled, which allows a malicious remote to make an arbitrary local channel read-only.	2024-08-01	4.1	CVE-2024-41162
mkucej--i-librarian-free	I, Librarian is an open-source version of a PDF managing SaaS. PDF notes are displayed on the Item Summary page without any form of validation or sanitation. An attacker can exploit this vulnerability by inserting a payload in the PDF notes that contains malicious code or script. This code will then be executed when the page is loaded in the browser. The vulnerability was fixed in version 5.11.1.	2024-07-30	4.6	CVE-2024-41943
MobSF--Mobile-Security-Framework-MobSF	Mobile Security Framework (MobSF) is a security research platform for mobile applications in Android, iOS and Windows Mobile. An open redirect vulnerability exist in MobSF authentication view. Update to MobSF v4.0.5.	2024-07-31	5.2	CVE-2024-41955
Modernaweb Studio--Black Widgets For Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Modernaweb Studio Black Widgets For Elementor allows Stored XSS.This issue affects Black Widgets For Elementor: from n/a through 1.3.5.	2024-08-01	6.5	CVE-2024-39644
Modernaweb Studio--Black Widgets For Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Modernaweb Studio Black Widgets For Elementor allows Stored XSS.This issue affects Black Widgets For Elementor: from n/a through 1.3.5.	2024-08-01	6.5	CVE-2024-39662
MotoPress--Timetable and Event Schedule	Deserialization of Untrusted Data vulnerability in MotoPress Timetable and Event Schedule allows Object Injection.This issue affects Timetable and Event Schedule: from n/a through 2.4.13.	2024-08-01	5.5	CVE-2024-39630
motovnet--Ebook Store	The Ebook Store plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 5.8001. This is due to the plugin utilizing fpdi-protection and not preventing direct access to test files that have display_errors 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.	2024-08-02	5.3	CVE-2024-6567

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--Mp3tag	A vulnerability has been found in Mp3tag up to 3.26d and classified as problematic. This vulnerability affects unknown code in the library tak_deco_lib.dll of the component DLL Handler. The manipulation leads to uncontrolled search path. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. Upgrading to version 3.26e is able to address this issue. It is recommended to upgrade the affected component. VDB-272614 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early, responded in a very professional manner and immediately released a fixed version of the affected product.	2024-07-29	5.3	CVE-2024-7193
n/a--n/a	Cross Site Scripting vulnerability in Lost and Found Information System 1.0 allows a remote attacker to escalate privileges via the page parameter to php-lfis/admin/index.php.	2024-07-29	6.1	CVE-2024-37859
n/a--n/a	A heap buffer overflow in the function cp_stored() (/vendor/cute_png.h) of hicolor v0.5.0 allows attackers to cause a Denial of Service (DoS) via a crafted PNG file.	2024-07-30	6.2	CVE-2024-41438
n/a--n/a	A heap buffer overflow in the function png_quantize() of hicolor v0.5.0 allows attackers to cause a Denial of Service (DoS) via a crafted PNG file.	2024-07-30	6.2	CVE-2024-41440
n/a--n/a	Cross Site Scripting (XSS) vulnerability in AML Surety Eco up to 3.5 allows an attacker to run arbitrary code via crafted GET request using the id parameter.	2024-07-29	6.1	CVE-2024-41640
n/a--n/a	In the Elliptic package 6.5.6 for Node.js, EDDSA signature malleability occurs because there is a missing signature length check, and thus zero-valued bytes can be removed or appended.	2024-08-02	5.3	CVE-2024-42459
n/a--n/a	In the Elliptic package 6.5.6 for Node.js, ECDSA signature malleability occurs because there is a missing check for whether the leading bit of r and s is zero.	2024-08-02	5.3	CVE-2024-42460
n/a--n/a	Cross Site Scripting vulnerability in Best House Rental Management System 1.0 allows a remote attacker to execute arbitrary code via the "House No" and "Description" parameters in the houses page at the index.php component.	2024-07-29	4.7	CVE-2024-40576
n/a--YouDianCMS	A vulnerability, which was classified as critical, was found in YouDianCMS 7. Affected is an unknown function of the file /Public/ckeditor/plugins/multiimage/dialogs/image_upload.php. The manipulation of the argument files leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273252. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-31	6.3	CVE-2024-7329

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--YouDianCMS	A vulnerability has been found in YouDianCMS 7 and classified as critical. Affected by this vulnerability is the function curl_exec of the file /App/Core/Extend/Function/ydLib.php. The manipulation of the argument url leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273253 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-01	6.3	CVE-2024-7330
n/a--YouDianCMS	A vulnerability, which was classified as problematic, has been found in YouDianCMS 7. This issue affects some unknown processing of the file /t.php?action=phpinfo. The manipulation leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273251. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-31	5.3	CVE-2024-7328
OpenMage--magento-lts	Magento-lts is a long-term support alternative to Magento Community Edition (CE). This XSS vulnerability affects the design/header/welcome, design/header/logo_src, design/header/logo_src_small, and design/header/logo_alt system configs.They are intended to enable admins to set a text in the two cases, and to define an image url for the other two cases. But because of previously missing escaping allowed to input arbitrary html and as a consequence also arbitrary JavaScript. The problem is patched with Version 20.10.1 or higher.	2024-07-29	4.1	CVE-2024-41676
petesheppard84--Extensions for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in petesheppard84 Extensions for Elementor allows Stored XSS.This issue affects Extensions for Elementor: from n/a through 2.0.31.	2024-08-01	6.5	CVE-2024-39668
pickplugins--Gutenberg Blocks, Page Builder ComboBlocks	The Gutenberg Blocks, Page Builder - ComboBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the redirectURL parameter of the Date Countdown widget, in all versions up to, and including, 2.2.85a 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.	2024-08-01	6.4	CVE-2024-6346
pimcore--admin-ui-classic-bundle	Pimcore's Admin Classic Bundle provides a backend user interface for Pimcore. Navigating to `/admin/index/statistics` with a logged in Pimcore user exposes information about the Pimcore installation, PHP version, MYSQL version, installed bundles and all database tables and their row count in the system. This vulnerability is fixed in 1.5.2, 1.4.6, and 1.3.10.	2024-07-30	6.3	CVE-2024-41109
Pixelcurve--Edubin	Server Side Request Forgery (SSRF) vulnerability in Pixelcurve Edubin edubin.This issue affects Edubin: from n/a through 9.2.0.	2024-08-01	5.4	CVE-2024-39637
Plug&Track--Sensor Net Connect V2	A "CWE-352: Cross-Site Request Forgery (CSRF)" can be exploited by remote attackers to perform state-changing operations with administrative privileges by luring authenticated victims into visiting a malicious web page.	2024-07-31	6.6	CVE-2024-3083
Plug&Track--Sensor Net Connect V2	A "CWE-256: Plaintext Storage of a Password" affecting the administrative account allows an attacker with physical access to the machine to retrieve the password in cleartext.	2024-07-31	4.2	CVE-2024-3082

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Plug&Track--Sensor Net Connect V2	A "CWE-201: Insertion of Sensitive Information Into Sent Data" affecting the administrative account allows an attacker with physical access to the machine to retrieve the password in cleartext when an administrative session is open in the browser.	2024-07-31	4.2	CVE-2024-31200
Plug&Track--Thermoscan IP	A "CWE-428: Unquoted Search Path or Element" affects the ThermoscanIP_Scrutation service. Such misconfiguration could be abused in scenarios where incorrect permissions were assigned to the C:\ path to attempt a privilege escalation on the local machine.	2024-07-31	6.5	CVE-2024-31201
Plug&Track--Thermoscan IP	A "CWE-121: Stack-based Buffer Overflow" in the wd210std.dll dynamic library packaged with the ThermoscanIP installer allows a local attacker to possibly trigger a Denial-of-Service (DoS) condition on the target component.	2024-07-31	4	CVE-2024-31203
pr-gateway--Blog2Social: Social Media Auto Post & Scheduler	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 3gp2 file uploads in all versions up to, and including, 7.5.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the 3gp2 file.	2024-08-01	6.4	CVE-2024-7302
Python Software Foundation--CPython	There is a MEDIUM severity vulnerability affecting CPython. The email module didn't properly quote newlines for email headers when serializing an email message allowing for header injection when an email is serialized.	2024-08-01	5.5	CVE-2024-6923
Red Hat--Red Hat Enterprise Linux 7	A flaw was found in Podman. This issue may allow an attacker to create a specially crafted container that, when configured to share the same IPC with at least one other container, can create a large number of IPC resources in /dev/shm. The malicious container will continue to exhaust resources until it is out-of-memory (OOM) killed. While the malicious container's cgroup will be removed, the IPC resources it created are not. Those resources are tied to the IPC namespace that will not be removed until all containers using it are stopped, and one non-malicious container is holding the namespace open. The malicious container is restarted, either automatically or by attacker control, repeating the process and increasing the amount of memory consumed. With a container configured to restart always, such as `podman run --restart=always`, this can result in a memory-based denial of service of the system.	2024-08-02	4.8	CVE-2024-3056
RegistrationMagic Forms--RegistrationMagic	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in RegistrationMagic Forms RegistrationMagic allows Stored XSS.This issue affects RegistrationMagic: from n/a through 6.0.0.1.	2024-08-01	5.8	CVE-2024-39643
ruby--rexml	REXML is an XML toolkit for Ruby. The REXML gem before 3.3.2 has some DoS vulnerabilities when it parses an XML that has many specific characters such as whitespace character, `>]` and `]>`. The REXML gem 3.3.3 or later include the patches to fix these vulnerabilities.	2024-08-01	5.3	CVE-2024-41123
ruby--rexml	REXML is an XML toolkit for Ruby. The REXML gem 3.3.2 has a DoS vulnerability when it parses an XML that has many entity expansions with SAX2 or pull parser API. The REXML gem 3.3.3 or later include the patch to fix the vulnerability.	2024-08-01	5.3	CVE-2024-41946

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SimpleMachines--SMF	A vulnerability, which was classified as critical, was found in SimpleMachines SMF 2.1.4. Affected is an unknown function of the file /index.php?action=profile;u=2;area=showalerts;do=remove of the component Delete User Handler. The manipulation of the argument aid leads to improper control of resource identifiers. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-273522 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-03	5.4	CVE-2024-7437
SimpleMachines--SMF	A vulnerability has been found in SimpleMachines SMF 2.1.4 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /index.php?action=profile;u=2;area=showalerts;do=read of the component User Alert Read Status Handler. The manipulation of the argument aid leads to improper control of resource identifiers. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273523. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-03	4.3	CVE-2024-7438
SourceCodester--Complaints Report Management System	A vulnerability was found in SourceCodester Complaints Report Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/manage_complaint.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. VDB-272618 is the identifier assigned to this vulnerability.	2024-07-29	6.3	CVE-2024-7197
SourceCodester--Complaints Report Management System	A vulnerability classified as critical has been found in SourceCodester Complaints Report Management System 1.0. This affects an unknown part of the file /admin/manage_station.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272619.	2024-07-29	6.3	CVE-2024-7198
SourceCodester--Complaints Report Management System	A vulnerability classified as critical was found in SourceCodester Complaints Report Management System 1.0. This vulnerability affects unknown code of the file /admin/manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272620.	2024-07-29	6.3	CVE-2024-7199
SourceCodester--Establishment Billing Management System	A vulnerability was found in SourceCodester Establishment Billing Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /manage_user.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273156.	2024-07-31	6.3	CVE-2024-7287
SourceCodester--Establishment Billing Management System	A vulnerability was found in SourceCodester Establishment Billing Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=delete_block. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273157 was assigned to this vulnerability.	2024-07-31	6.3	CVE-2024-7288
SourceCodester--Establishment Billing Management System	A vulnerability was found in SourceCodester Establishment Billing Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /manage_payment.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. VDB-273158 is the identifier assigned to this vulnerability.	2024-07-31	6.3	CVE-2024-7289

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SourceCodester--Establishment Billing Management System	A vulnerability classified as critical has been found in SourceCodester Establishment Billing Management System 1.0. This affects an unknown part of the file /manage_tenant.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273159.	2024-07-31	6.3	CVE-2024-7290
SourceCodester--Establishment Billing Management System	A vulnerability, which was classified as critical, was found in SourceCodester Establishment Billing Management System 1.0. Affected is an unknown function of the file /manage_block.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-273198 is the identifier assigned to this vulnerability.	2024-07-31	6.3	CVE-2024-7306
SourceCodester--Establishment Billing Management System	A vulnerability has been found in SourceCodester Establishment Billing Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /manage_billing.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273199.	2024-07-31	6.3	CVE-2024-7307
SourceCodester--Establishment Billing Management System	A vulnerability was found in SourceCodester Establishment Billing Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /view_bill.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. The identifier of this vulnerability is VDB-273200.	2024-07-31	6.3	CVE-2024-7308
SourceCodester--Lot Reservation Management System	A vulnerability, which was classified as critical, was found in SourceCodester Lot Reservation Management System 1.0. Affected is an unknown function of the file /home.php. The manipulation of the argument type leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-272802 is the identifier assigned to this vulnerability.	2024-07-30	6.3	CVE-2024-7222
SourceCodester--Lot Reservation Management System	A vulnerability has been found in SourceCodester Lot Reservation Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /view_model.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272803.	2024-07-30	6.3	CVE-2024-7223
SourceCodester--Lot Reservation Management System	A vulnerability was found in SourceCodester Lot Reservation Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /lot_details.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. The identifier of this vulnerability is VDB-272804.	2024-07-30	6.3	CVE-2024-7224
SourceCodester--Lot Reservation Management System	A vulnerability was found in SourceCodester Lot Reservation Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/view_reserved.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273149 was assigned to this vulnerability.	2024-07-31	6.3	CVE-2024-7280
SourceCodester--Lot Reservation Management System	A vulnerability classified as critical has been found in SourceCodester Lot Reservation Management System 1.0. Affected is an unknown function of the file /admin/index.php?page=manage_lot. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been	2024-07-31	6.3	CVE-2024-7281

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disclosed to the public and may be used. VDB-273150 is the identifier assigned to this vulnerability.			
SourceCodester--Lot Reservation Management System	A vulnerability classified as critical was found in SourceCodester Lot Reservation Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/manage_model.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273151.	2024-07-31	6.3	CVE-2024-7282
SourceCodester--Lot Reservation Management System	A vulnerability, which was classified as critical, has been found in SourceCodester Lot Reservation Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/manage_user.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. The identifier of this vulnerability is VDB-273152.	2024-07-31	6.3	CVE-2024-7283
SourceCodester--Medicine Tracker System	A vulnerability was found in SourceCodester Medicine Tracker System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /classes/Users.php?f=save_user of the component Password Change Handler. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-272806 is the identifier assigned to this vulnerability.	2024-07-30	4.3	CVE-2024-7226
SourceCodester--School Log Management System	A vulnerability classified as critical was found in SourceCodester School Log Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/print_barcode.php. The manipulation of the argument tbl leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272791.	2024-07-30	6.3	CVE-2024-7220
SourceCodester--School Log Management System	A vulnerability, which was classified as critical, has been found in SourceCodester School Log Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/manage_user.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. The identifier of this vulnerability is VDB-272792.	2024-07-30	6.3	CVE-2024-7221
SourceCodester--Simple Realtime Quiz System	A vulnerability was found in SourceCodester Simple Realtime Quiz System 1.0. It has been classified as critical. Affected is an unknown function of the file /manage_quiz.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-273354 is the identifier assigned to this vulnerability.	2024-08-01	6.3	CVE-2024-7370
SourceCodester--Simple Realtime Quiz System	A vulnerability was found in SourceCodester Simple Realtime Quiz System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /quiz_view.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273355.	2024-08-01	6.3	CVE-2024-7371
SourceCodester--Simple Realtime Quiz System	A vulnerability was found in SourceCodester Simple Realtime Quiz System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /quiz_board.php. The manipulation of the argument quiz leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273356.	2024-08-02	6.3	CVE-2024-7372
SourceCodester--Simple Realtime	A vulnerability classified as critical has been found in SourceCodester Simple Realtime Quiz System 1.0. This affects an unknown part of the file /ajax.php?action=load_answered. The manipulation of the argument id leads to sql	2024-08-02	6.3	CVE-2024-7373

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Quiz System	injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273357 was assigned to this vulnerability.			
SourceCodester--Simple Realtime Quiz System	A vulnerability classified as critical was found in SourceCodester Simple Realtime Quiz System 1.0. This vulnerability affects unknown code of the file /manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273358 is the identifier assigned to this vulnerability.	2024-08-02	6.3	CVE-2024-7374
SourceCodester--Simple Realtime Quiz System	A vulnerability, which was classified as critical, has been found in SourceCodester Simple Realtime Quiz System 1.0. This issue affects some unknown processing of the file /my_quiz_result.php. The manipulation of the argument quiz leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273359.	2024-08-02	6.3	CVE-2024-7375
SourceCodester--Simple Realtime Quiz System	A vulnerability, which was classified as critical, was found in SourceCodester Simple Realtime Quiz System 1.0. Affected is an unknown function of the file /print_quiz_records.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273360.	2024-08-02	6.3	CVE-2024-7376
SourceCodester--Simple Realtime Quiz System	A vulnerability has been found in SourceCodester Simple Realtime Quiz System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /view_result.php. The manipulation of the argument qid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273361 was assigned to this vulnerability.	2024-08-02	6.3	CVE-2024-7377
SourceCodester--Simple Realtime Quiz System	A vulnerability was found in SourceCodester Simple Realtime Quiz System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /manage_question.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. VDB-273362 is the identifier assigned to this vulnerability.	2024-08-02	6.3	CVE-2024-7378
SourceCodester--Simple Realtime Quiz System	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Realtime Quiz System 1.0. This affects an unknown part of the file /ajax.php?action=save_user. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273351.	2024-08-01	4.3	CVE-2024-7367
SourceCodester--Tracking Monitoring Management System	A vulnerability classified as critical was found in SourceCodester Tracking Monitoring Management System 1.0. This vulnerability affects unknown code of the file /ajax.php?action=save_establishment. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273340.	2024-08-01	6.3	CVE-2024-7361
SourceCodester--Tracking Monitoring Management System	A vulnerability, which was classified as critical, has been found in SourceCodester Tracking Monitoring Management System 1.0. This issue affects some unknown processing of the file /manage_user.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273341 was assigned to this vulnerability.	2024-08-01	6.3	CVE-2024-7362
SourceCodester--Tracking	A vulnerability, which was classified as critical, was found in SourceCodester Tracking Monitoring Management System 1.0. Affected is an unknown function of	2024-08-01	6.3	CVE-2024-7363

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Monitoring Management System	the file /manage_person.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-273342 is the identifier assigned to this vulnerability.			
SourceCodester--Tracking Monitoring Management System	A vulnerability has been found in SourceCodester Tracking Monitoring Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /manage_records.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273343.	2024-08-01	6.3	CVE-2024-7364
SourceCodester--Tracking Monitoring Management System	A vulnerability was found in SourceCodester Tracking Monitoring Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /manage_establishment.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. The identifier of this vulnerability is VDB-273344.	2024-08-01	6.3	CVE-2024-7365
SourceCodester--Tracking Monitoring Management System	A vulnerability classified as problematic has been found in SourceCodester Tracking Monitoring Management System 1.0. This affects an unknown part of the file /ajax.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. The associated identifier of this vulnerability is VDB-273339.	2024-08-01	4.3	CVE-2024-7360
strategy11team--Formidable Forms Contact Form Plugin, Survey, Quiz, Payment, Calculator Form & Custom Form Builder	The Formidable Forms - Contact Form Plugin, Survey, Quiz, Payment, Calculator Form & Custom Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'html' parameter in all versions up to, and including, 6.11.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with form editing permissions and Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-31	4.9	CVE-2024-6725
takanakui--WP Mobile Menu The Mobile-Friendly Responsive Menu	The WP Mobile Menu plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_menu_item_icon function in all versions up to, and including, 2.8.4.4. This makes it possible for unauthenticated attackers to add the '_mobmenu_icon' post meta to arbitrary posts with an arbitrary (but sanitized) value. NOTE: Version 2.8.4.4 contains a partial fix for this vulnerability.	2024-07-31	5.3	CVE-2024-2508
templatespare--TemplateSpare: Quick & Easy WordPress Site Builder 475+ Ready-Made Demos for News, Blogs, eCommerce, and More. One-Click Import, No Coding Needed	The Build Your Dream Website Fast with 400+ Starter Templates and Landing Pages, No Coding Needed, One-Click Import for Elementor & Gutenberg Blocks! - TemplateSpare plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'templatespare_activate_required_theme' and 'templatespare_get_theme_status' functions in all versions up to, and including, 2.4.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to activate any installed theme and read any theme status. If the attacker attempts to activate a theme that is not installed, a non-existent theme with the slug chosen by the attacker will be considered the active theme, leaving the site with no theme functionality.	2024-08-03	4.3	CVE-2024-6872
ThemeGrill--Himalayas	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeGrill Himalayas allows Stored XSS.This issue affects Himalayas: from n/a through 1.3.2.	2024-08-01	5.9	CVE-2024-39629

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Themewinter--Eventin	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themewinter Eventin allows Stored XSS.This issue affects Eventin: from n/a through 4.0.5.	2024-08-01	5.9	CVE-2024-39648
TOTOLINK--A3600R	A vulnerability has been found in TOTOLINK A3600R 4.1.2cu.5182_B20201102 and classified as critical. This vulnerability affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ipDoamin leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272596. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	6.3	CVE-2024-7175
TOTOLINK--A3600R	A vulnerability classified as critical was found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. This vulnerability affects the function setTelnetCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument telnet_enabled leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-272602 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	6.3	CVE-2024-7181
TOTOLINK--CA300-PoE	A vulnerability was found in TOTOLINK CA300-PoE 6.2c.884. It has been declared as critical. This vulnerability affects the function loginauth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272788. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-30	6.3	CVE-2024-7217
TOTOLINK--LR1200	A vulnerability was found in TOTOLINK LR1200 9.3.1cu.2832 and classified as critical. Affected by this issue is the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument host_time leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-272786 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-30	6.3	CVE-2024-7215
TOTOLINK--LR350	A vulnerability has been found in TOTOLINK LR350 9.3.5u.6369_B20220309 and classified as critical. Affected by this vulnerability is the function setWanCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272785 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-30	6.3	CVE-2024-7214
TVT--DVR TD-2104TS-CL	A vulnerability has been found in TVT DVR TD-2104TS-CL, DVR TD-2108TS-HP, Provision-ISR DVR SH-4050A5-5L(MM) and AVISION DVR AV108T and classified as problematic. This vulnerability affects unknown code of the file /queryDevInfo. The manipulation leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273262 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-01	5.3	CVE-2024-7339
twisted--twisted	Twisted is an event-based framework for internet applications, supporting Python 3.6+. The `twisted.web.util.redirectTo` function contains an HTML injection vulnerability. If application code allows an attacker to control the redirect URL this vulnerability may result in Reflected Cross-Site Scripting (XSS) in the redirect response HTML body. This vulnerability is fixed in 24.7.0rc1.	2024-07-29	6.1	CVE-2024-41810
Unknown--Donation Block For	The Donation Block For PayPal WordPress plugin through 2.1.0 does not sanitise and escape form submissions, leading to a stored cross-site scripting vulnerability	2024-07-30	6.8	CVE-2024-6021

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
PayPal				
Unknown--Email Encoder	The Email Encoder WordPress plugin before 2.2.2 does not escape the WP_Email_Encoder_Bundle_options[protection_text] parameter before outputting it back in an attribute in an admin page, leading to a Stored Cross-Site Scripting	2024-07-29	5.4	CVE-2024-4483
Unknown--Essential Blocks	The Essential Blocks WordPress plugin before 4.7.0 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	2024-08-02	5.4	CVE-2024-5595
Unknown--Floating Notification Bar, Sticky Menu on Scroll, Announcement Banner, and Sticky Header for Any Theme	The Floating Notification Bar, Sticky Menu on Scroll, Announcement Banner, and Sticky Header for Any WordPress plugin before 2.7.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	2024-08-01	4.8	CVE-2024-4090
Unknown--FormFlow: WhatsApp Social and Advanced Form Builder with Easy Lead Collection	The FormFlow: WhatsApp Social and Advanced Form Builder with Easy Lead Collection WordPress plugin before 2.12.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2024-07-30	5.9	CVE-2024-3113
Unknown--HTML Forms	The HTML Forms WordPress plugin before 1.3.34 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	2024-07-31	6.5	CVE-2024-6412
Unknown--Inline Related Posts	The Inline Related Posts WordPress plugin before 3.8.0 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)	2024-07-29	5.9	CVE-2024-6487
Unknown--pmpro-member-directory	The pmpro-member-directory WordPress plugin before 1.2.6 does not prevent users with at least the contributor role from leaking other users' sensitive information, including password hashes.	2024-07-30	6.5	CVE-2024-1287
Unknown--pmpro-membership-maps	The pmpro-membership-maps WordPress plugin before 0.7 does not prevent users with at least the contributor role from leaking sensitive information about users with a membership on the site.	2024-07-30	6.5	CVE-2024-1286
Unknown--Responsive Tabs	The Responsive Tabs WordPress plugin through 4.0.8 does not sanitise and escape some of its Tab settings, which could allow high privilege users such as Contributors and above to perform Stored Cross-Site Scripting attacks	2024-07-30	5.9	CVE-2024-4096
Unknown--Send email only on Reply to My Comment	The Send email only on Reply to My Comment WordPress plugin through 1.0.6 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	2024-07-30	6.1	CVE-2024-6223
Unknown--Send email only on Reply to My	The Send email only on Reply to My Comment WordPress plugin through 1.0.6 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	2024-07-30	5.9	CVE-2024-6224

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Comment				
Unknown--Slider by 10Web	The Slider by 10Web WordPress plugin before 1.2.57 does not sanitise and escape its Slider Title, which could allow high privilege users such as editors and above to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	2024-07-31	5.4	CVE-2024-6408
Unknown--socialdriver-framework	The socialdriver-framework WordPress plugin before 2024.04.30 does not sanitise and escape some of its settings, which could allow high privilege users such as contributor to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2024-08-01	4.8	CVE-2024-2872
Unknown--SpiderContacts	The SpiderContacts WordPress plugin through 1.1.7 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	2024-07-31	6.1	CVE-2024-6272
Unknown--Ultimate Blocks	The Ultimate Blocks WordPress plugin before 3.2.0 does not validate and escape some of its post-grid block attributes before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	2024-07-29	4.6	CVE-2024-6362
Unknown--Ultimate Classified Listings	The Ultimate Classified Listings WordPress plugin before 1.3 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	2024-07-29	4.7	CVE-2024-5883
Unknown--WANotifier	The WANotifier WordPress plugin before 2.6.1 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)	2024-07-31	4.8	CVE-2024-6165
Unknown--Web Directory Free	The Web Directory Free WordPress plugin before 1.7.2 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	2024-07-30	6.8	CVE-2024-3669
Unknown--WooCommerce Customers Manager	The WooCommerce Customers Manager WordPress plugin before 30.2 does not have authorisation and CSRF in various AJAX actions, allowing any authenticated users, such as subscriber, to call them and update/delete/create customer metadata, also leading to Stored Cross-Site Scripting due to the lack of escaping of said metadata values.	2024-08-01	6.5	CVE-2024-1747
Unknown--WP Ajax Contact Form	The WP Ajax Contact Form WordPress plugin through 2.2.2 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 admin users	2024-07-30	6.1	CVE-2024-5809
Unknown--WP Ajax Contact Form	The WP Ajax Contact Form WordPress plugin through 2.2.2 does not have CSRF check in place when deleting emails from the email list, which could allow attackers to make a logged in admin perform such action via a CSRF attack	2024-07-30	4.3	CVE-2024-5808
Unknown--wp-affiliate-platform	The wp-affiliate-platform WordPress plugin before 6.5.2 does not have CSRF check in place when deleting affiliates, which could allow attackers to make a logged in user change delete them via a CSRF attack	2024-07-29	5.5	CVE-2024-5285
Unknown--WpStickyBar	The WpStickyBar WordPress plugin through 2.1.0 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	2024-07-30	6.1	CVE-2024-6226
vim--vim	Vim is an open source command line text editor. Vim < v9.1.0647 has double free in src/alloc.c:616. When closing a window, the corresponding tagstack data will be cleared and freed. However a bit later, the quickfix list belonging to that window will also be cleared and if that quickfix list points to the same tagstack data, Vim will try to free it again, resulting in a double-free/use-after-free access exception. Impact is low since the user must intentionally execute vim with several non-	2024-08-01	4.5	CVE-2024-41957

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	default flags, but it may cause a crash of Vim. The issue has been fixed as of Vim patch v9.1.0647			
vim--vim	Vim is an open source command line text editor. double-free in dialog_changed() in Vim < v9.1.0648. When abandoning a buffer, Vim may ask the user what to do with the modified buffer. If the user wants the changed buffer to be saved, Vim may create a new Untitled file, if the buffer did not have a name yet. However, when setting the buffer name to Unnamed, Vim will falsely free a pointer twice, leading to a double-free and possibly later to a heap-use-after-free, which can lead to a crash. The issue has been fixed as of Vim patch v9.1.0648.	2024-08-01	4.2	CVE-2024-41965
Webangon--The Pack Elementor addons	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Webangon The Pack Elementor addons allows PHP Local File Inclusion, Path Traversal.This issue affects The Pack Elementor addons: from n/a through 2.0.8.6.	2024-08-01	4.3	CVE-2024-38768
WPDeveloper--Essential Addons for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloper Essential Addons for Elementor allows Stored XSS.This issue affects Essential Addons for Elementor: from n/a through 5.9.26.	2024-08-01	6.5	CVE-2024-39649
xibosignage--xibo-cms	Xibo is a content management system (CMS). An SQL injection vulnerability was discovered in the API route inside the CMS responsible for Adding/Editing DataSet Column Formulas. This allows an authenticated user to to obtain and modify arbitrary data from the Xibo database by injecting specially crafted values in to the `formula` parameter. Users should upgrade to version 3.3.12 or 4.0.14 which fix this issue.	2024-07-30	6.5	CVE-2024-41804
xibosignage--xibo-cms	Xibo is a content management system (CMS). An SQL injection vulnerability was discovered in the `report/data/proofofplayReport` API route inside the CMS. This allows an authenticated user to to obtain and modify arbitrary data from the Xibo database by injecting specially crafted values in to the `sortBy` parameter. Users should upgrade to version 3.3.12 or 4.0.14 which fix this issue.	2024-07-30	6.5	CVE-2024-41944
xibosignage--xibo-cms	Xibo is a content management system (CMS). An SQL injection vulnerability was discovered in the API routes inside the CMS responsible for Filtering DataSets. This allows an authenticated user to to obtain arbitrary data from the Xibo database by injecting specially crafted values in to the API for viewing DataSet data. Users should upgrade to version 3.3.12 or 4.0.14 which fix this issue.	2024-07-30	4.9	CVE-2024-41803
Xinhu--RockOA	A vulnerability classified as critical was found in Xinhu RockOA 2.6.2. This vulnerability affects the function dataAction of the file /webmain/task/openapi/openmodhetongAction.php. The manipulation of the argument nickName leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273250 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-31	6.3	CVE-2024-7327
xwiki--xwiki-platform	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. When uploading an attachment with a malicious filename, malicious JavaScript code could be executed. This requires a social engineering attack to get the victim into uploading a file with a malicious name. The malicious code is solely executed during the upload and affects only the user uploading the attachment. While this allows performing actions in the name of that user, it seems unlikely that a user wouldn't notice the malicious filename while uploading the attachment. This has been patched in XWiki 14.10.21, 15.5.5, 15.10.6 and 16.0.0.	2024-07-31	6.4	CVE-2024-37900

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xwiki--xwiki-platform	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. When a user has view but not edit right on a page in XWiki, that user can delete the page and replace it by a page with new content without having delete right. The previous version of the page is moved into the recycle bin and can be restored from there by an admin. As the user is recorded as deleter, the user would in theory also be able to view the deleted content, but this is not directly possible as rights of the previous version are transferred to the new page and thus the user still doesn't have view right on the page. It therefore doesn't seem to be possible to exploit this to gain any rights. This has been patched in XWiki 14.10.21, 15.5.5 and 15.10.6 by cancelling save operations by users when a new document shall be saved despite the document's existing already.	2024-07-31	4.3	CVE-2024-37898
YMC--Filter & Grids	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in YMC Filter & Grids allows Stored XSS.This issue affects Filter & Grids: from n/a through 2.9.2.	2024-08-01	6.5	CVE-2024-39665
Yonle--bostr	Bostr is an nostr relay aggregator proxy that acts like a regular nostr relay. bostr let everyone in even having authorized_keys being set when noscraper is set to true. This vulnerability is fixed in 3.0.10.	2024-08-01	4.6	CVE-2024-41962
zitadel--zitadel	Zitadel is an open source identity management system. ZITADEL administrators can enable a setting called "Ignoring unknown usernames" which helps mitigate attacks that try to guess/enumerate usernames. If enabled, ZITADEL will show the password prompt even if the user doesn't exist and report "Username or Password invalid". Due to a implementation change to prevent deadlocks calling the database, the flag would not be correctly respected in all cases and an attacker would gain information if an account exist within ZITADEL, since the error message shows "object not found" instead of the generic error message. This vulnerability is fixed in 2.58.1, 2.57.1, 2.56.2, 2.55.5, 2.54.8, and 2.53.9.	2024-07-31	5.3	CVE-2024-41952
zitadel--zitadel	Zitadel is an open source identity management system. ZITADEL uses HTML for emails and renders certain information such as usernames dynamically. That information can be entered by users or administrators. Due to a missing output sanitization, these emails could include malicious code. This may potentially lead to a threat where an attacker, without privileges, could send out altered notifications that are part of the registration processes. An attacker could create a malicious link, where the injected code would be rendered as part of the email. On the user's detail page, the username was also not sanitized and would also render HTML, giving an attacker the same vulnerability. While it was possible to inject HTML including javascript, the execution of such scripts would be prevented by most email clients and the Content Security Policy in Console UI. This vulnerability is fixed in 2.58.1, 2.57.1, 2.56.2, 2.55.5, 2.54.8 2.53.9, and 2.52.3.	2024-07-31	4.3	CVE-2024-41953
1E--1E Platform	The 1E Platform's component utilized the third-party Duende Identity Server, which suffered from an open redirect vulnerability, permitting an attacker to control the redirection path of end users. Note: 1E Platform's component utilizing	2024-08-01	4.7	CVE-2024-7211

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the third-party Duende Identity Server has been updated with the patch that includes the fix.			
5 Star Plugins--Pretty Simple Popup Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in 5 Star Plugins Pretty Simple Popup Builder allows Stored XSS.This issue affects Pretty Simple Popup Builder: from n/a through 1.0.7.	2024-08-01	5.9	CVE-2024-39626
AccuPOS--AccuPOS	AccuPOS - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	2024-07-30	5.3	CVE-2024-41701
Adobe--Acrobat for Edge	Acrobat for Edge versions 126.0.2592.81 and earlier are affected by an out-of-bounds read vulnerability that could lead to arbitrary file system read access. An attacker could exploit this vulnerability to read contents from a location in memory past the buffer boundary, potentially leading to sensitive information disclosure. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-07-31	5.5	CVE-2024-39379
Adobe--InDesign Desktop	InDesign Desktop versions ID18.5.2, ID19.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-02	5.5	CVE-2024-39396
advancedcoding--Comments wpDiscuz	The Comments - wpDiscuz plugin for WordPress is vulnerable to HTML Injection in all versions up to, and including, 7.6.21. This is due to a lack of filtering of HTML tags in comments. This makes it possible for unauthenticated attackers to add HTML such as hyperlinks to comments when rich editing is disabled.	2024-08-02	5.3	CVE-2024-6704
Ai3--QbiBot	Ai3 QbiBot does not properly filter user input, allowing unauthenticated remote attackers to insert JavaScript code into the chat box. Once the recipient views the message, they will be subject to a Stored XSS attack.	2024-08-02	6.1	CVE-2024-7204
Akana--Akana API Platform	In versions of Akana API Platform prior to 2024.1.0 a flaw resulting in XML External Entity (XXE) was discovered.	2024-07-30	6.3	CVE-2024-3930
Akana--Akana API Platform	In versions of Akana API Platform prior to 2024.1.0, SAML tokens can be replayed.	2024-07-30	5.4	CVE-2024-5249
AkshuDev--PheonixAppAPI	Pheonix App is a Python application designed to streamline various tasks, from managing files to playing mini-games. The issue is that the map of encoding/decoding languages are visible in code. The Problem was patched in 0.2.4.	2024-07-31	4.4	CVE-2024-41951
Apple--iOS and iPadOS	The issue was addressed with improved memory handling. This issue is fixed in iOS 17 and iPadOS 17, macOS Sonoma 14, watchOS 10, tvOS 17. An app may be able to execute arbitrary code with kernel privileges.	2024-07-29	6.6	CVE-2023-40396
Apple--macOS	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.6. An app with root privileges may be able to execute arbitrary code with kernel privileges.	2024-07-29	6.5	CVE-2024-27878

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Apple--macOS	A logic issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.6. Enabling Lockdown Mode while setting up a Mac may cause FileVault to become unexpectedly disabled.	2024-07-29	5.3	CVE-2024-27862
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 'end_redirect_link' parameter in versions up to, and including, 5.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-02	6.4	CVE-2024-4643
BdThemes--Element Pack Elementor Addons	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BdThemes Element Pack Elementor Addons allows Stored XSS.This issue affects Element Pack Elementor Addons: from n/a through 5.6.11.	2024-08-01	6.5	CVE-2024-39667
BDThemes--Element Pack Pro - Addon for Elementor Page Builder WordPress Plugin	The Element Pack - Addon for Elementor Page Builder WordPress Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the widget wrapper link URL in all versions up to, and including, 7.9.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-01	6.4	CVE-2024-2455
boldthemes--Bold Page Builder	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's bt_bb_button shortcode in all versions up to, and including, 5.0.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-30	6.4	CVE-2024-7100
Brainstorm Force--Spectra Pro	The Spectra Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via block ids in all versions up to, and including, 1.1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-02	6.4	CVE-2024-3827
Breakdance--Breakdance	The Breakdance plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the breakdance_css_file_paths_cache parameter in all versions up to, and including, 1.7.2 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.	2024-08-01	6.4	CVE-2024-5330
Breakdance--Breakdance	The Breakdance plugin for WordPress is vulnerable to unauthorized access of data in all versions up to, and including, 1.7.2. This makes it possible for authenticated attackers, with Contributor-level access and above, to export form submissions.	2024-08-01	4.3	CVE-2024-5331
Cato Networks--SDP Client	A vulnerability in Cato Networks SDP Client on Windows allows the insertion of sensitive information into the log file, which can lead to an account takeover. However, the attack requires bypassing protections on modifying the tunnel token on a the attacker's system.This issue affects SDP Client: before 5.10.34.	2024-07-31	6.5	CVE-2024-6977

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cato Networks--SDP Client	Cato Networks Windows SDP Client Local root certificates can be installed by low-privileged users.This issue affects SDP Client: before 5.10.28.	2024-07-31	5.6	CVE-2024-6978
CHANGING Information Technology--HWATAIServiSign Windows Version	The specific API in HWATAIServiSign Windows Version from CHANGING Information Technology does not properly validate the length of server-side inputs. When a user visits a spoofed website, unauthenticated remote attackers can cause a stack-based buffer overflow in the HWATAIServiSign, temporarily disrupting its service.	2024-08-02	4.3	CVE-2024-40723
CHANGING Information Technology--TCBServiSign Windows Version	The encryption strength of the authorization keys in CHANGING Information Technology TCBServiSign Windows Version is insufficient. When a remote attacker tricks a victim into visiting a malicious website, TCBServiSign will treat that website as a legitimate server and interact with it.	2024-08-02	6.5	CVE-2024-40719
CHANGING Information Technology--TCBServiSign Windows Version	The specific API in TCBServiSign Windows Version from CHANGING Information Technology does does not properly validate the length of server-side input. When a user visits a spoofed website, unauthenticated remote attackers can cause a stack-based buffer overflow in the TCBServiSign, temporarily disrupting its service.	2024-08-02	4.3	CVE-2024-40722
codename065--Download Manager	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpdm_all_packages' shortcode in all versions up to, and including, 3.2.97 due to insufficient input sanitization and output escaping on the 'cols' parameter. 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.	2024-07-31	6.4	CVE-2024-6208
Crocoblock--JetWidgets for Elementor and WooCommerce	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Crocoblock JetWidgets for Elementor and WooCommerce allows PHP Local File Inclusion.This issue affects JetWidgets for Elementor and WooCommerce: from n/a through 1.1.7.	2024-08-01	6.5	CVE-2024-38772
Cybonet--PineApp Mail Relay	Cybonet - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	2024-07-30	5.3	CVE-2024-41694
D-Link--DI-8100	A vulnerability, which was classified as critical, has been found in D-Link DI-8100 16.07. This issue affects the function msp_info_htm of the file msp_info.htm. The manipulation of the argument cmd leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273521 was assigned to this vulnerability.	2024-08-03	6.3	CVE-2024-7436
Dahua--NVR4XXX	A vulnerability has been found in Dahua products.After obtaining the administrator's username and password, the attacker can send a carefully crafted data packet to the interface with vulnerabilities, causing device initialization.	2024-07-31	6	CVE-2024-39946
Dahua--NVR4XXX	A vulnerability has been found in Dahua products.After obtaining the ordinary user's username and password, the attacker can send a carefully crafted data packet to the interface with vulnerabilities, causing the device to crash.	2024-07-31	6.5	CVE-2024-39947
Dahua--NVR4XXX	A vulnerability has been found in Dahua products. After obtaining the administrator's username and password, the attacker can send a carefully crafted data packet to the interface with vulnerabilities, causing the device to crash.	2024-07-31	4.9	CVE-2024-39945

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dell -- iDRAC Service Module	Dell iDRAC Service Module version 5.3.0.0 and prior, contain an Out of bound Read Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event.	2024-08-01	4.4	CVE-2024-25947
Dell -- iDRAC Service Module	Dell iDRAC Service Module version 5.3.0.0 and prior, contain a Out of bound Write Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event.	2024-08-01	4.4	CVE-2024-25948
Dell--CloudLink	CloudLink, versions 7.1.x and 8.x, contain an Improper check or handling of Exceptional Conditions Vulnerability in Cluster Component. A highly privileged malicious user with remote access could potentially exploit this vulnerability, leading to execute unauthorized actions and retrieve sensitive information from the database.	2024-08-02	6.6	CVE-2024-38482
Dell--Dell BSAFE Micro Edition Suite	Dell BSAFE Crypto-C Micro Edition 4.1.5 and Dell BSAFE Micro Edition Suite, versions 4.0 through 4.6.1 and version 5.0 contain a buffer over-read vulnerability.	2024-07-31	6.2	CVE-2023-28074
Dell--Dell Inventory Collector	Dell Inventory Collector, versions prior to 12.3.0.6 contains a Path Traversal vulnerability. A local authenticated malicious user could potentially exploit this vulnerability, leading to arbitrary code execution on the system.	2024-07-31	6.7	CVE-2024-37129
Dell--iDRAC Service Module	Dell iDRAC Service Module version 5.3.0.0 and prior, contain a Out of bound Read Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event.	2024-08-01	4.4	CVE-2024-38481
Dell--iDRAC Service Module	Dell iDRAC Service Module version 5.3.0.0 and prior contains Out of bound write Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service (partial) event.	2024-08-01	4.4	CVE-2024-38489
Dell--iDRAC Service Module	Dell iDRAC Service Module version 5.3.0.0 and prior, contain a Out of bound Write Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event.	2024-08-01	4.4	CVE-2024-38490
Dell--InsightIQ	Dell InsightIQ, Verion 5.0.0, contains a use of a broken or risky cryptographic algorithm vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to information disclosure.	2024-08-01	5.9	CVE-2024-28972
Delphix--Data Control Tower (DCT)	A flaw in versions of Delphix Data Control Tower (DCT) prior to 19.0.0 results in broken authentication through the enable-scale-testing functionality of the application.	2024-07-29	5.4	CVE-2024-6727
Digiwin--EasyFlow .NET	Digiwin EasyFlow .NET lacks proper access control for specific functionality, and the functionality do not adequately filter user input. A remote attacker with regular privilege can exploit this vulnerability to download arbitrary files from the remote server .	2024-08-02	6.5	CVE-2024-7323
discourse--discourse	Discourse is an open source discussion platform. Prior to 3.2.3 and 3.3.0.beta3, improperly sanitized Onebox data could lead to an XSS vulnerability in some situations. This vulnerability only affects Discourse instances which have disabled the default Content Security Policy. This vulnerability is fixed in 3.2.3 and 3.3.0.beta3.	2024-07-30	6.3	CVE-2024-37165
discourse--discourse	Discourse is an open source discussion platform. Prior to 3.2.5 and 3.3.0.beta5, the vulnerability allows an attacker to inject iframes from any domain, bypassing the	2024-07-30	6.1	CVE-2024-39320

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	intended restrictions enforced by the allowed_iframes setting. This vulnerability is fixed in 3.2.5 and 3.3.0.beta5.			
discourse--discourse	Discourse is an open source discussion platform. Prior to 3.2.5 and 3.3.0.beta5, crafting requests to submit very long tag group names can reduce the availability of a Discourse instance. This vulnerability is fixed in 3.2.5 and 3.3.0.beta5.	2024-07-30	4.9	CVE-2024-37299
doublesharp--Remote Content Shortcode	The Remote Content Shortcode plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.5 via the remote_content shortcode. This makes it possible for authenticated attackers, with contributor-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	2024-08-01	6.4	CVE-2024-2090
DuendeSoftware--IdentityServer	Duende IdentityServer is an OpenID Connect and OAuth 2.x framework for ASP.NET Core. It is possible for an attacker to craft malicious Urls that certain functions in IdentityServer will incorrectly treat as local and trusted. If such a Url is returned as a redirect, some browsers will follow it to a third-party, untrusted site. Note: by itself, this vulnerability does **not** allow an attacker to obtain user credentials, authorization codes, access tokens, refresh tokens, or identity tokens. An attacker could however exploit this vulnerability as part of a phishing attack designed to steal user credentials. This vulnerability is fixed in 7.0.6, 6.3.10, 6.2.5, 6.1.8, and 6.0.5. Duende.IdentityServer 5.1 and earlier and all versions of IdentityServer4 are no longer supported and will not be receiving updates. If upgrading is not possible, use `IUrlHelper.IsLocalUrl` from ASP.NET Core to validate return Urls in user interface code in the IdentityServer host.	2024-07-31	4.7	CVE-2024-39694
dylanjkotze--Zephyr Project Manager	The Zephyr Project Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'filename' parameter in all versions up to, and including, 3.3.100 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-08-03	6.4	CVE-2024-7356
Elastic--APM Server	APM server logs contain document body from a partially failed bulk index request. For example, in case of unavailable_shards_exception for a specific document, since the ES response line contains the document body, and that APM server logs the ES response line on error, the document is effectively logged.	2024-08-03	5.7	CVE-2024-37286 bressers@elastic.co
Elastic--Elasticsearch	It was discovered by Elastic engineering that when elasticsearch-certutil CLI tool is used with the csr option in order to create a new Certificate Signing Requests, the associated private key that is generated is stored on disk unencrypted even if the --pass parameter is passed in the command invocation.	2024-07-31	4.9	CVE-2024-23444 bressers@elastic.co
Elastic--Kibana	An issue was discovered in Kibana where a user with Viewer role could cause a Kibana instance to crash by sending a large number of maliciously crafted requests to a specific endpoint.	2024-07-30	6.5	CVE-2024-37281 bressers@elastic.co
ELECOM CO.,LTD.--WRC-2533GS2V-B	Unrestricted upload of file with dangerous type vulnerability exists in ELECOM wireless LAN routers. A specially crafted file may be uploaded to the affected product by a logged-in user with an administrative privilege, resulting in an arbitrary OS command execution.	2024-08-01	6.8	CVE-2024-34021
ELECOM CO.,LTD.--WRC-X6000XS-G	OS command injection vulnerability exists in ELECOM wireless LAN routers. A specially crafted request may be sent to the affected product by a logged-in user with an administrative privilege to execute an arbitrary OS command.	2024-08-01	6.8	CVE-2024-39607

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ExtendThemes--Kubio AI Page Builder	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ExtendThemes Kubio AI Page Builder.This issue affects Kubio AI Page Builder: from n/a through 2.2.4.	2024-08-01	6.5	CVE-2024-39661
FFRI Security, Inc.--FFRI AMC	FFRI AMC versions 3.4.0 to 3.5.3 and some OEM products that implement/bundle FFRI AMC versions 3.4.0 to 3.5.3 allow a remote unauthenticated attacker to execute arbitrary OS commands when certain conditions are met in an environment where the notification program setting is enabled and the executable file path is set to a batch file (.bat) or command file (.cmd) extension.	2024-07-30	6.4	CVE-2024-40895
FOGProject--fogproject	FOG is a cloning/imaging/rescue suite/inventory management system. The application stores plaintext service account credentials in the "/opt/fog/.fogsettings" file. This file is by default readable by all users on the host. By exploiting these credentials, a malicious user could create new accounts for the web application and much more. The vulnerability is fixed in 1.5.10.41.	2024-07-31	5.3	CVE-2024-41954
FOGProject--fogproject	FOG is a cloning/imaging/rescue suite/inventory management system. FOG Server 1.5.10.41.4 and earlier can leak authorized and rejected logins via logs stored directly on the root of the web server. FOG Server creates 2 logs on the root of the web server (fog_login_accepted.log and fog_login_failed.log), exposing the name of the user account used to manage FOG, the IP address of the computer used to login and the User-Agent. This vulnerability is fixed in 1.5.10.47.	2024-08-02	5.3	CVE-2024-42349
gpriday--SiteOrigin Widgets Bundle	The SiteOrigin Widgets Bundle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Image Grid widget in all versions up to, and including, 1.62.2 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.	2024-07-30	6.4	CVE-2024-5901
harbor--harbor	Incorrect user permission validation in Harbor <v2.9.5 and Harbor <v2.10.3 allows authenticated users to modify configurations.	2024-08-02	5.4	CVE-2024-22278
Hewlett Packard Enterprise (HPE)--ClearPass Policy Manager (CPPM)	A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further access to network services supported by ClearPass Policy Manager.	2024-07-30	6.8	CVE-2024-41916
Hewlett Packard Enterprise (HPE)--ClearPass Policy Manager (CPPM)	A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further access to network services supported by ClearPass Policy Manager	2024-07-30	5.8	CVE-2024-5486
ibexa--admin-ui	The Ibexa Admin UI Bundle contains all the necessary parts to run the Ibexa DXP Back Office interface. The file upload widget is vulnerable to XSS payloads in filenames. Access permission to upload files is required. As such, in most cases only authenticated editors and administrators will have the required permission. It is not persistent, i.e. the payload is only executed during the upload. In effect, an attacker will have to trick an editor/administrator into uploading a strangely named file.	2024-07-31	5.4	CVE-2024-39318
IBM--Aspera Orchestrator	IBM Aspera Orchestrator 4.0.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 260206.	2024-07-30	6.5	CVE-2023-38001

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--Aspera Orchestrator	IBM Aspera Orchestrator 4.0.1 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: 248477.	2024-07-30	5.5	CVE-2023-26288
IBM--Aspera Orchestrator	IBM Aspera Orchestrator 4.0.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 248478.	2024-07-30	5.4	CVE-2023-26289
IBM--Business Automation Workflow	IBM Business Automation Workflow 22.0.2, 23.0.1, 23.0.2, and 24.0.0 stores potentially sensitive information in log files under certain situations that could be read by an authenticated user. IBM X-Force ID: 284868.	2024-08-03	5.3	CVE-2024-38321
Imagely--NextGEN Gallery	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Imagely NextGEN Gallery allows Stored XSS.This issue affects NextGEN Gallery: from n/a through 3.59.3.	2024-08-01	5.9	CVE-2024-39627
itsourcecode--Alton Management System	A vulnerability classified as critical was found in itsourcecode Alton Management System 1.0. This vulnerability affects unknown code of the file search.php. The manipulation of the argument rcode leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273142 is the identifier assigned to this vulnerability.	2024-07-30	6.3	CVE-2024-7273
itsourcecode--Alton Management System	A vulnerability, which was classified as critical, has been found in itsourcecode Alton Management System 1.0. This issue affects some unknown processing of the file /reservation_status.php. The manipulation of the argument rcode leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273143.	2024-07-30	4.7	CVE-2024-7274
itsourcecode--Alton Management System	A vulnerability, which was classified as critical, was found in itsourcecode Alton Management System 1.0. Affected is an unknown function of the file /admin/category_save.php. The manipulation of the argument category leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273144.	2024-07-30	4.7	CVE-2024-7275
itsourcecode--Alton Management System	A vulnerability has been found in itsourcecode Alton Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/member_save.php. The manipulation of the argument last/first leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273145 was assigned to this vulnerability.	2024-07-30	4.7	CVE-2024-7276
itsourcecode--Alton Management System	A vulnerability was found in itsourcecode Alton Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/menu.php of the component Add a Menu. The manipulation of the argument image leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-273146 is the identifier assigned to this vulnerability.	2024-07-31	4.7	CVE-2024-7277
itsourcecode--Alton Management System	A vulnerability was found in itsourcecode Alton Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/team_save.php. The manipulation of the argument team leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273147.	2024-07-31	4.7	CVE-2024-7278

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
itsourcecode--Online Blood Bank Management System	A vulnerability classified as problematic was found in itsourcecode Online Blood Bank Management System 1.0. This vulnerability affects unknown code of the file signup.php of the component User Registration Handler. The manipulation of the argument user leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273232.	2024-07-31	4.3	CVE-2024-7321
itsourcecode--Online Food Ordering System	A vulnerability classified as critical has been found in itsourcecode Online Food Ordering System 1.0. Affected is an unknown function of the file editproduct.php. The manipulation of the argument photo leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-272610 is the identifier assigned to this vulnerability.	2024-07-29	6.3	CVE-2024-7189
itsourcecode--Society Management System	A vulnerability classified as critical was found in itsourcecode Society Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/get_price.php. The manipulation of the argument expenses_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272611.	2024-07-29	6.3	CVE-2024-7190
itsourcecode--Society Management System	A vulnerability, which was classified as critical, has been found in itsourcecode Society Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/get_balance.php. The manipulation of the argument student_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272612.	2024-07-29	6.3	CVE-2024-7191
itsourcecode--Society Management System	A vulnerability, which was classified as critical, was found in itsourcecode Society Management System 1.0. This affects an unknown part of the file /admin/student.php. The manipulation of the argument 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. The identifier VDB-272613 was assigned to this vulnerability.	2024-07-29	6.3	CVE-2024-7192
itsourcecode--Society Management System	A vulnerability was found in itsourcecode Society Management System 1.0 and classified as critical. This issue affects some unknown processing of the file check_student.php. The manipulation of the argument student_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272615.	2024-07-29	6.3	CVE-2024-7194
itsourcecode--Society Management System	A vulnerability was found in itsourcecode Society Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/check_admin.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. The identifier of this vulnerability is VDB-272616.	2024-07-29	6.3	CVE-2024-7195
itsourcecode--Ticket Reservation System	A vulnerability, which was classified as critical, has been found in itsourcecode Ticket Reservation System 1.0. Affected by this issue is some unknown functionality of the file checkout_ticket_save.php. The manipulation of the argument data leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-273530 is the identifier assigned to this vulnerability.	2024-08-03	4.7	CVE-2024-7445
itsourcecode--Ticket Reservation System	A vulnerability, which was classified as critical, was found in itsourcecode Ticket Reservation System 1.0. This affects an unknown part of the file list_tickets.php. The manipulation of the argument prefSeat_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273531.	2024-08-03	4.7	CVE-2024-7446

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Johnson Controls--exacqVision	Under certain circumstances the ExacqVision Web Services does not provide sufficient protection from untrusted domains.	2024-08-01	6.8	CVE-2024-32862
Johnson Controls--exacqVision	Under certain circumstances the exacqVision Web Services may be susceptible to Cross-Site Request Forgery (CSRF)	2024-08-01	6.8	CVE-2024-32863
Johnson Controls--exacqVision	Under certain circumstances exacqVision Web Services will not enforce secure web communications (HTTPS)	2024-08-01	6.4	CVE-2024-32864
Johnson Controls--exacqVision	Under certain circumstances the exacqVision Server will not properly validate TLS certificates provided by connected devices.	2024-08-01	6.4	CVE-2024-32865
Johnson Controls--exacqVision	Under certain circumstances the exacqVision Web Service can expose authentication token details within communications.	2024-08-01	5.7	CVE-2024-32931
Jordy Meow--AI Engine: ChatGPT Chatbot	Server-Side Request Forgery (SSRF) vulnerability in Jordy Meow AI Engine: ChatGPT Chatbot allows Server Side Request Forgery.This issue affects AI Engine: ChatGPT Chatbot: from n/a through 2.4.7.	2024-08-01	4.9	CVE-2024-38791
Jordy Meow--Photo Engine	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jordy Meow Photo Engine allows Stored XSS.This issue affects Photo Engine: from n/a through 6.3.1.	2024-08-01	5.9	CVE-2024-39660
kp4coder--Sync Post With Other Site	The Sync Post With Other Site plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'sps_add_update_post' function in all versions up to, and including, 1.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create new draft posts and update existing posts.	2024-08-03	4.3	CVE-2024-6709
Lenovo--PC Manager	A vulnerability was reported in Lenovo PC Manager versions prior to 2.6.40.3154 that could allow an attacker to cause a system reboot.	2024-07-31	5.5	CVE-2017-3772
leogermani--Tainacan	The Tainacan plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'get_file' function in all versions up to, and including, 0.21.7. The function is also vulnerable to directory traversal. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	2024-07-31	6.5	CVE-2024-7135
Lester GaMerZ Chan--WP-PostRatings	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Lester 'GaMerZ' Chan WP-PostRatings allows Stored XSS.This issue affects WP-PostRatings: from n/a through 1.91.1.	2024-08-01	6.5	CVE-2024-39659
limpinho--CTT Expresso para	The CTT Expresso para WooCommerce plugin for WordPress is vulnerable to sensitive information exposure in all versions up to and including 3.2.12 via the /wp-content/uploads/cepw directory. The generated .pdf and log files are publicly	2024-08-01	5.3	CVE-2024-6687

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WooCommerce	accessible and contain sensitive information such as sender and receiver names, phone numbers, physical addresses, and email addresses			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nfsd: initialise nfsd_info.mutex early. nfsd_info.mutex can be dereferenced by svc_pool_stats_start() immediately after the new netns is created. Currently this can trigger an oops. Move the initialisation earlier before it can possibly be dereferenced.	2024-07-29	5.5	CVE-2024-42078
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix NULL pointer dereference in gfs2_log_flush In gfs2_jindex_free(), set sdp->sd_jdesc to NULL under the log flush lock to provide exclusion against gfs2_log_flush(). In gfs2_log_flush(), check if sdp->sd_jdesc is non-NULL before dereferencing it. Otherwise, we could run into a NULL pointer dereference when outstanding glock work races with an unmount (glock_work_func -> run_queue -> do_xmote -> inode_go_sync -> gfs2_log_flush).	2024-07-29	5.5	CVE-2024-42079
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/restrack: Fix potential invalid address access struct rdma_restrack_entry's kern_name was set to KBUILD_MODNAME in ib_create_cq(), while if the module exited but forgot del this rdma_restrack_entry, it would cause a invalid address access in rdma_restrack_clean() when print the owner of this rdma_restrack_entry. These code is used to help find one forgotten PD release in one of the ULPs. But it is not needed anymore, so delete them.	2024-07-29	5.5	CVE-2024-42080
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/xe_devcoredump: Check NULL before assignments Assign 'xe_devcoredump_snapshot *' and 'xe_device *' only if 'coredump' is not NULL. v2 - Fix commit messages. v3 - Define variables before code.(Ashutosh/Jose) v4 - Drop return check for coredump_to_xe. (Jose/Rodrigo) v5 - Modify misleading commit message. (Matt)	2024-07-29	5.5	CVE-2024-42081
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xdp: Remove WARN() from __xdp_reg_mem_model() syzkaller reports a warning in __xdp_reg_mem_model(). The warning occurs only if __mem_id_init_hash_table() returns an error. It returns the error in two cases: 1. memory allocation fails; 2. rhashtable_init() fails when some fields of rhashtable_params struct are not initialized properly. The second case cannot happen since there is a static const rhashtable_params struct with valid fields. So, warning is only triggered when there is a problem with memory allocation. Thus, there is no sense in using WARN() to handle this error and it can be safely removed. WARNING: CPU: 0 PID: 5065 at net/core/xdp.c:299 __xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 CPU: 0 PID: 5065 Comm: syz-executor883 Not tainted 6.8.0-syzkaller-05271-gf99c5f563c17 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:__xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 Call Trace: xdp_reg_mem_model+0x22/0x40 net/core/xdp.c:344 xdp_test_run_setup net/bpf/test_run.c:188 [inline] bpf_test_run_xdp_live+0x365/0x1e90 net/bpf/test_run.c:377 bpf_prog_test_run_xdp+0x813/0x11b0 net/bpf/test_run.c:1267 bpf_prog_test_run+0x33a/0x3b0 kernel/bpf/syscall.c:4240 __sys_bpf+0x48d/0x810 kernel/bpf/syscall.c:5649 __do_sys_bpf kernel/bpf/syscall.c:5738 [inline] __se_sys_bpf kernel/bpf/syscall.c:5736 [inline] __x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:5736 do_syscall_64+0xfb/0x240 entry_SYSCALL_64_after_hwframe+0x6d/0x75 Found by Linux Verification Center (linuxtesting.org) with syzkaller.	2024-07-29	5.5	CVE-2024-42082
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ionic: fix kernel panic due to multi-buffer handling Currently, the ionic_run_xdp() doesn't handle multi-buffer packets properly for XDP_TX and XDP_REDIRECT. When a jumbo frame is received, the ionic_run_xdp() first makes xdp frame with all necessary	2024-07-29	5.5	CVE-2024-42083

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	pages in the rx descriptor. And if the action is either XDP_TX or XDP_REDIRECT, it should unmap dma-mapping and reset page pointer to NULL for all pages, not only the first page. But it doesn't for SG pages. So, SG pages unexpectedly will be reused. It eventually causes kernel panic. Oops: general protection fault, probably for non-canonical address 0x504f4e4dbebc64ff: 0000 [#1] PREEMPT SMP NOPTI CPU: 3 PID: 0 Comm: swapper/3 Not tainted 6.10.0-rc3+ #25 RIP: 0010:xdp_return_frame+0x42/0x90 Code: 01 75 12 5b 4c 89 e6 5d 31 c9 41 5c 31 d2 41 5d e9 73 fd ff ff 44 8b 6b 20 0f b7 43 0a 49 81 ed 68 01 00 00 49 29 c5 49 01 fd <41> 80 7d0 RSP: 0018:ffff99d00122ce08 EFLAGS: 00010202 RAX: 0000000000005453 RBX: ffff8d325f904000 RCX: 0000000000000001 RDX: 00000000670e1000 RSI: 000000011f90d000 RDI: 504f4e4d4c4b4a49 RBP: ffff99d003907740 R08: 0000000000000000 R09: 0000000000000000 R10: 000000011f90d000 R11: 0000000000000000 R12: ffff8d325f904010 R13: 504f4e4dbebc64fd R14: ffff8d3242b070c8 R15: ffff99d0039077c0 FS: 0000000000000000(0000) GS:ffff8d399f780000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f41f6c85e38 CR3: 000000037ac30000 CR4: 00000000007506f0 PKRU: 55555554 Call Trace: <IRQ> ? die_addr+0x33/0x90 ? exc_general_protection+0x251/0x2f0 ? asm_exc_general_protection+0x22/0x30 ? xdp_return_frame+0x42/0x90 ionic_tx_clean+0x211/0x280 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] ionic_tx_cq_service+0xd3/0x210 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] ionic_txrx_napi+0x41/0x1b0 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] __napi_poll.constprop.0+0x29/0x1b0 net_rx_action+0x2c4/0x350 handle_softirqs+0xf4/0x320 irq_exit_rcu+0x78/0xa0 common_interrupt+0x77/0x90			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: tda10048: Fix integer overflow state->xtal_hz can be up to 16M, so it can overflow a 32 bit integer when multiplied by pll_mfactor. Create a new 64 bit variable to hold the calculations.	2024-07-30	5.5	CVE-2024-42223
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: fix calc_available_free_space() for zoned mode calc_available_free_space() returns the total size of metadata (or system) block groups, which can be allocated from unallocated disk space. The logic is wrong on zoned mode in two places. First, the calculation of data_chunk_size is wrong. We always allocate one zone as one chunk, and no partial allocation of a zone. So, we should use zone_size (= data_sinfo->chunk_size) as it is. Second, the result "avail" may not be zone aligned. Since we always allocate one zone as one chunk on zoned mode, returning non-zone size aligned bytes will result in less pressure on the async metadata reclaim process. This is serious for the nearly full state with a large zone size device. Allowing over-commit too much will result in less async reclaim work and end up in ENOSPC. We can align down to the zone size to avoid that.	2024-07-30	5.5	CVE-2024-42231
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Skip pipe if the pipe idx not set properly [why] Driver crashes when pipe idx not set properly [how] Add code to skip the pipe that idx not set properly	2024-07-29	5.5	CVE-2024-42064
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Add a NULL check in xe_ttm_stolen_mgr_init Add an explicit check to ensure that the mgr is not NULL.	2024-07-29	5.5	CVE-2024-42065

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix potential integer overflow in page size calculation Explicitly cast tbo->page_alignment to u64 before bit-shifting to prevent overflow when assigning to min_page_size.	2024-07-29	5.5	CVE-2024-42066
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_rox() into account with bpf_jit_binary_lock_ro() set_memory_rox() can fail, leaving memory unprotected. Check return and bail out when bpf_jit_binary_lock_ro() returns an error.	2024-07-29	5.5	CVE-2024-42067
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_ro() into account with bpf_prog_lock_ro() set_memory_ro() can fail, leaving memory unprotected. Check its return and take it into account as an error.	2024-07-29	5.5	CVE-2024-42068
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: mana: Fix possible double free in error handling path When auxiliary_device_add() returns error and then calls auxiliary_device_uninit(), callback function adev_release calls kfree(madev). We shouldn't call kfree(madev) again in the error handling path. Set 'madev' to NULL.	2024-07-29	5.5	CVE-2024-42069
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fully validate NFT_DATA_VALUE on store to data registers register store validation for NFT_DATA_VALUE is conditional, however, the datatype is always either NFT_DATA_VALUE or NFT_DATA_VERDICT. This only requires a new helper function to infer the register type from the set datatype so this conditional check can be removed. Otherwise, pointer to chain object can be leaked through the registers.	2024-07-29	5.5	CVE-2024-42070
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ionic: use dev_consume_skb_any outside of napi If we're not in a NAPI softirq context, we need to be careful about how we call napi_consume_skb(), specifically we need to call it with budget==0 to signal to it that we're not in a safe context. This was found while running some configuration stress testing of traffic and a change queue config loop running, and this curious note popped out: [4371.402645] BUG: using smp_processor_id() in preemptible [00000000] code: ethtool/20545 [4371.402897] caller is napi_skb_cache_put+0x16/0x80 [4371.403120] CPU: 25 PID: 20545 Comm: ethtool Kdump: loaded Tainted: G OE 6.10.0-rc3-netnext+ #8 [4371.403302] Hardware name: HPE ProLiant DL360 Gen10/ProLiant DL360 Gen10, BIOS U32 01/23/2021 [4371.403460] Call Trace: [4371.403613] <TASK> [4371.403758] dump_stack_lvl+0x4f/0x70 [4371.403904] check_preemption_disabled+0xc1/0xe0 [4371.404051] napi_skb_cache_put+0x16/0x80 [4371.404199] ionic_tx_clean+0x18a/0x240 [ionic] [4371.404354] ionic_tx_cq_service+0xc4/0x200 [ionic] [4371.404505] ionic_tx_flush+0x15/0x70 [ionic] [4371.404653] ? ionic_lif_qcq_deinit.isra.23+0x5b/0x70 [ionic] [4371.404805] ionic_txrx_deinit+0x71/0x190 [ionic] [4371.404956] ionic_reconfigure_queues+0x5f5/0xff0 [ionic] [4371.405111] ionic_set_ringparam+0x2e8/0x3e0 [ionic] [4371.405265]	2024-07-29	5.5	CVE-2024-42071

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ethnl_set_rings+0x1f1/0x300 [4371.405418] ethnl_default_set_doit+0xbb/0x160 [4371.405571] genl_family_rcv_msg_doit+0xff/0x130 [...] I found that ionic_tx_clean() calls napi_consume_skb() which calls napi_skb_cache_put(), but before that last call is the note /* Zero budget indicate non-NAPI context called us, like netpoll */ and DEBUG_NET_WARN_ON_ONCE(!in_softirq()); Those are pretty big hints that we're doing it wrong. We can pass a context hint down through the calls to let ionic_tx_clean() know what we're doing so it can call napi_consume_skb() correctly.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_buffers: Fix memory corruptions on Spectrum-4 systems The following two shared buffer operations make use of the Shared Buffer Status Register (SBSR): # devlink sb occupancy snapshot pci/0000:01:00.0 # devlink sb occupancy clearmax pci/0000:01:00.0 The register has two masks of 256 bits to denote on which ingress / egress ports the register should operate on. Spectrum-4 has more than 256 ports, so the register was extended by cited commit with a new 'port_page' field. However, when filling the register's payload, the driver specifies the ports as absolute numbers and not relative to the first port of the port page, resulting in memory corruptions [1]. Fix by specifying the ports relative to the first port of the port page. [1] BUG: KASAN: slab-use-after-free in mlxsw_sp_sb_occ_snapshot+0xb6d/0xbc0 Read of size 1 at addr ffff8881068cb00f by task devlink/1566 [...] Call Trace: <TASK> dump_stack_lvl+0xc6/0x120 print_report+0xce/0x670 kasan_report+0xd7/0x110 mlxsw_sp_sb_occ_snapshot+0xb6d/0xbc0 mlxsw_devlink_sb_occ_snapshot+0x75/0xb0 devlink_nl_sb_occ_snapshot_doit+0x1f9/0x2a0 genl_family_rcv_msg_doit+0x20c/0x300 genl_rcv_msg+0x567/0x800 netlink_rcv_skb+0x170/0x450 genl_rcv+0x2d/0x40 netlink_unicast+0x547/0x830 netlink_sendmsg+0x8d4/0xdb0 __sys_sendto+0x49b/0x510 __x64_sys_sendto+0xe5/0x1c0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f [...] Allocated by task 1: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 __kasan_kmalloc+0x8f/0xa0 copy_verifier_state+0xbc2/0xfb0 do_check_common+0x2c51/0xc7e0 bpf_check+0x5107/0x9960 bpf_prog_load+0xf0e/0x2690 __sys_bpf+0x1a61/0x49d0 __x64_sys_bpf+0x7d/0xc0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 1: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3b/0x60 poison_slab_object+0x109/0x170 __kasan_slab_free+0x14/0x30 kfree+0xca/0x2b0 free_verifier_state+0xce/0x270 do_check_common+0x4828/0xc7e0 bpf_check+0x5107/0x9960 bpf_prog_load+0xf0e/0x2690 __sys_bpf+0x1a61/0x49d0 __x64_sys_bpf+0x7d/0xc0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f	2024-07-29	5.5	CVE-2024-42073
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd: acp: add a null check for chip_pdev structure When acp platform device creation is skipped, chip->chip_pdev value will remain NULL. Add NULL check for chip->chip_pdev structure in snd_acp_resume() function to avoid null pointer dereference.	2024-07-29	5.5	CVE-2024-42074
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix remap of arena. The bpf arena logic didn't account for mremap operation. Add a refcnt for multiple mmap events to prevent use-after-free in arena_vm_close.	2024-07-29	5.5	CVE-2024-42075
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: can: j1939: Initialize unused data in j1939_send_one() syzbot reported kernel-infoleak in raw_recvmsg() [1]. j1939_send_one() creates full frame including unused data, but it doesn't initialize it. This causes the kernel-infoleak issue. Fix this by initializing	2024-07-29	5.5	CVE-2024-42076

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unused data. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in copy_to_user_iter lib/iov_iter.c:24 [inline] BUG: KMSAN: kernel-infoleak in iterate_ubuf include/linux/iov_iter.h:29 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance2 include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance include/linux/iov_iter.h:271 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 instrument_copy_to_user include/linux/instrumented.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline] iterate_ubuf include/linux/iov_iter.h:29 [inline] iterate_and_advance2 include/linux/iov_iter.h:245 [inline] iterate_and_advance include/linux/iov_iter.h:271 [inline] _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 copy_to_iter include/linux/uio.h:196 [inline] memcpy_to_msg include/linux/skbuff.h:4113 [inline] raw_recvmsg+0x2b8/0x9e0 net/can/raw.c:1008 sock_recvmsg_nosec net/socket.c:1046 [inline] sock_recvmsg+0x2c4/0x340 net/socket.c:1068 ____sys_recvmsg+0x18a/0x620 net/socket.c:2803 ___sys_recvmsg+0x223/0x840 net/socket.c:2845 do_recvmmsg+0x4fc/0xfd0 net/socket.c:2939 __sys_recvmmsg net/socket.c:3018 [inline] __do_sys_recvmmsg net/socket.c:3041 [inline] __se_sys_recvmmsg net/socket.c:3034 [inline] __x64_sys_recvmmsg+0x397/0x490 net/socket.c:3034 x64_sys_call+0xf6c/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:300 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3804 [inline] slab_alloc_node mm/slub.c:3845 [inline] kmem_cache_alloc_node+0x613/0xc50 mm/slub.c:3888 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:577 __alloc_skb+0x35b/0x7a0 net/core/skbuff.c:668 alloc_skb include/linux/skbuff.h:1313 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6504 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2795 sock_alloc_send_skb include/net/sock.h:1842 [inline] j1939_sk_alloc_skb net/can/j1939/socket.c:878 [inline] j1939_sk_send_loop net/can/j1939/socket.c:1142 [inline] j1939_sk_sendmsg+0xc0a/0x2730 net/can/j1939/socket.c:1277 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 ____sys_sendmsg+0x877/0xb60 net/socket.c:2584 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2638 __sys_sendmsg net/socket.c:2667 [inline] __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] __x64_sys_sendmsg+0x307/0x4a0 net/socket.c:2674 x64_sys_call+0xc4b/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Bytes 12-15 of 16 are uninitialized Memory access of size 16 starts at ffff888120969690 Data copied to user address 00000000200017c0 CPU: 1 PID: 5050 Comm: syz-executor198 Not tainted 6.9.0-rc5-syzkaller-00031-g71b1543c83d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix DIO failure due to insufficient transaction credits The code in ocfs2_dio_end_io_write() estimates number of necessary transaction credits using ocfs2_calc_extend_credits(). This however does not take into account that the IO could be arbitrarily large and can contain arbitrary number of extents. Extent tree manipulations do often extend the current transaction but not in all of the cases. For example if we have only single block extents in the tree, ocfs2_mark_extent_written() will end up calling ocfs2_replace_extent_rec() all the time and we will never extend the current transaction and eventually exhaust all the transaction credits if the IO contains many single block extents. Once that happens a WARN_ON(jbd2_handle_buffer_credits(handle) <= 0) is triggered in jbd2_journal_dirty_metadata() and subsequently OCFS2 aborts in response to this error. This was actually triggered by one of our customers on a heavily fragmented	2024-07-29	5.5	CVE-2024-42077

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	OCFS2 filesystem. To fix the issue make sure the transaction always has enough credits for one extent insert before each call of ocfs2_mark_extent_written(). Heming Zhao said: ------ PANIC: "Kernel panic - not syncing: OCFS2: (device dm-1): panic forced after error" PID: xxx TASK: xxxx CPU: 5 COMMAND: "SubmitThread-CA" #0 machine_kexec at ffffffff8c069932 #1 __crash_kexec at ffffffff8c1338fa #2 panic at ffffffff8c1d69b9 #3 ocfs2_handle_error at ffffffffc0c86c0c [ocfs2] #4 __ocfs2_abort at ffffffffc0c88387 [ocfs2] #5 ocfs2_journal_dirty at ffffffffc0c51e98 [ocfs2] #6 ocfs2_split_extent at ffffffffc0c27ea3 [ocfs2] #7 ocfs2_change_extent_flag at ffffffffc0c28053 [ocfs2] #8 ocfs2_mark_extent_written at ffffffffc0c28347 [ocfs2] #9 ocfs2_dio_end_io_write at ffffffffc0c2bef9 [ocfs2] #10 ocfs2_dio_end_io at ffffffffc0c2c0f5 [ocfs2] #11 dio_complete at ffffffff8c2b9fa7 #12 do_blockdev_direct_IO at ffffffff8c2bc09f #13 ocfs2_direct_IO at ffffffffc0c2b653 [ocfs2] #14 generic_file_direct_write at ffffffff8c1dcf14 #15 __generic_file_write_iter at ffffffff8c1dd07b #16 ocfs2_file_write_iter at ffffffffc0c49f1f [ocfs2] #17 aio_write at ffffffff8c2cc72e #18 kmem_cache_alloc at ffffffff8c248dde #19 do_io_submit at ffffffff8c2ccada #20 do_syscall_64 at ffffffff8c004984 #21 entry_SYSCALL_64_after_hwframe at ffffffff8c8000ba			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Wipe copies of clear-key structures on failure Wipe all sensitive data from stack for all IOCTLs, which convert a clear-key into a protected- or secure-key.	2024-07-30	4.1	CVE-2024-42156
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Wipe sensitive data on failure Wipe sensitive data from stack also if the copy_to_user() fails.	2024-07-30	4.1	CVE-2024-42157
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Use kfree_sensitive() to fix Coccinelle warnings Replace memzero_explicit() and kfree() with kfree_sensitive() to fix warnings reported by Coccinelle: WARNING opportunity for kfree_sensitive/kvfree_sensitive (line 1506) WARNING opportunity for kfree_sensitive/kvfree_sensitive (line 1643) WARNING opportunity for kfree_sensitive/kvfree_sensitive (line 1770)	2024-07-30	4.1	CVE-2024-42158
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: usb: xhci: prevent potential failure in handle_tx_event() for Transfer events without TRB Some transfer events don't always point to a TRB, and consequently don't have a endpoint ring. In these cases, function handle_tx_event() should not proceed, because if 'ep->skip' is set, the pointer to the endpoint ring is used. To prevent a potential failure and make the code logical, return after checking the completion code for a Transfer event without TRBs.	2024-07-30	4.6	CVE-2024-42226
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix overlapping copy within dml_core_mode_programming [WHY] &mode_lib->mp.Watermark and &locals->Watermark are the same address. memcpy may lead to unexpected behavior. [HOW] memmove should be used.	2024-07-30	4.7	CVE-2024-42227
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: aead,cipher - zeroize key buffer after use I.G 9.7.B for FIPS 140-3 specifies that variables temporarily holding cryptographic information should be zeroized once	2024-07-30	4.1	CVE-2024-42229

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	they are no longer needed. Accomplish this by using kfree_sensitive for buffers that previously held the private key.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: Fix scv instruction crash with kexec kexec on pseries disables AIL (reloc_on_exc), required for scv instruction support, before other CPUs have been shut down. This means they can execute scv instructions after AIL is disabled, which causes an interrupt at an unexpected entry location that crashes the kernel. Change the kexec sequence to disable AIL after other CPUs have been brought down. As a refresher, the real-mode scv interrupt vector is 0x17000, and the fixed-location head code probably couldn't easily deal with implementing such high addresses so it was just decided not to support that interrupt at all.	2024-07-30	4.4	CVE-2024-42230
LiquidPoll--LiquidPoll Advanced Polls for Creators and Brands	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in LiquidPoll LiquidPoll - Advanced Polls for Creators and Brands.This issue affects LiquidPoll - Advanced Polls for Creators and Brands: from n/a through 3.3.77.	2024-08-01	6.5	CVE-2024-39655
ManageEngine--Applications Manager	Zohocorp ManageEngine Applications Manager versions 170900 and below are vulnerable to the authenticated admin-only SQL Injection in the Create Monitor feature.	2024-08-01	4.7	CVE-2024-5678
Mashov--Mashov	Mashov - CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	2024-07-30	6.1	CVE-2024-41693
Matrix--Tafnit v8	Matrix - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2024-07-30	5.4	CVE-2024-38430
Matrix--Tafnit v8	Matrix Tafnit v8 - CWE-204: Observable Response Discrepancy	2024-07-30	5.3	CVE-2024-38431
Matrix--Tafnit v8	Matrix Tafnit v8 - CWE-646: Reliance on File Name or Extension of Externally-Supplied File	2024-07-30	5.5	CVE-2024-38432
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0, 9.5.x <= 9.5.6, 9.7.x <= 9.7.5, 9.8.x <= 9.8.1 fail to properly safeguard an error handling which allows a malicious remote to permanently delete local data by abusing dangerous error handling, when share channels were enabled.	2024-08-01	6.8	CVE-2024-39832
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0, 9.5.x <= 9.5.6, 9.7.x <= 9.7.5, 9.8.x <= 9.8.1 fail to properly validate synced posts, when shared channels are enabled, which allows a malicious remote to create/update/delete arbitrary posts in arbitrary channels	2024-08-01	5.5	CVE-2024-41144
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0, 9.5.x <= 9.5.6, 9.7.x <= 9.7.5, 9.8.x <= 9.8.1 fail to disallow users to set their own remote username, when shared channels were enabled, which allows a user on a remote to set their remote username prop to an arbitrary string, which would be then synced to the local server as long as the user hadn't been synced before.	2024-08-01	4.3	CVE-2024-39839
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0, 9.5.x <= 9.5.6, 9.7.x <= 9.7.5 and 9.8.x <= 9.8.1 fail to disallow the modification of local channels by a remote, when shared channels are enabled, which allows a malicious remote to make an arbitrary local channel read-only.	2024-08-01	4.1	CVE-2024-41162

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mkucej--i-librarian-free	I, Librarian is an open-source version of a PDF managing SaaS. PDF notes are displayed on the Item Summary page without any form of validation or sanitation. An attacker can exploit this vulnerability by inserting a payload in the PDF notes that contains malicious code or script. This code will then be executed when the page is loaded in the browser. The vulnerability was fixed in version 5.11.1.	2024-07-30	4.6	CVE-2024-41943
MobSF--Mobile-Security-Framework-MobSF	Mobile Security Framework (MobSF) is a security research platform for mobile applications in Android, iOS and Windows Mobile. An open redirect vulnerability exist in MobSF authentication view. Update to MobSF v4.0.5.	2024-07-31	5.2	CVE-2024-41955
Modernaweb Studio--Black Widgets For Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Modernaweb Studio Black Widgets For Elementor allows Stored XSS.This issue affects Black Widgets For Elementor: from n/a through 1.3.5.	2024-08-01	6.5	CVE-2024-39644
Modernaweb Studio--Black Widgets For Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Modernaweb Studio Black Widgets For Elementor allows Stored XSS.This issue affects Black Widgets For Elementor: from n/a through 1.3.5.	2024-08-01	6.5	CVE-2024-39662
MotoPress--Timetable and Event Schedule	Deserialization of Untrusted Data vulnerability in MotoPress Timetable and Event Schedule allows Object Injection.This issue affects Timetable and Event Schedule: from n/a through 2.4.13.	2024-08-01	5.5	CVE-2024-39630
motovnet--Ebook Store	The Ebook Store plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 5.8001. This is due to the plugin utilizing fpdi-protection and not preventing direct access to test files that have display_errors 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.	2024-08-02	5.3	CVE-2024-6567
n/a--Mp3tag	A vulnerability has been found in Mp3tag up to 3.26d and classified as problematic. This vulnerability affects unknown code in the library tak_deco_lib.dll of the component DLL Handler. The manipulation leads to uncontrolled search path. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. Upgrading to version 3.26e is able to address this issue. It is recommended to upgrade the affected component. VDB-272614 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early, responded in a very professional manner and immediately released a fixed version of the affected product.	2024-07-29	5.3	CVE-2024-7193
n/a--n/a	Cross Site Scripting vulnerability in Lost and Found Information System 1.0 allows a remote attacker to escalate privileges via the page parameter to php-lfis/admin/index.php.	2024-07-29	6.1	CVE-2024-37859
n/a--n/a	A heap buffer overflow in the function cp_stored() (/vendor/cute_png.h) of hicolor v0.5.0 allows attackers to cause a Denial of Service (DoS) via a crafted PNG file.	2024-07-30	6.2	CVE-2024-41438

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
n/a--n/a	A heap buffer overflow in the function png_quantize() of hicolor v0.5.0 allows attackers to cause a Denial of Service (DoS) via a crafted PNG file.	2024-07-30	6.2	CVE-2024-41440
n/a--n/a	Cross Site Scripting (XSS) vulnerability in AML Surety Eco up to 3.5 allows an attacker to run arbitrary code via crafted GET request using the id parameter.	2024-07-29	6.1	CVE-2024-41640
n/a--n/a	In the Elliptic package 6.5.6 for Node.js, EDDSA signature malleability occurs because there is a missing signature length check, and thus zero-valued bytes can be removed or appended.	2024-08-02	5.3	CVE-2024-42459
n/a--n/a	In the Elliptic package 6.5.6 for Node.js, ECDSA signature malleability occurs because there is a missing check for whether the leading bit of r and s is zero.	2024-08-02	5.3	CVE-2024-42460
n/a--n/a	Cross Site Scripting vulnerability in Best House Rental Management System 1.0 allows a remote attacker to execute arbitrary code via the "House No" and "Description" parameters in the houses page at the index.php component.	2024-07-29	4.7	CVE-2024-40576
n/a--YouDianCMS	A vulnerability, which was classified as critical, was found in YouDianCMS 7. Affected is an unknown function of the file /Public/ckeditor/plugins/multiimage/dialogs/image_upload.php. The manipulation of the argument files leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273252. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-31	6.3	CVE-2024-7329
n/a--YouDianCMS	A vulnerability has been found in YouDianCMS 7 and classified as critical. Affected by this vulnerability is the function curl_exec of the file /App/Core/Extend/Function/ydLib.php. The manipulation of the argument url leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273253 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-01	6.3	CVE-2024-7330
n/a--YouDianCMS	A vulnerability, which was classified as problematic, has been found in YouDianCMS 7. This issue affects some unknown processing of the file /t.php?action=phpinfo. The manipulation leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273251. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-31	5.3	CVE-2024-7328
OpenMage--magento-lts	Magento-lts is a long-term support alternative to Magento Community Edition (CE). This XSS vulnerability affects the design/header/welcome, design/header/logo_src, design/header/logo_src_small, and design/header/logo_alt system configs.They are intended to enable admins to set a text in the two cases, and to define an image url for the other two cases. But because of previously missing escaping allowed to input arbitrary html and as a consequence also arbitrary JavaScript. The problem is patched with Version 20.10.1 or higher.	2024-07-29	4.1	CVE-2024-41676

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
petesheppard84--Extensions for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in petesheppard84 Extensions for Elementor allows Stored XSS.This issue affects Extensions for Elementor: from n/a through 2.0.31.	2024-08-01	6.5	CVE-2024-39668
pickplugins--Gutenberg Blocks, Page Builder ComboBlocks	The Gutenberg Blocks, Page Builder - ComboBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the redirectURL parameter of the Date Countdown widget, in all versions up to, and including, 2.2.85a 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.	2024-08-01	6.4	CVE-2024-6346
pimcore--admin-ui-classic-bundle	Pimcore's Admin Classic Bundle provides a backend user interface for Pimcore. Navigating to `/admin/index/statistics` with a logged in Pimcore user exposes information about the Pimcore installation, PHP version, MYSQL version, installed bundles and all database tables and their row count in the system. This vulnerability is fixed in 1.5.2, 1.4.6, and 1.3.10.	2024-07-30	6.3	CVE-2024-41109
Pixelcurve--Edubin	Server Side Request Forgery (SSRF) vulnerability in Pixelcurve Edubin edubin.This issue affects Edubin: from n/a through 9.2.0.	2024-08-01	5.4	CVE-2024-39637
Plug&Track--Sensor Net Connect V2	A "CWE-352: Cross-Site Request Forgery (CSRF)" can be exploited by remote attackers to perform state-changing operations with administrative privileges by luring authenticated victims into visiting a malicious web page.	2024-07-31	6.6	CVE-2024-3083
Plug&Track--Sensor Net Connect V2	A "CWE-256: Plaintext Storage of a Password" affecting the administrative account allows an attacker with physical access to the machine to retrieve the password in cleartext.	2024-07-31	4.2	CVE-2024-3082
Plug&Track--Sensor Net Connect V2	A "CWE-201: Insertion of Sensitive Information Into Sent Data" affecting the administrative account allows an attacker with physical access to the machine to retrieve the password in cleartext when an administrative session is open in the browser.	2024-07-31	4.2	CVE-2024-31200
Plug&Track--Thermoscan IP	A "CWE-428: Unquoted Search Path or Element" affects the ThermoscanIP_Scrutation service. Such misconfiguration could be abused in scenarios where incorrect permissions were assigned to the C:\ path to attempt a privilege escalation on the local machine.	2024-07-31	6.5	CVE-2024-31201
Plug&Track--Thermoscan IP	A "CWE-121: Stack-based Buffer Overflow" in the wd210std.dll dynamic library packaged with the ThermoscanIP installer allows a local attacker to possibly trigger a Denial-of-Service (DoS) condition on the target component.	2024-07-31	4	CVE-2024-31203
pr-gateway--Blog2Social: Social Media Auto Post & Scheduler	The Blog2Social: Social Media Auto Post & Scheduler plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 3gp2 file uploads in all versions up to, and including, 7.5.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the 3gp2 file.	2024-08-01	6.4	CVE-2024-7302
Python Software Foundation--CPython	There is a MEDIUM severity vulnerability affecting CPython. The email module didn't properly quote newlines for email headers when serializing an email message allowing for header injection when an email is serialized.	2024-08-01	5.5	CVE-2024-6923

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Enterprise Linux 7	A flaw was found in Podman. This issue may allow an attacker to create a specially crafted container that, when configured to share the same IPC with at least one other container, can create a large number of IPC resources in /dev/shm. The malicious container will continue to exhaust resources until it is out-of-memory (OOM) killed. While the malicious container's cgroup will be removed, the IPC resources it created are not. Those resources are tied to the IPC namespace that will not be removed until all containers using it are stopped, and one non-malicious container is holding the namespace open. The malicious container is restarted, either automatically or by attacker control, repeating the process and increasing the amount of memory consumed. With a container configured to restart always, such as `podman run --restart=always`, this can result in a memory-based denial of service of the system.	2024-08-02	4.8	CVE-2024-3056
RegistrationMagic Forms--RegistrationMagic	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in RegistrationMagic Forms RegistrationMagic allows Stored XSS.This issue affects RegistrationMagic: from n/a through 6.0.0.1.	2024-08-01	5.8	CVE-2024-39643
ruby--rexml	REXML is an XML toolkit for Ruby. The REXML gem before 3.3.2 has some DoS vulnerabilities when it parses an XML that has many specific characters such as whitespace character, `>]` and `]>`. The REXML gem 3.3.3 or later include the patches to fix these vulnerabilities.	2024-08-01	5.3	CVE-2024-41123
ruby--rexml	REXML is an XML toolkit for Ruby. The REXML gem 3.3.2 has a DoS vulnerability when it parses an XML that has many entity expansions with SAX2 or pull parser API. The REXML gem 3.3.3 or later include the patch to fix the vulnerability.	2024-08-01	5.3	CVE-2024-41946
SimpleMachines--SMF	A vulnerability, which was classified as critical, was found in SimpleMachines SMF 2.1.4. Affected is an unknown function of the file /index.php?action=profile;u=2;area=showalerts;do=remove of the component Delete User Handler. The manipulation of the argument aid leads to improper control of resource identifiers. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-273522 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-03	5.4	CVE-2024-7437
SimpleMachines--SMF	A vulnerability has been found in SimpleMachines SMF 2.1.4 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /index.php?action=profile;u=2;area=showalerts;do=read of the component User Alert Read Status Handler. The manipulation of the argument aid leads to improper control of resource identifiers. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273523. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-03	4.3	CVE-2024-7438
SourceCodester--Complaints Report Management System	A vulnerability was found in SourceCodester Complaints Report Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/manage_complaint.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. VDB-272618 is the identifier assigned to this vulnerability.	2024-07-29	6.3	CVE-2024-7197
SourceCodester--Complaints Report Management	A vulnerability classified as critical has been found in SourceCodester Complaints Report Management System 1.0. This affects an unknown part of the file /admin/manage_station.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been	2024-07-29	6.3	CVE-2024-7198

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
System	disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272619.			
SourceCodester--Complaints Report Management System	A vulnerability classified as critical was found in SourceCodester Complaints Report Management System 1.0. This vulnerability affects unknown code of the file /admin/manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272620.	2024-07-29	6.3	CVE-2024-7199
SourceCodester--Establishment Billing Management System	A vulnerability was found in SourceCodester Establishment Billing Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /manage_user.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273156.	2024-07-31	6.3	CVE-2024-7287
SourceCodester--Establishment Billing Management System	A vulnerability was found in SourceCodester Establishment Billing Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=delete_block. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273157 was assigned to this vulnerability.	2024-07-31	6.3	CVE-2024-7288
SourceCodester--Establishment Billing Management System	A vulnerability was found in SourceCodester Establishment Billing Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /manage_payment.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. VDB-273158 is the identifier assigned to this vulnerability.	2024-07-31	6.3	CVE-2024-7289
SourceCodester--Establishment Billing Management System	A vulnerability classified as critical has been found in SourceCodester Establishment Billing Management System 1.0. This affects an unknown part of the file /manage_tenant.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273159.	2024-07-31	6.3	CVE-2024-7290
SourceCodester--Establishment Billing Management System	A vulnerability, which was classified as critical, was found in SourceCodester Establishment Billing Management System 1.0. Affected is an unknown function of the file /manage_block.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-273198 is the identifier assigned to this vulnerability.	2024-07-31	6.3	CVE-2024-7306
SourceCodester--Establishment Billing Management System	A vulnerability has been found in SourceCodester Establishment Billing Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /manage_billing.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273199.	2024-07-31	6.3	CVE-2024-7307
SourceCodester--Establishment Billing Management System	A vulnerability was found in SourceCodester Establishment Billing Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /view_bill.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. The identifier of this vulnerability is VDB-273200.	2024-07-31	6.3	CVE-2024-7308
SourceCodester--Lot Reservation Management	A vulnerability, which was classified as critical, was found in SourceCodester Lot Reservation Management System 1.0. Affected is an unknown function of the file /home.php. The manipulation of the argument type leads to sql injection. It is	2024-07-30	6.3	CVE-2024-7222

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
System	possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-272802 is the identifier assigned to this vulnerability.			
SourceCodester--Lot Reservation Management System	A vulnerability has been found in SourceCodester Lot Reservation Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /view_model.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272803.	2024-07-30	6.3	CVE-2024-7223
SourceCodester--Lot Reservation Management System	A vulnerability was found in SourceCodester Lot Reservation Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /lot_details.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. The identifier of this vulnerability is VDB-272804.	2024-07-30	6.3	CVE-2024-7224
SourceCodester--Lot Reservation Management System	A vulnerability was found in SourceCodester Lot Reservation Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/view_reserved.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273149 was assigned to this vulnerability.	2024-07-31	6.3	CVE-2024-7280
SourceCodester--Lot Reservation Management System	A vulnerability classified as critical has been found in SourceCodester Lot Reservation Management System 1.0. Affected is an unknown function of the file /admin/index.php?page=manage_lot. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-273150 is the identifier assigned to this vulnerability.	2024-07-31	6.3	CVE-2024-7281
SourceCodester--Lot Reservation Management System	A vulnerability classified as critical was found in SourceCodester Lot Reservation Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/manage_model.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273151.	2024-07-31	6.3	CVE-2024-7282
SourceCodester--Lot Reservation Management System	A vulnerability, which was classified as critical, has been found in SourceCodester Lot Reservation Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/manage_user.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. The identifier of this vulnerability is VDB-273152.	2024-07-31	6.3	CVE-2024-7283
SourceCodester--Medicine Tracker System	A vulnerability was found in SourceCodester Medicine Tracker System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /classes/Users.php?f=save_user of the component Password Change Handler. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-272806 is the identifier assigned to this vulnerability.	2024-07-30	4.3	CVE-2024-7226
SourceCodester--School Log Management System	A vulnerability classified as critical was found in SourceCodester School Log Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/print_barcode.php. The manipulation of the argument tbl leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-272791.	2024-07-30	6.3	CVE-2024-7220
SourceCodester--School Log	A vulnerability, which was classified as critical, has been found in SourceCodester School Log Management System 1.0. Affected by this issue is some unknown	2024-07-30	6.3	CVE-2024-7221

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	functionality of the file /admin/manage_user.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. The identifier of this vulnerability is VDB-272792.			
SourceCodester--Simple Realtime Quiz System	A vulnerability was found in SourceCodester Simple Realtime Quiz System 1.0. It has been classified as critical. Affected is an unknown function of the file /manage_quiz.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-273354 is the identifier assigned to this vulnerability.	2024-08-01	6.3	CVE-2024-7370
SourceCodester--Simple Realtime Quiz System	A vulnerability was found in SourceCodester Simple Realtime Quiz System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /quiz_view.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273355.	2024-08-01	6.3	CVE-2024-7371
SourceCodester--Simple Realtime Quiz System	A vulnerability was found in SourceCodester Simple Realtime Quiz System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /quiz_board.php. The manipulation of the argument quiz leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273356.	2024-08-02	6.3	CVE-2024-7372
SourceCodester--Simple Realtime Quiz System	A vulnerability classified as critical has been found in SourceCodester Simple Realtime Quiz System 1.0. This affects an unknown part of the file /ajax.php?action=load_answered. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273357 was assigned to this vulnerability.	2024-08-02	6.3	CVE-2024-7373
SourceCodester--Simple Realtime Quiz System	A vulnerability classified as critical was found in SourceCodester Simple Realtime Quiz System 1.0. This vulnerability affects unknown code of the file /manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273358 is the identifier assigned to this vulnerability.	2024-08-02	6.3	CVE-2024-7374
SourceCodester--Simple Realtime Quiz System	A vulnerability, which was classified as critical, has been found in SourceCodester Simple Realtime Quiz System 1.0. This issue affects some unknown processing of the file /my_quiz_result.php. The manipulation of the argument quiz leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273359.	2024-08-02	6.3	CVE-2024-7375
SourceCodester--Simple Realtime Quiz System	A vulnerability, which was classified as critical, was found in SourceCodester Simple Realtime Quiz System 1.0. Affected is an unknown function of the file /print_quiz_records.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273360.	2024-08-02	6.3	CVE-2024-7376
SourceCodester--Simple Realtime Quiz System	A vulnerability has been found in SourceCodester Simple Realtime Quiz System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /view_result.php. The manipulation of the argument qid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273361 was assigned to this vulnerability.	2024-08-02	6.3	CVE-2024-7377

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SourceCodester--Simple Realtime Quiz System	A vulnerability was found in SourceCodester Simple Realtime Quiz System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /manage_question.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. VDB-273362 is the identifier assigned to this vulnerability.	2024-08-02	6.3	CVE-2024-7378
SourceCodester--Simple Realtime Quiz System	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Realtime Quiz System 1.0. This affects an unknown part of the file /ajax.php?action=save_user. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273351.	2024-08-01	4.3	CVE-2024-7367
SourceCodester--Tracking Monitoring Management System	A vulnerability classified as critical was found in SourceCodester Tracking Monitoring Management System 1.0. This vulnerability affects unknown code of the file /ajax.php?action=save_establishment. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273340.	2024-08-01	6.3	CVE-2024-7361
SourceCodester--Tracking Monitoring Management System	A vulnerability, which was classified as critical, has been found in SourceCodester Tracking Monitoring Management System 1.0. This issue affects some unknown processing of the file /manage_user.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273341 was assigned to this vulnerability.	2024-08-01	6.3	CVE-2024-7362
SourceCodester--Tracking Monitoring Management System	A vulnerability, which was classified as critical, was found in SourceCodester Tracking Monitoring Management System 1.0. Affected is an unknown function of the file /manage_person.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-273342 is the identifier assigned to this vulnerability.	2024-08-01	6.3	CVE-2024-7363
SourceCodester--Tracking Monitoring Management System	A vulnerability has been found in SourceCodester Tracking Monitoring Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /manage_records.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-273343.	2024-08-01	6.3	CVE-2024-7364
SourceCodester--Tracking Monitoring Management System	A vulnerability was found in SourceCodester Tracking Monitoring Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /manage_establishment.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. The identifier of this vulnerability is VDB-273344.	2024-08-01	6.3	CVE-2024-7365
SourceCodester--Tracking Monitoring Management System	A vulnerability classified as problematic has been found in SourceCodester Tracking Monitoring Management System 1.0. This affects an unknown part of the file /ajax.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. The associated identifier of this vulnerability is VDB-273339.	2024-08-01	4.3	CVE-2024-7360
strategy11team--Formidable Forms Contact Form Plugin, Survey, Quiz, Payment,	The Formidable Forms - Contact Form Plugin, Survey, Quiz, Payment, Calculator Form & Custom Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'html' parameter in all versions up to, and including, 6.11.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with form editing permissions and Subscriber-level access	2024-07-31	4.9	CVE-2024-6725

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Calculator Form & Custom Form Builder	and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
takanakui--WP Mobile Menu The Mobile-Friendly Responsive Menu	The WP Mobile Menu plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_menu_item_icon function in all versions up to, and including, 2.8.4.4. This makes it possible for unauthenticated attackers to add the '_mobmenu_icon' post meta to arbitrary posts with an arbitrary (but sanitized) value. NOTE: Version 2.8.4.4 contains a partial fix for this vulnerability.	2024-07-31	5.3	CVE-2024-2508
templatespare--TemplateSpare: Quick & Easy WordPress Site Builder 475+ Ready-Made Demos for News, Blogs, eCommerce, and More. One-Click Import, No Coding Needed	The Build Your Dream Website Fast with 400+ Starter Templates and Landing Pages, No Coding Needed, One-Click Import for Elementor & Gutenberg Blocks! - TemplateSpare plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'templatespare_activate_required_theme' and 'templatespare_get_theme_status' functions in all versions up to, and including, 2.4.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to activate any installed theme and read any theme status. If the attacker attempts to activate a theme that is not installed, a non-existent theme with the slug chosen by the attacker will be considered the active theme, leaving the site with no theme functionality.	2024-08-03	4.3	CVE-2024-6872
ThemeGrill--Himalayas	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeGrill Himalayas allows Stored XSS.This issue affects Himalayas: from n/a through 1.3.2.	2024-08-01	5.9	CVE-2024-39629
Themewinter--Eventin	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themewinter Eventin allows Stored XSS.This issue affects Eventin: from n/a through 4.0.5.	2024-08-01	5.9	CVE-2024-39648
TOTOLINK--A3600R	A vulnerability has been found in TOTOLINK A3600R 4.1.2cu.5182_B20201102 and classified as critical. This vulnerability affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ipDoamin leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272596. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	6.3	CVE-2024-7175
TOTOLINK--A3600R	A vulnerability classified as critical was found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. This vulnerability affects the function setTelnetCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument telnet_enabled leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-272602 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-29	6.3	CVE-2024-7181
TOTOLINK--CA300-PoE	A vulnerability was found in TOTOLINK CA300-PoE 6.2c.884. It has been declared as critical. This vulnerability affects the function loginauth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272788. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-30	6.3	CVE-2024-7217
TOTOLINK--LR1200	A vulnerability was found in TOTOLINK LR1200 9.3.1cu.2832 and classified as critical. Affected by this issue is the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument host_time leads to command injection. The attack may be launched remotely. The exploit has been disclosed to	2024-07-30	6.3	CVE-2024-7215

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the public and may be used. VDB-272786 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			
TOTOLINK--LR350	A vulnerability has been found in TOTOLINK LR350 9.3.5u.6369_B20220309 and classified as critical. Affected by this vulnerability is the function setWanCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272785 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-30	6.3	CVE-2024-7214
TVT--DVR TD-2104TS-CL	A vulnerability has been found in TVT DVR TD-2104TS-CL, DVR TD-2108TS-HP, Provision-ISR DVR SH-4050A5-5L(MM) and AVISION DVR AV108T and classified as problematic. This vulnerability affects unknown code of the file /queryDevInfo. The manipulation leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273262 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-01	5.3	CVE-2024-7339
twisted--twisted	Twisted is an event-based framework for internet applications, supporting Python 3.6+. The `twisted.web.util.redirectTo` function contains an HTML injection vulnerability. If application code allows an attacker to control the redirect URL this vulnerability may result in Reflected Cross-Site Scripting (XSS) in the redirect response HTML body. This vulnerability is fixed in 24.7.0rc1.	2024-07-29	6.1	CVE-2024-41810
Unknown--Donation Block For PayPal	The Donation Block For PayPal WordPress plugin through 2.1.0 does not sanitise and escape form submissions, leading to a stored cross-site scripting vulnerability	2024-07-30	6.8	CVE-2024-6021
Unknown--Email Encoder	The Email Encoder WordPress plugin before 2.2.2 does not escape the WP_Email_Encoder_Bundle_options[protection_text] parameter before outputting it back in an attribute in an admin page, leading to a Stored Cross-Site Scripting	2024-07-29	5.4	CVE-2024-4483
Unknown--Essential Blocks	The Essential Blocks WordPress plugin before 4.7.0 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	2024-08-02	5.4	CVE-2024-5595
Unknown--Floating Notification Bar, Sticky Menu on Scroll, Announcement Banner, and Sticky Header for Any Theme	The Floating Notification Bar, Sticky Menu on Scroll, Announcement Banner, and Sticky Header for Any WordPress plugin before 2.7.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	2024-08-01	4.8	CVE-2024-4090
Unknown--FormFlow: WhatsApp Social and Advanced Form Builder with Easy Lead Collection	The FormFlow: WhatsApp Social and Advanced Form Builder with Easy Lead Collection WordPress plugin before 2.12.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2024-07-30	5.9	CVE-2024-3113

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Unknown--HTML Forms	The HTML Forms WordPress plugin before 1.3.34 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks	2024-07-31	6.5	CVE-2024-6412
Unknown--Inline Related Posts	The Inline Related Posts WordPress plugin before 3.8.0 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)	2024-07-29	5.9	CVE-2024-6487
Unknown--pmpro-member-directory	The pmpro-member-directory WordPress plugin before 1.2.6 does not prevent users with at least the contributor role from leaking other users' sensitive information, including password hashes.	2024-07-30	6.5	CVE-2024-1287
Unknown--pmpro-membership-maps	The pmpro-membership-maps WordPress plugin before 0.7 does not prevent users with at least the contributor role from leaking sensitive information about users with a membership on the site.	2024-07-30	6.5	CVE-2024-1286
Unknown--Responsive Tabs	The Responsive Tabs WordPress plugin through 4.0.8 does not sanitise and escape some of its Tab settings, which could allow high privilege users such as Contributors and above to perform Stored Cross-Site Scripting attacks	2024-07-30	5.9	CVE-2024-4096
Unknown--Send email only on Reply to My Comment	The Send email only on Reply to My Comment WordPress plugin through 1.0.6 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	2024-07-30	6.1	CVE-2024-6223
Unknown--Send email only on Reply to My Comment	The Send email only on Reply to My Comment WordPress plugin through 1.0.6 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	2024-07-30	5.9	CVE-2024-6224
Unknown--Slider by 10Web	The Slider by 10Web WordPress plugin before 1.2.57 does not sanitise and escape its Slider Title, which could allow high privilege users such as editors and above to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	2024-07-31	5.4	CVE-2024-6408
Unknown--socialdriver-framework	The socialdriver-framework WordPress plugin before 2024.04.30 does not sanitise and escape some of its settings, which could allow high privilege users such as contributor to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2024-08-01	4.8	CVE-2024-2872
Unknown--SpiderContacts	The SpiderContacts WordPress plugin through 1.1.7 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	2024-07-31	6.1	CVE-2024-6272
Unknown--Ultimate Blocks	The Ultimate Blocks WordPress plugin before 3.2.0 does not validate and escape some of its post-grid block attributes before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	2024-07-29	4.6	CVE-2024-6362
Unknown--Ultimate Classified Listings	The Ultimate Classified Listings WordPress plugin before 1.3 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	2024-07-29	4.7	CVE-2024-5883
Unknown--WANotifier	The WANotifier WordPress plugin before 2.6.1 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)	2024-07-31	4.8	CVE-2024-6165

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Unknown--Web Directory Free	The Web Directory Free WordPress plugin before 1.7.2 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	2024-07-30	6.8	CVE-2024-3669
Unknown--WooCommerce Customers Manager	The WooCommerce Customers Manager WordPress plugin before 30.2 does not have authorisation and CSRF in various AJAX actions, allowing any authenticated users, such as subscriber, to call them and update/delete/create customer metadata, also leading to Stored Cross-Site Scripting due to the lack of escaping of said metadata values.	2024-08-01	6.5	CVE-2024-1747
Unknown--WP Ajax Contact Form	The WP Ajax Contact Form WordPress plugin through 2.2.2 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 admin users	2024-07-30	6.1	CVE-2024-5809
Unknown--WP Ajax Contact Form	The WP Ajax Contact Form WordPress plugin through 2.2.2 does not have CSRF check in place when deleting emails from the email list, which could allow attackers to make a logged in admin perform such action via a CSRF attack	2024-07-30	4.3	CVE-2024-5808
Unknown--wp-affiliate-platform	The wp-affiliate-platform WordPress plugin before 6.5.2 does not have CSRF check in place when deleting affiliates, which could allow attackers to make a logged in user change delete them via a CSRF attack	2024-07-29	5.5	CVE-2024-5285
Unknown--WpStickyBar	The WpStickyBar WordPress plugin through 2.1.0 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	2024-07-30	6.1	CVE-2024-6226
vim--vim	Vim is an open source command line text editor. Vim < v9.1.0647 has double free in src/alloc.c:616. When closing a window, the corresponding tagstack data will be cleared and freed. However a bit later, the quickfix list belonging to that window will also be cleared and if that quickfix list points to the same tagstack data, Vim will try to free it again, resulting in a double-free/use-after-free access exception. Impact is low since the user must intentionally execute vim with several non-default flags, but it may cause a crash of Vim. The issue has been fixed as of Vim patch v9.1.0647	2024-08-01	4.5	CVE-2024-41957
vim--vim	Vim is an open source command line text editor. double-free in dialog_changed() in Vim < v9.1.0648. When abandoning a buffer, Vim may ask the user what to do with the modified buffer. If the user wants the changed buffer to be saved, Vim may create a new Untitled file, if the buffer did not have a name yet. However, when setting the buffer name to Unnamed, Vim will falsely free a pointer twice, leading to a double-free and possibly later to a heap-use-after-free, which can lead to a crash. The issue has been fixed as of Vim patch v9.1.0648.	2024-08-01	4.2	CVE-2024-41965
Webangon--The Pack Elementor addons	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Webangon The Pack Elementor addons allows PHP Local File Inclusion, Path Traversal.This issue affects The Pack Elementor addons: from n/a through 2.0.8.6.	2024-08-01	4.3	CVE-2024-38768
WPDeveloper--Essential Addons for Elementor	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloper Essential Addons for Elementor allows Stored XSS.This issue affects Essential Addons for Elementor: from n/a through 5.9.26.	2024-08-01	6.5	CVE-2024-39649
xibosignage--xibo-cms	Xibo is a content management system (CMS). An SQL injection vulnerability was discovered in the API route inside the CMS responsible for Adding/Editing DataSet Column Formulas. This allows an authenticated user to to obtain and modify arbitrary data from the Xibo database by injecting specially crafted values in to the `formula` parameter. Users should upgrade to version 3.3.12 or 4.0.14 which fix this issue.	2024-07-30	6.5	CVE-2024-41804

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xibosignage--xibo-cms	Xibo is a content management system (CMS). An SQL injection vulnerability was discovered in the `report/data/proofofplayReport` API route inside the CMS. This allows an authenticated user to to obtain and modify arbitrary data from the Xibo database by injecting specially crafted values in to the `sortBy` parameter. Users should upgrade to version 3.3.12 or 4.0.14 which fix this issue.	2024-07-30	6.5	CVE-2024-41944
xibosignage--xibo-cms	Xibo is a content management system (CMS). An SQL injection vulnerability was discovered in the API routes inside the CMS responsible for Filtering DataSets. This allows an authenticated user to to obtain arbitrary data from the Xibo database by injecting specially crafted values in to the API for viewing DataSet data. Users should upgrade to version 3.3.12 or 4.0.14 which fix this issue.	2024-07-30	4.9	CVE-2024-41803
Xinhu--RockOA	A vulnerability classified as critical was found in Xinhu RockOA 2.6.2. This vulnerability affects the function dataAction of the file /webmain/task/openapi/openmodhetongAction.php. The manipulation of the argument nickName leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273250 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-31	6.3	CVE-2024-7327
xwiki--xwiki-platform	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. When uploading an attachment with a malicious filename, malicious JavaScript code could be executed. This requires a social engineering attack to get the victim into uploading a file with a malicious name. The malicious code is solely executed during the upload and affects only the user uploading the attachment. While this allows performing actions in the name of that user, it seems unlikely that a user wouldn't notice the malicious filename while uploading the attachment. This has been patched in XWiki 14.10.21, 15.5.5, 15.10.6 and 16.0.0.	2024-07-31	6.4	CVE-2024-37900
xwiki--xwiki-platform	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. When a user has view but not edit right on a page in XWiki, that user can delete the page and replace it by a page with new content without having delete right. The previous version of the page is moved into the recycle bin and can be restored from there by an admin. As the user is recorded as deleter, the user would in theory also be able to view the deleted content, but this is not directly possible as rights of the previous version are transferred to the new page and thus the user still doesn't have view right on the page. It therefore doesn't seem to be possible to exploit this to gain any rights. This has been patched in XWiki 14.10.21, 15.5.5 and 15.10.6 by cancelling save operations by users when a new document shall be saved despite the document's existing already.	2024-07-31	4.3	CVE-2024-37898
YMC--Filter & Grids	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in YMC Filter & Grids allows Stored XSS.This issue affects Filter & Grids: from n/a through 2.9.2.	2024-08-01	6.5	CVE-2024-39665
Yonle--bostr	Bostr is an nostr relay aggregator proxy that acts like a regular nostr relay. bostr let everyone in even having authorized_keys being set when noscraper is set to true. This vulnerability is fixed in 3.0.10.	2024-08-01	4.6	CVE-2024-41962
zitadel--zitadel	Zitadel is an open source identity management system. ZITADEL administrators can enable a setting called "Ignoring unknown usernames" which helps mitigate attacks that try to guess/enumerate usernames. If enabled, ZITADEL will show the password prompt even if the user doesn't exist and report "Username or Password invalid". Due to a implementation change to prevent deadlocks calling the database, the flag would not be correctly respected in all cases and an attacker would gain information if an account exist within ZITADEL, since the error message	2024-07-31	5.3	CVE-2024-41952

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	shows "object not found" instead of the generic error message. This vulnerability is fixed in 2.58.1, 2.57.1, 2.56.2, 2.55.5, 2.54.8, and 2.53.9.			
zitadel--zitadel	Zitadel is an open source identity management system. ZITADEL uses HTML for emails and renders certain information such as usernames dynamically. That information can be entered by users or administrators. Due to a missing output sanitization, these emails could include malicious code. This may potentially lead to a threat where an attacker, without privileges, could send out altered notifications that are part of the registration processes. An attacker could create a malicious link, where the injected code would be rendered as part of the email. On the user's detail page, the username was also not sanitized and would also render HTML, giving an attacker the same vulnerability. While it was possible to inject HTML including javascript, the execution of such scripts would be prevented by most email clients and the Content Security Policy in Console UI. This vulnerability is fixed in 2.58.1, 2.57.1, 2.56.2, 2.55.5, 2.54.8 2.53.9, and 2.52.3.	2024-07-31	4.3	CVE-2024-41953
10web -- slider	The Slider by 10Web WordPress plugin before 1.2.56 does not sanitise and escape some of its Slide options, which could allow authenticated users with access to the Sliders (by default Administrator, however this can be changed via the Slider by 10Web WordPress plugin before 1.2.56's options) and the ability to add images (Editor+) to perform Stored Cross-Site Scripting attacks	2024-07-11	5.4	CVE-2024-6026
Adobe--Bridge	Bridge versions 14.0.4, 13.0.7, 14.1 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.	2024-07-09	5.5	CVE-2024-34140
amandato--PowerPress Podcasting plugin by Blubrry	The PowerPress Podcasting plugin by Blubrry plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'media_url' parameter in all versions up to, and including, 11.9.10 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.	2024-07-12	6.4	CVE-2024-6588
apache -- nifi	Apache NiFi 1.10.0 through 1.26.0 and 2.0.0-M1 through 2.0.0-M3 support a description field in the Parameter Context configuration that is vulnerable to cross-site scripting. An authenticated user, authorized to configure a Parameter Context, can enter arbitrary JavaScript code, which the client browser will execute within the session context of the authenticated user. Upgrading to Apache NiFi 1.27.0 or 2.0.0-M4 is the recommended mitigation.	2024-07-08	5.4	CVE-2024-37389
aprokopenko--Just Custom Fields	The Just Custom Fields plugin for WordPress is vulnerable to unauthorized access of functionality due to a missing capability check on several AJAX functions in all versions up to, and including, 3.3.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to invoke this functionality intended for admin users. This enables subscribers to manage field groups, change visibility of items among other things.	2024-07-09	4.3	CVE-2024-6167

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aprokopenko--Just Custom Fields	The Just Custom Fields plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.3.2. This is due to missing or incorrect nonce validation on several AJAX function. This makes it possible for unauthenticated attackers to invoke this functionality intended for admin users via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This enables subscribers to manage field groups, change visibility of items among other things.	2024-07-09	4.3	CVE-2024-6168
aumkub--Featured Image Generator	The Featured Image Generator plugin for WordPress is vulnerable to unauthorized image upload due to a missing capability check on the fig_save_after_generate_image function in all versions up to, and including, 1.3.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary images to a post-related gallery.	2024-07-10	4.3	CVE-2024-5677
auth0--Login by Auth0	The Login by Auth0 plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'wle' parameter in all versions up to, and including, 4.6.0 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.	2024-07-10	6.1	CVE-2023-6813
AWSM Innovations--AWSM Team	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in AWSM Innovations AWSM Team allows Path Traversal.This issue affects AWSM Team: from n/a through 1.3.1.	2024-07-09	6.5	CVE-2024-37454
ays-pro --secure_copy_content_protection_and_content_locking	The Secure Copy Content Protection and Content Locking WordPress plugin before 4.0.9 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).	2024-07-11	4.8	CVE-2024-6138
bastho--Event post	The Event post plugin for WordPress is vulnerable to unauthorized bulk metadata update due to a missing nonce check on the save_bulkdatas function in all versions up to, and including, 5.9.5. This makes it possible for unauthenticated attackers to update post_meta_data via a forged request, granted they can trick a logged-in user into performing an action such as clicking on a link.	2024-07-12	4.3	CVE-2024-1375
Beaver Addons--PowerPack Lite for Beaver Builder	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Beaver Addons PowerPack Lite for Beaver Builder allows Path Traversal.This issue affects PowerPack Lite for Beaver Builder: from n/a through 1.3.0.3.	2024-07-09	4.9	CVE-2024-37410
bible_text_project -- bible_text	The Bible Text WordPress plugin through 0.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	2024-07-11	5.4	CVE-2024-5444
BinaryCarpenter--Ultimate Custom Add To Cart Button (Ajax) For WooCommerce by Binary Carpenter	Missing Authorization vulnerability in BinaryCarpenter Ultimate Custom Add To Cart Button (Ajax) For WooCommerce by Binary Carpenter allows Cross-Site Scripting (XSS).This issue affects Ultimate Custom Add To Cart Button (Ajax) For WooCommerce by Binary Carpenter: from n/a through 1.222.16.	2024-07-12	6.5	CVE-2024-37202
Blue Plugins--Events Calendar for Google	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Blue Plugins Events Calendar for Google allows PHP Local File Inclusion.This issue affects Events Calendar for Google: from n/a through 2.1.0.	2024-07-12	6.5	CVE-2024-38716

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bobbingwide--oik	The oik plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's bw_button shortcode in all versions up to, and including, 4.10.3 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.	2024-07-09	6.4	CVE-2024-6391
Bootstrap--Bootstrap	A vulnerability has been identified in Bootstrap that exposes users to Cross-Site Scripting (XSS) attacks. The issue is present in the carousel component, where the data-slide and data-slide-to attributes can be exploited through the href attribute of an <a> tag due to inadequate sanitization. This vulnerability could potentially enable attackers to execute arbitrary JavaScript within the victim's browser.	2024-07-11	6.4	CVE-2024-6484 36c7be3b-2937-45df-85ea-ca7133ea542c
Bootstrap--Bootstrap	A security vulnerability has been discovered in bootstrap that could enable Cross-Site Scripting (XSS) attacks. The vulnerability is associated with the data-loading-text attribute within the button plugin. This vulnerability can be exploited by injecting malicious JavaScript code into the attribute, which would then be executed when the button's loading state is triggered.	2024-07-11	6.4	CVE-2024-6485 36c7be3b-2937-45df-85ea-ca7133ea542c
Bootstrap--Bootstrap	A vulnerability has been identified in Bootstrap that exposes users to Cross-Site Scripting (XSS) attacks. The issue is present in the carousel component, where the data-slide and data-slide-to attributes can be exploited through the href attribute of an <a> tag due to inadequate sanitization. This vulnerability could potentially enable attackers to execute arbitrary JavaScript within the victim's browser.	2024-07-11	6.4	CVE-2024-6531 36c7be3b-2937-45df-85ea-ca7133ea542c
Checkmk GmbH--Checkmk	Certain http endpoints of Checkmk in Checkmk < 2.3.0p10 < 2.2.0p31, < 2.1.0p46, <= 2.0.0p39 allows remote attacker to bypass authentication and access data	2024-07-08	5.3	CVE-2024-6163
Cisco--Cisco IOS XR Software	A vulnerability in the boot process of Cisco IOS XR Software could allow an authenticated, local attacker with high privileges to bypass the Cisco Secure Boot functionality and load unverified software on an affected device. To exploit this successfully, the attacker must have root-system privileges on the affected device. This vulnerability is due to an error in the software build process. An attacker could exploit this vulnerability by manipulating the system’s configuration options to bypass some of the integrity checks that are performed during the booting process. A successful exploit could allow the attacker to control the boot configuration, which could enable them to bypass of the requirement to run Cisco signed images or alter the security properties of the running system.	2024-07-10	6.7	CVE-2024-20456
cliengo--Cliengo Chatbot	The Cliengo - Chatbot plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_chatbot_token' and 'update_chatbot_position' functions in all versions up to, and including, 3.0.1. This makes it possible for unauthenticated attackers to change chatbot settings, which can lead to unavailability or other changes to the chatbot.	2024-07-09	6.5	CVE-2024-5992
cliengo--Cliengo Chatbot	The Cliengo - Chatbot plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'update_session' function in all versions up to, and including, 3.0.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update the session token of the chatbot.	2024-07-09	5.4	CVE-2024-5993
codersaiful--UltraAddons Elementor Addons (Header Footer Builder, Custom Font, Custom CSS,Woo Widget, Menu Builder,	The UltraAddons - Elementor Addons (Header Footer Builder, Custom Font, Custom CSS,Woo Widget, Menu Builder, Anywhere Elementor Shortcode) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 1.1.6 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.	2024-07-10	6.4	CVE-2024-4866

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Anywhere Elementor Shortcode)				
Cog-Creators--Red-DiscordBot	Red is a fully modular Discord bot. Due to a bug in Red's Core API, 3rd-party cogs using the `@commands.can_manage_channel()` command permission check without additional permission controls may authorize a user to run a command even when that user doesn't have permissions to manage a channel. None of the core commands or core cogs are affected. The maintainers of the project are not aware of any _public_ 3rd-party cog utilizing this API at the time of writing this advisory. The problem was patched and released in version 3.5.10.	2024-07-11	5.3	CVE-2024-39905
decidim--decidim	Decidim is a participatory democracy framework, written in Ruby on Rails, originally developed for the Barcelona City government online and offline participation website. If an attacker can infer the slug or URL of an unpublished or private resource, and this resource can be embbeded (such as a Participatory Process, an Assembly, a Proposal, a Result, etc), then some data of this resource could be accessed. This vulnerability is fixed in 0.27.6.	2024-07-10	5.3	CVE-2024-27090
decidim--decidim	Decidim is a participatory democracy framework. The admin panel is subject to potential XSS attach in case the attacker manages to modify some records being uploaded to the server. This vulnerability is fixed in 0.27.6 and 0.28.1.	2024-07-10	5.4	CVE-2024-27095
Dell--Alienware Command Center (AWCC)	Dell Alienware Command Center, version 5.7.3.0 and prior, contains an improper access control vulnerability. A low privileged attacker could potentially exploit this vulnerability, leading to denial of service on the local system and information disclosure.	2024-07-10	6.7	CVE-2024-38301
Dell--PowerSwitch Z9664F-ON BIOS	Dell Edge Gateway BIOS, versions 3200 and 5200, contains an out-of-bounds write vulnerability. A local authenticated malicious user with high privileges could potentially exploit this vulnerability leading to exposure of some UEFI code, leading to arbitrary code execution or escalation of privilege.	2024-07-10	5.7	CVE-2023-32467
Dell--PowerSwitch Z9664F-ON BIOS	Dell Edge Gateway BIOS, versions 3200 and 5200, contains an out-of-bounds write vulnerability. A local authenticated malicious user with high privileges could potentially exploit this vulnerability leading to exposure of some code in System Management Mode, leading to arbitrary code execution or escalation of privilege.	2024-07-10	5.7	CVE-2023-32472
directus--directus	Directus is a real-time API and App dashboard for managing SQL database content. Directus >=9.23.0, <=v10.5.3 improperly handles _in, _nin operators. It evaluates empty arrays as valid so expressions like {"role": {"_in": $CURRENT_USER.some_field}} would evaluate to true allowing the request to pass. This results in Broken Access Control because the rule fails to do what it was intended to do: Pass rule if **field** matches any of the **values**. This vulnerability is fixed in 10.6.0.	2024-07-08	6.3	CVE-2024-39701
directus--directus	Directus is a real-time API and App dashboard for managing SQL database content. A denial of service (DoS) attack by field duplication in GraphQL is a type of attack where an attacker exploits the flexibility of GraphQL to overwhelm a server by requesting the same field multiple times in a single query. This can cause the server to perform redundant computations and consume excessive resources, leading to a denial of service for legitimate users. Request to the endpoint /graphql are sent when visualizing graphs generated at a dashboard. By modifying the data sent and duplicating many times the fields a DoS attack is possible. This vulnerability is fixed in 10.12.0.	2024-07-08	6.5	CVE-2024-39895
dj-extensions -- dj-helpfularticles	XSS vulnerability in DJ-HelpfulArticles component for Joomla.	2024-07-09	6.1	CVE-2024-27183 security@joomla.org

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
docker -- desktop	In Docker Desktop on Windows before v4.31.0Â allows a user in the docker-usersÂ group to cause a Windows Denial-of-Service through the exec-pathÂ Docker daemon config option in Windows containers mode.	2024-07-09	5.5	CVE-2024-5652 security@docker.com
dotcamp -- ultimate_blocks	The Ultimate Blocks WordPress plugin before 3.1.9 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	2024-07-11	5.4	CVE-2024-4655
DynamicWebLab--WordPress Team Manager	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in DynamicWebLab WordPress Team Manager allows PHP Local File Inclusion.This issue affects WordPress Team Manager: from n/a through 2.1.12.	2024-07-12	6.5	CVE-2024-38704
Elementor--Elementor Website Builder	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Elementor Elementor Website Builder allows Cross-Site Scripting (XSS), Stored XSS.This issue affects Elementor Website Builder: from n/a through 3.22.1.	2024-07-09	5.5	CVE-2024-37437
elfsight--Pricing Table	The Pricing Table plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.1. This is due to missing or incorrect nonce validation on the ajax() function. This makes it possible for unauthenticated attackers to perform a variety of actions related to managing pricing tables via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2024-07-09	5.3	CVE-2024-4100
elfsight--Pricing Table	The Pricing Table plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the ajax() function in all versions up to, and including, 2.0.1. This makes it possible for authenticated attackers, with subscriber-level access and above, to perform unauthorized actions like editing pricing tables.	2024-07-09	5.4	CVE-2024-4102
exiv2 -- exiv2	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 version v0.28.2. The vulnerability is in the parser for the ASF video format, which was a new feature in v0.28.0. The out-of-bounds read is triggered when Exiv2 is used to read the metadata of a crafted video file. The bug is fixed in version v0.28.3.	2024-07-08	6.5	CVE-2024-39695
expresstech -- quiz_and_survey_master	The Quiz and Survey Master (QSM) WordPress plugin before 9.0.5 does not sanitise and escape some of its Quiz settings, which could allow contributors and higher to perform Stored Cross-Site Scripting attacks	2024-07-11	5.4	CVE-2024-6025
ExS--ExS Widgets	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ExS ExS Widgets allows PHP Local File Inclusion.This issue affects ExS Widgets: from n/a through 0.3.1.	2024-07-12	6.5	CVE-2024-38715
FOGProject--fogproject	FOG is a free open-source cloning/imaging/rescue suite/inventory management system. There is a security issue with the NFS configuration in /etc/exports generated by the installer that allows an attacker to modify files outside the export in the default installation. The exports have the no_subtree_check option. The no_subtree_check option means that if a client performs a file operation, the server will only check if the requested file is on the correct filesystem, not if it is in the correct directory. This enables modifying files in /images, accessing other files on the same filesystem, and accessing files on other filesystems. This vulnerability is fixed in 1.5.10.30.	2024-07-12	6.4	CVE-2024-39916
Fortinet--FortiADC	An improper certificate validation vulnerability [CWE-295] in FortiADC 7.4.0, 7.2 all versions, 7.1 all versions, 7.0 all versions may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and public SDN connectors.	2024-07-09	4.8	CVE-2023-50179

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Fortinet--FortiADC	An improper access control vulnerability [CWE-284] in Fortinet FortiADC version 7.4.0 through 7.4.1 and before 7.2.4 allows a read only authenticated attacker to perform some write actions via crafted HTTP or HTTPS requests.	2024-07-09	4.9	CVE-2023-50181
Fortinet--FortiAIOps	An improper neutralization of formula elements in a CSV File vulnerability [CWE-1236] in FortiAIOps version 2.0.0 may allow a remote authenticated attacker to execute arbitrary commands on a client's workstation via poisoned CSV reports.	2024-07-09	5.4	CVE-2024-27785
Fortinet--FortiPortal	An authorization bypass through user-controlled key in Fortinet FortiPortal version 7.2.0, and versions 7.0.0 through 7.0.6 allows attacker to view unauthorized resources via HTTP or HTTPS requests.	2024-07-09	4.3	CVE-2024-21759
Fortinet--FortiWeb	An improper certificate validation vulnerability [CWE-295] in FortiWeb 7.2.0 through 7.2.1, 7.0 all versions, 6.4 all versions and 6.3 all versions may allow a remote and unauthenticated attacker in a Man-in-the-Middle position to decipher and/or tamper with the communication channel between the device and different endpoints used to fetch data for Web Application Firewall (WAF).	2024-07-09	4.8	CVE-2024-33509
gaizhenbiao -- chuanhuchatgpt	A Stored Cross-Site Scripting (XSS) vulnerability exists in gaizhenbiao/chuanhuchatgpt version 20240410. This vulnerability allows an attacker to inject malicious JavaScript code into the chat history file. When a victim uploads this file, the malicious script is executed in the victim's browser. This can lead to user data theft, session hijacking, malware distribution, and phishing attacks.	2024-07-11	6.1	CVE-2024-6035
Gallagher--Controller 6000 and Controller 7000	External Control of Critical State Data (CWE-642) in the Controller 6000 and Controller 7000 diagnostic web interface allows an authenticated user to modify device I/O connections leading to unexpected behavior that in some circumstances could compromise site physical security controls. Gallagher recommend the diagnostic web page is not enabled (default is off) unless advised by Gallagher Technical support. This interface is intended only for diagnostic purposes. This issue affects:Â Gallagher Controller 6000 and 7000 9.10 prior to vCR9.10.240520a (distributed in 9.10.1268(MR1)), 9.00 prior to vCR9.00.240521a (distributed in 9.00.1990(MR3)), 8.90 prior to vCR8.90.240520a (distributed in 8.90.1947 (MR4)),Â 8.80 prior to vCR8.80.240520a (distributed in 8.80.1726 (MR5)), 8.70 prior to vCR8.70.240520a (distributed in 8.70.2824 (MR7)), all versions of 8.60 and prior.	2024-07-11	6.8	CVE-2024-22387
Gallagher--Controller 6000 and Controller 7000	External Control of File Name or Path (CWE-73) in the Controller 6000 and Controller 7000 allows an attacker with local access to the Controller to perform arbitrary code execution. This issue affects:Â 9.10 prior to vCR9.10.240520a (distributed in 9.10.1268(MR1)), 9.00 prior to vCR9.00.240521a (distributed in 9.00.1990(MR3)), 8.90 prior to vCR8.90.240520a (distributed in 8.90.1947 (MR4)), 8.80 prior to vCR8.80.240520a (distributed in 8.80.1726 (MR5)), 8.70 prior to vCR8.70.240520a (distributed in 8.70.2824 (MR7)), all versions of 8.60 and prior.	2024-07-11	6.3	CVE-2024-23317
Gallagher--Controller 6000 and Controller 7000	Improperly Preserved Integrity of Hardware Configuration State During a Power Save/Restore Operation (CWE-1304) in the Controller 6000 and 7000 can lead to secured door locks connected via Aperio Communication Hubs to momentarily allow free access.Â This issue affects:Â Gallagher Controller 6000 and 7000Â 9.10 prior to vCR9.10.240520a (distributed in 9.10.1268(MR1)), 9.00 prior to vCR9.00.240521a (distributed in 9.00.1990(MR3)), Â 8.90 prior to vCR8.90.240520a (distributed in 8.90.1947 (MR4)),Â 8.80 prior to vCR8.80.240520a (distributed in 8.80.1726 (MR5)), 8.70 prior to vCR8.70.240520a (distributed in 8.70.2824 (MR7)), all versions of 8.60 and prior.	2024-07-11	4.6	CVE-2024-23485
GitLab--GitLab	A Cross Window Forgery vulnerability exists within GitLab CE/EE affecting all versions from 16.3 prior to 16.11.5, 17.0 prior to 17.0.3, and 17.1 prior to 17.1.1. This condition allows for an attacker to abuse the OAuth authentication flow via a crafted payload.	2024-07-09	6.8	CVE-2024-2177

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
glpi-project--glpi	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. An authenticated user can attach a document to any item, even if the user has no write access on it. Upgrade to 10.0.16.	2024-07-10	4.3	CVE-2024-37147
Google--Android	In increment_annotation_count of stats_event.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	6.3	CVE-2024-31311
Google--Android	In updateServicesLocked of AccessibilityManagerService.java, there is a possible way for an app to be hidden from the Setting while retaining Accessibility Service due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-07-09	6.3	CVE-2024-31322
Google--Android	In DevmemIntFreeDefBackingPage of devicemem_server.c, there is a possible arbitrary code execution due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-07-09	6.7	CVE-2024-31334
Google--Android	In multiple functions of ManagedServices.java, there is a possible way to hide an app with notification access in the Device & app notifications settings due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-07-09	5.3	CVE-2024-31315
Google--Android	In multiple functions of MessageQueueBase.h, there is a possible out of bounds write 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.	2024-07-09	5.3	CVE-2024-31327
Google--Android	In onTransact of ParcelableListBinder.java , there is a possible way to steal mAllowlistToken to launch an app from background 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.	2024-07-09	5.3	CVE-2024-34723
hackmdio--codimd	CodiMD allows realtime collaborative markdown notes on all platforms. CodiMD before 2.5.4 is missing authentication and access control vulnerability allowing an unauthenticated attacker to gain unauthorised access to image data uploaded to CodiMD. CodiMD does not require valid authentication to access uploaded images or to upload new image data. An attacker who can determine an uploaded image's URL can gain unauthorised access to uploaded image data. Due to the insecure random filename generation in the underlying Formidable library, an attacker can determine the filenames for previously uploaded images and the likelihood of this issue being exploited is increased. This vulnerability is fixed in 2.5.4.	2024-07-10	5.3	CVE-2024-38353
happymonkeyagency--SCSS Happy Compiler Compile SCSS to CSS & Automatic Enqueue	The SCSS Happy Compiler - Compile SCSS to CSS & Automatic Enqueue plugin for WordPress is vulnerable to Stored Cross-Site Scripting due to a missing capability check and insufficient sanitization on the import_settings() function in all versions up to, and including, 1.3.10. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject malicious web scripts.	2024-07-09	5.4	CVE-2024-5600
HasThemes--HT Mega	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in HasThemes HT Mega allows Path Traversal.This issue affects HT Mega: from n/a through 2.5.7.	2024-07-12	6.5	CVE-2024-38706
ibm -- cloud_pak_for_bus	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended	2024-07-08	5.4	CVE-2024-37528

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
iness_automation	functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 294293.			
ibm -- cloud_pak_for_business_automation	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, 22.0.2, 23.0.1, and 23.0.2 vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 288178.	2024-07-08	4.3	CVE-2024-31897
ibm -- storage_virtualize	IBM FlashSystem 5300 USB ports may be usable even if the port has been disabled by the administrator. A user with physical access to the system could use the USB port to cause loss of access to data. IBM X-Force ID: 295935.	2024-07-08	4.6	CVE-2024-39723
IBM--InfoSphere Server	IBM InfoSphere Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 297720.	2024-07-12	5.4	CVE-2024-40690
IBM--MQ Operator	IBM MQ Operator 3.2.2 and IBM MQ Operator 2.0.24 IBM MQ Container Developer Edition is vulnerable to denial of service caused by incorrect memory de-allocation. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. IBM X-Force ID: 297172.	2024-07-08	5.9	CVE-2024-39743
IBM--QRadar Suite Software	IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 and IBM QRadar Suite Software 1.10.12.0 through 1.10.22.0 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 281429.	2024-07-10	6.2	CVE-2024-25023
IBM--Security QRadar EDR	IBM Security QRadar EDR 3.12 could disclose sensitive information due to an observable login response discrepancy. IBM X-Force ID: 257697.	2024-07-10	5.3	CVE-2023-33859
IBM--Security QRadar EDR	IBM Security QRadar EDR 3.12 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 257702.	2024-07-10	5.3	CVE-2023-33860
IBM--Security QRadar EDR	IBM Security QRadar EDR 3.12 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 297165.	2024-07-10	5.4	CVE-2023-35006
Internal Link Juicer--Internal Link Juicer: SEO Auto Linker for WordPress	Cross-Site Request Forgery (CSRF) vulnerability in Internal Link Juicer Internal Link Juicer: SEO Auto Linker for WordPress.This issue affects Internal Link Juicer: SEO Auto Linker for WordPress: from n/a through 2.24.3.	2024-07-12	4.3	CVE-2024-37941
itsourcecode--Gym Management System	A vulnerability was found in itsourcecode Gym Management System 1.0. It has been classified as critical. This affects an unknown part of the file manage_member.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-271059.	2024-07-10	6.3	CVE-2024-6652
Juniper Networks--Junos OS Evolved	An Improper Physical Access Control vulnerability in the console port control of Juniper Networks Junos OS Evolved allows an attacker with physical access to the device to get access to a user account. When the console cable is disconnected, the logged in user is not logged out.Â This allows a malicious attacker with physical access to the console to resume a previous session and possibly gain administrative	2024-07-10	6.6	CVE-2024-39512

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privileges. This issue affects Junos OS Evolved: * from 23.2R2-EVO before 23.2R2-S1-EVO,Â * from 23.4R1-EVO before 23.4R2-EVO.			
Juniper Networks--Junos OS Evolved	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX7000 Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). On all ACX 7000 Series platforms running Junos OS Evolved, and configured with IRBs, if a Customer Edge device (CE) device is dual homed to two Provider Edge devices (PE) a traffic loop will occur when the CE sends multicast packets. This issue can be triggered by IPv4 and IPv6 traffic. This issue affects Junos OS Evolved:Â All versions from 22.2R1-EVO and later versions before 22.4R2-EVO, This issue does not affect Junos OS Evolved versions before 22.1R1-EVO.	2024-07-11	6.5	CVE-2024-39519
Juniper Networks--Junos OS Evolved	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX 7000 Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). When a device has a Layer 3 or an IRB interface configured in a VPLS instance and specific traffic is received, the evo-pfemand processes crashes which causes a service outage for the respective FPC until the system is recovered manually. This issue only affects Junos OS Evolved 22.4R2-S1 and 22.4R2-S2 releases and is fixed in 22.4R3. No other releases are affected.	2024-07-11	6.5	CVE-2024-39535
Juniper Networks--Junos OS Evolved	An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in Juniper Networks Junos OS Evolved on ACX 7000 Series allows an unauthenticated, network-based attacker to cause a limited information disclosure and availability impact to the device. Due to a wrong initialization, specific processes which should only be able to communicate internally within the device can be reached over the network via open ports. This issue affectsÂ Junos OS Evolved on ACX 7000 Series: * All versions before 21.4R3-S7-EVO, * 22.2-EVO versions before 22.2R3-S4-EVO, * 22.3-EVO versions before 22.3R3-S3-EVO, * 22.4-EVO versions before 22.4R3-S2-EVO, * 23.2-EVO versions before 23.2R2-EVO, * 23.4-EVO versions before 23.4R1-S1-EVO, 23.4R2-EVO.	2024-07-11	6.5	CVE-2024-39537
Juniper Networks--Junos OS Evolved	A Buffer Copy without Checking Size of Input vulnerability in the PFE management daemon (evo-pfemand) of Juniper Networks Junos OS Evolved on ACX7000 Series allows an unauthenticated, adjacent attacker to cause aÂ Denial-of-Service (DoS).When multicast traffic with a specific, valid (S,G) is received, evo-pfemand crashes which leads to an outage of the affected FPC until it is manually recovered. This issue affects Junos OS Evolved on ACX7000 Series: * All versions before 21.2R3-S8-EVO, * 21.4-EVO versions before 21.4R3-S7-EVO, * 22.2-EVO versions before 22.2R3-S4-EVO, * 22.3-EVO versions before 22.3R3-S3-EVO,Â * 22.4-EVO versions before 22.4R3-S2-EVO,Â * 23.2-EVO versions before 23.2R2-EVO,Â * 23.4-EVO versions before 23.4R1-S2-EVO, 23.4R2-EVO.	2024-07-11	6.5	CVE-2024-39538
Juniper Networks--Junos OS Evolved	An Exposure of Resource to Wrong Sphere vulnerability in the sampling serviceÂ of Juniper Networks Junos OS Evolved allows an unauthenticated network-based attacker to send arbitrary data to the device, which leads msvcsd process to crash with limited availability impacting Denial of Service (DoS) and allows unauthorized network access to the device, potentially impacting system integrity. This issue only happens when inline jflow is configured. This does not impact any forwarding traffic. The impacted services MSVCS-DB app crashes momentarily and recovers by itself.Â This issue affects Juniper Networks Junos OS Evolved:Â * 21.4 versions earlier than 21.4R3-S7-EVO;Â * 22.2 versions earlier thanÂ 22.2R3-S3-EVO; * 22.3 versions earlier than 22.3R3-S2-EVO; * 22.4 versions earlier than 22.4R3-EVO; * 23.2 versions earlier than 23.2R1-S2-EVO, 23.2R2-EVO.	2024-07-11	6.5	CVE-2024-39553
Juniper Networks--Junos OS Evolved	An Uncontrolled Resource Consumption vulnerability in the Layer 2 Address Learning Daemon (l2ald) of Juniper Networks Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a memory leak, eventually exhausting all system memory, leading to a system crash and Denial of Service (DoS). Certain MAC table updates cause a small amount of memory to leak.Â Once memory	2024-07-10	6.5	CVE-2024-39557

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	utilization reaches its limit, the issue will result in a system crash and restart. To identify the issue, execute the CLI command: user@device> show platform application-info allocations app l2ald-agent EVL Object Allocation Statistics: Node Â Application Â Â Context Name Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Â Live Â Allocs Â Fails Â Â Guids re0 Â l2ald-agent Â Â Â Â Â Â Â net::juniper::rtnh::L2Rtinfo Â Â Â 1069096 1069302 Â 0 Â Â Â Â 1069302 re0 Â l2ald-agent Â Â Â Â Â Â Â net::juniper::rtnh::NHOpaqueTlv Â Â 114 Â Â 195 Â Â Â 0 Â Â Â Â 195 This issue affects Junos OS Evolved: * All versions before 21.4R3-S8-EVO, * from 22.2-EVO before 22.2R3-S4-EVO, * from 22.3-EVOÂ before 22.3R3-S3-EVO, * from 22.4-EVO before 22.4R3-EVO, * from 23.2-EVO before 23.2R2-EVO.			
Juniper Networks--Junos OS Evolved	An Improper Input Validation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved allows a local, low-privileged attacker to cause a Denial of Service (DoS). When a specific "clear" command is run, theÂ Advanced Forwarding Toolkit manager (evo-aftmand-bt or evo-aftmand-zx) crashes and restarts. The crashÂ impacts all traffic going through the FPCs, causing a DoS. Running the command repeatedly leads to a sustained DoS condition. This issue affects Junos OS Evolved:Â * All versions before 20.4R3-S9-EVO,Â * from 21.2-EVO before 21.2R3-S7-EVO,Â * from 21.3-EVO before 21.3R3-S5-EVO,Â * from 21.4-EVO before 21.4R3-S6-EVO,Â * from 22.1-EVO before 22.1R3-S4-EVO,Â * from 22.2-EVO before 22.2R3-S3-EVO,Â * from 22.3-EVO before 22.3R3-S3-EVO,Â * from 22.4-EVO before 22.4R3-EVO, * from 23.2-EVO before 23.2R2-EVO.	2024-07-10	5.5	CVE-2024-39513
Juniper Networks--Junos OS Evolved	An Improper Check for Unusual or Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS Evolved may allow a network-based unauthenticated attacker to crash the device (vmcore) by sending a specific TCP packet over an established TCP session with MD5 authentication enabled, destined to an accessible port on the device, resulting in a Denial of Service (DoS).Â The receipt of this packet must occur within a specific timing window outside the attacker's control (i.e., race condition). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affectsÂ dual RE systems with Nonstop Active Routing (NSR) enabled. Exploitation can only occur over TCP sessions with MD5 authentication enabled (e.g., BGP with MD5 authentication). This issue affects Junos OS Evolved:Â * All versions before 21.2R3-S8-EVO, * from 21.4-EVO before 21.4R3-S6-EVO, * from 22.1-EVO before 22.1R3-S4-EVO, * from 22.2-EVO before 22.2R3-S4-EVO, * from 22.3-EVO before 22.3R3-S3-EVO, * from 22.4-EVO before 22.4R2-S2-EVO, 22.4R3-EVO.	2024-07-10	5.9	CVE-2024-39559
Juniper Networks--Junos OS	An Improper Check or Handling of Exceptional Conditions vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). An attacker can send specific traffic to the device, which causes the rpd to crash and restart. Continued receipt of this traffic will result in a sustained DoS condition. This issue only affects devices with an EVPN-VPWS instance with IGMP-snooping enabled. This issue affects Junos OS: * All versions before 20.4R3-S10,Â * from 21.4 before 21.4R3-S6,Â * from 22.1 before 22.1R3-S5,Â * from 22.2 before 22.2R3-S3,Â * from 22.3 before 22.3R3-S2,Â * from 22.4 before 22.4R3,Â * from 23.2 before 23.2R2; Junos OS Evolved: * All versions before 20.4R3-S10-EVO,Â * from 21.4-EVO before 21.4R3-S6-EVO,Â * from 22.1-EVO before 22.1R3-S5-EVO,Â * from 22.2-EVO before 22.2R3-S3-EVO,Â * from 22.3-EVO before 22.3R3-S2-EVO,Â * from 22.4-EVO before 22.4R3-EVO,Â * from 23.2-EVO before 23.2R2-EVO.	2024-07-10	6.5	CVE-2024-39514
Juniper Networks--Junos OS	An Improper Check for Unusual or Exceptional Conditions vulnerability in theÂ Layer 2 Address Learning Daemon (l2ald) on Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause Denial of Service (DoS). In an EVPN/VXLAN scenario, when a high amount specific Layer 2 packets are processed by the device, it can cause the Routing Protocol Daemon (rpd) to utilize all CPU resources which causes the device to hang. A manual restart	2024-07-10	6.5	CVE-2024-39517

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of the rpd is required to restore services. This issue affects both IPv4 and IPv6 implementations. This issue affects Junos OS: All versions earlier thanÂ 21.4R3-S7; 22.1Â versions earlier than 22.1R3-S5; 22.2 versions earlier thanÂ 22.2R3-S3; 22.3 versions earlier thanÂ 22.3R3-S3; 22.4 versions earlier thanÂ 22.4R3-S2; 23.2 versions earlier thanÂ 23.2R2; 23.4 versions earlier thanÂ 23.4R1-S1. Junos OS Evolved: All versions earlier thanÂ 21.4R3-S7-EVO; 22.1-EVO versions earlier thanÂ 22.1R3-S5-EVO; 22.2-EVO versions earlier thanÂ 22.2R3-S3-EVO; 22.3-EVO versions earlier than 22.3R3-S3-EVO; 22.4-EVO versions earlier thanÂ 22.4R3-S2-EVO; 23.2-EVO versions earlier thanÂ 23.2R2-EVO; 23.4-EVO versions earlier thanÂ 23.4R1-S1-EVO, 23.4R2-EVO.			
Juniper Networks--Junos OS	AnÂ Insertion of Sensitive Information into Log File vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows a local, authenticated attacker with high privileges to access sensitive information. When another user performs a specific operation, sensitive information is stored as plain text in a specific log file, so that a high-privileged attacker has access to this information. This issue affects: Junos OS: * All versions before 22.1R2-S2, * 22.1R3 and later versions, * 22.2 versions before 22.2R2-S1, 22.2R3, * 22.3 versions before 22.3R1-S2, 22.3R2; Junos OS Evolved: * All versions before before 22.1R3-EVO, * 22.2-EVO versions before 22.2R2-S1-EVO, 22.2R3-EVO, * 22.3-EVO versions before 22.3R1-S1-EVO, 22.3R2-EVO.	2024-07-11	6.3	CVE-2024-39532
Juniper Networks--Junos OS	An Improper Handling of Exceptional Conditions vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). When conflicting information (IP or ISO addresses) about a node is added to the Traffic Engineering (TE) database and then a subsequent operation attempts to process these, rpd will crash and restart. This issue affects: Junos OS: * 22.4 versions before 22.4R3-S1, * 23.2 versions before 23.2R2,Â * 23.4 versions before 23.4R1-S1, 23.4R2,Â This issue does not affect Junos OS versions earlier than 22.4R1. Junos OS Evolved: * 22.4-EVO versions before 22.4R3-S2-EVO, * 23.2-EVO versions before 23.2R2-EVO, * 23.4-EVO versions before 23.4R1-S1-EVO, 23.4R2-EVO, This issue does not affect Junos OS Evolved versions earlier than before 22.4R1.	2024-07-11	6.5	CVE-2024-39541
Juniper Networks--Junos OS	A Buffer Copy without Checking Size of InputÂ vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Juniper Networks Junos OS Evolved allows an unauthenticated, adjacent attacker to send specific RPKI-RTR packets resulting in a crash,Â creating a Denial of Service (DoS) condition.Â Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affectsÂ Junos OS:Â * All versions before 21.2R3-S8,Â * from 21.4 before 21.4R3-S8, * from 22.2 before 22.2R3-S4,Â * from 22.3 before 22.3R3-S3,Â * from 22.4 before 22.4R3-S2,Â * from 23.2 before 23.2R2-S1,Â * from 23.4 before 23.4R2. Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * from 21.4 before 21.4R3-S8-EVO, * from 22.2 before 22.2R3-S4-EVO,Â * from 22.3 before 22.3R3-S3-EVO, * from 22.4 before 22.4R3-S2-EVO,Â * from 23.2 before 23.2R2-S1-EVO, * from 23.4 before 23.4R2-EVO.	2024-07-11	6.5	CVE-2024-39543
Juniper Networks--Junos OS	A Missing Release of Memory after Effective Lifetime vulnerability in the rtlogd processÂ of Juniper Networks Junos OS on MX Series with SPC3 allows an unauthenticated, adjacent attacker to trigger internal events cause (which can be done by repeated port flaps)Â to cause a slow memory leak, ultimately leading to a Denial of Service (DoS). Memory can only be recovered by manually restarting rtlogd process.Â The memory usage can be monitored using the below command. â€ƒâ€ƒâ€ƒuser@host> show system processes extensive | match rtlogÂ This issue affects Junos OS on MX Series with SPC3 line card:Â * from 21.2R3 before 21.2R3-S8,Â * from 21.4R2 before 21.4R3-S6,Â * from 22.1 before 22.1R3-S5,Â * from 22.2 before 22.2R3-S3,Â * from 22.3 before 22.3R3-S2,Â * from 22.4 before 22.4R3-S1,Â * from 23.2 before 23.2R2,Â * from 23.4 before 23.4R2.	2024-07-11	6.5	CVE-2024-39550

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Juniper Networks--Junos OS	A Stack-Based Buffer Overflow vulnerability in Juniper Networks Junos OS and Juniper Networks Junos OS Evolved may allow a local, low-privileged attacker with access to the CLI the ability to load a malicious certificate file, leading to a limited Denial of Service (DoS) or privileged code execution. By exploiting the 'set security certificates' command with a crafted certificate file, a malicious attacker with access to the CLI could cause a crash of the command management daemon (mgd), limited to the local user's command interpreter, or potentially trigger a stack-based buffer overflow. This issue affects: Â Junos OS: * All versions before 21.4R3-S7, * from 22.1 before 22.1R3-S6, * from 22.2 before 22.2R3-S4, * from 22.3 before 22.3R3-S3, * from 22.4 before 22.4R3-S2, * from 23.2 before 23.2R2, * from 23.4 before 23.4R1-S1, 23.4R2;Â Junos OS Evolved: * All versions before 21.4R3-S7-EVO, * from 22.1-EVO before 22.1R3-S6-EVO, * from 22.2-EVO before 22.2R3-S4-EVO, * from 22.3-EVO before 22.3R3-S3-EVO, * from 22.4-EVO before 22.4R3-S2-EVO, * from 23.2-EVO before 23.2R2-EVO, * from 23.4-EVO before 23.4R1-S1-EVO, 23.4R2-EVO.	2024-07-10	6.4	CVE-2024-39556
Juniper Networks--Junos OS	An Unchecked Return Value vulnerability in the Routing Protocol Daemon (rpd) on Juniper Networks Junos OS and Juniper Networks Junos OS Evolved allows a logically adjacent, unauthenticated attacker sending a specific PIM packet to cause rpd to crash and restart, resulting in a Denial of Service (DoS), when PIM is configured with Multicast-only Fast Reroute (MoFRR). Continued receipt and processing of this packet may create a sustained Denial of Service (DoS) condition. This issue is observed on Junos and Junos Evolved platforms where PIM is configured along with MoFRR. MoFRR tries to select the active path, but due to an internal timing issue, rpd is unable to select the forwarding next-hop towards the source, resulting in an rpd crash. This issue affects: Junos OS: * All versions before 20.4R3-S10, * from 21.2 before 21.2R3-S7, * from 21.4 before 21.4R3-S6, * from 22.1 before 22.1R3-S5, * from 22.2 before 22.2R3-S3, * from 22.3 before 22.3R3, * from 22.4 before 22.4R2;Â Junos OS Evolved: * All versions before 20.4R3-S10 -EVO, * from 21.2-EVO before 21.2R3-S7 -EVO, * from 21.4-EVO before 21.4R3-S6 -EVO, * from 22.1-EVO before 22.1R3-S5 -EVO, * from 22.2-EVO before 22.2R3-S3-EVO, * from 22.3-EVO before 22.3R3-EVO, * from 22.4-EVO before 22.4R2-EVO.	2024-07-10	6.5	CVE-2024-39558
Juniper Networks--Junos OS	An Improper Handling of Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a logically adjacent downstream RSVP neighbor to cause kernel memory exhaustion, leading to a kernel crash, resulting in a Denial of Service (DoS). The kernel memory leak and eventual crash will be seen when the downstream RSVP neighbor has a persistent error which will not be corrected. System kernel memory can be monitored through the use of the 'show system statistics kernel memory' command as shown below: user@router> show system statistics kernel memory Memory Â Â Â Â Â Â Â Size (kB) Percentage When Â Active Â Â Â Â Â Â Â Â 753092 Â Â 18.4% Now Â Inactive Â Â Â Â Â Â Â 574300 Â Â 14.0% Now Â WiredÂ Â Â Â Â Â Â Â Â 443236 Â Â 10.8% Now Â CachedÂ Â Â Â Â Â Â Â 1911204 Â Â 46.6% Now Â Buf Â Â Â Â Â Â Â Â Â 32768Â Â Â 0.8% Now Â Free Â Â Â Â Â Â Â Â 385072Â Â Â 9.4% Now Kernel MemoryÂ Â Â Â Â Â Â Â Â Â Â Â Â Â Â Now Â Data Â Â Â Â Â Â Â Â 312908Â Â Â 7.6% Now Â Text Â Â Â Â Â Â Â Â Â 2560Â Â Â 0.1% Now ... This issue affects: Junos OS: * All versions before 20.4R3-S9, * All versions of 21.2, * from 21.4 before 21.4R3-S5, * from 22.1 before 22.1R3-S5, * from 22.2 before 22.2R3-S3, * from 22.3 before 22.3R3-S2, * from 22.4 before 22.4R3, * from 23.2 before 23.2R2; Junos OS Evolved: * All versions before 21.4R3-S5-EVO, * from 22.1-EVO before 22.1R3-S5-EVO, * from 22.2-EVO before 22.2R3-S3-EVO, * from 22.3-EVO before 22.3R3-S2-EVO, * from 22.4-EVO before 22.4R3-EVO, * from 23.2-EVO before 23.2R2-EVO.	2024-07-10	6.5	CVE-2024-39560

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Juniper Networks--Junos OS	An Improper Input Validation vulnerability in the 802.1X Authentication (dot1x) Daemon of Juniper Networks Junos OS allows a local, low-privileged attacker with access to the CLI to cause a Denial of Service (DoS). On running a specific operational dot1x command, the dot1x daemon crashes. An attacker can cause a sustained DoS condition by running this command repeatedly. When the crash occurs, the authentication status of any 802.1x clients is cleared, and any authorized dot1x port becomes unauthorized. The client cannot re-authenticate until the dot1x daemon restarts. This issue affects Junos OS: * All versions before 20.4R3-S10; * 21.2 versions before 21.2R3-S7; * 21.4 versions before 21.4R3-S6; * 22.1 versions before 22.1R3-S5; * 22.2 versions before 22.2R3-S3; * 22.3 versions before 22.3R3-S2; * 22.4 versions before 22.4R3-S1; * 23.2 versions before 23.2R2.	2024-07-10	5.5	CVE-2024-39511
Juniper Networks--Junos OS	A Use After Free vulnerability in the Routing Protocol Daemon (rpd) ofÂ Juniper Networks Junos OS and Junos OS Evolved allows an authenticated, network-based attacker to cause a Denial of Service (DoS).On all Junos OS and Junos Evolved platforms, if a routing-instance deactivation is triggered, and at the same time a specific SNMP request is received, a segmentation fault occurs which causes rpd to crash and restart. This issue affects: Â Â Junos OS: * All versions before 21.2R3-S8,Â * 21.4 versions before 21.4R3-S5, * 22.2 versions before 22.2R3-S3, * 22.3 versions before 22.3R3-S2, * 22.4 versions before 22.4R3, * 23.2 versions before 23.2R2. Â Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * 21.4-EVO versions before 21.4R3-S5-EVO, * 22.2-EVO versions before 22.2R3-S3-EVO,Â * 22.3-EVO versions before 22.3R3-S2-EVO, * 22.4-EVO versions before 22.4R3-EVO, * 23.2-EVO versions before 23.2R2-EVO.	2024-07-11	5.7	CVE-2024-39528
Juniper Networks--Junos OS	An Unimplemented or Unsupported Feature in the UI vulnerability in Juniper Networks Junos OS on QFX5000 Series and EX4600 Series allows an unauthenticated, network-based attacker to cause a minor integrity impact to downstream networks.If one or more of the following match conditions ip-source-address ip-destination-address arp-type which are not supported for this type of filter, are used in an ethernet switching filter,Â and then this filter is applied as an output filter, the configuration can be committed but the filter will not be in effect. This issue affects Junos OS on QFX5000 Series and EX4600 Series: * All version before 21.2R3-S7,Â * 21.4 versions before 21.4R3-S6, * 22.1 versions before 22.1R3-S5, * 22.2 versions before 22.2R3-S3, * 22.3 versions before 22.3R3-S2,Â * 22.4 versions before 22.4R3, * 23.2 versions before 23.2R2. Please note that the implemented fix ensures these unsupported match conditions cannot be committed anymore.	2024-07-11	5.8	CVE-2024-39533
Juniper Networks--Junos OS	A Missing Release of Memory after Effective Lifetime vulnerability in the Periodic Packet Management Daemon (ppmd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker to cause a Denial-of-Service (DoS). When aÂ BFD session configured with authentication flaps,Â ppmd memory can leak. Whether the leak happens depends on aÂ race condition which is outside the attackers control. This issue only affects BFD operating in distributed aka delegated (which is the default behavior) or inline mode. Whether the leak occurs can be monitored with the following CLI command: > show ppm request-queue FPC Â Â Pending-request fpc0Â Â Â Â Â Â Â Â Â Â Â Â 2 request-total-pending: 2 where a continuously increasing number of pending requests is indicative of the leak.Â This issue affects: Junos OS: * All versions before 21.2R3-S8, * 21.4 versions before 21.4R3-S7, * 22.1 versions before 22.1R3-S4, * 22.2 versions before 22.2R3-S4, * 22.3 versions before 22.3R3, * 22.4 versions before 22.4R2-S2, 22.4R3. Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * 21.4-EVO versions before 21.4R3-S7-EVO, * 22.2-EVO versions before 22.2R3-S4-EVO, * 22.3-EVO versions before 22.3R3-EVO, * 22.4-EVO versions before 22.4R3-EVO.	2024-07-11	5.3	CVE-2024-39536
Juniper Networks--Junos OS	A Missing Release of Memory after Effective Lifetime vulnerability in Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause aÂ Denial-of-Service (DoS). In a subscriber management scenario continuous subscriber logins will trigger a memory leak and eventually lead to an FPC crash	2024-07-11	5.3	CVE-2024-39539

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and restart. This issue affects Junos OS on MX Series: * All version before 21.2R3-S6, * 21.4 versions before 21.4R3-S6, * 22.1 versions before 22.1R3-S5, * 22.2 versions before 22.2R3-S3,Â * 22.3 versions before 22.3R3-S2, * 22.4 versions before 22.4R3, * 23.2 versions before 23.2R2.			
Juniper Networks--Junos OS	A Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to inject incremental routing updates when BGP multipath is enabled, causing rpd to crash and restart, resulting in a Denial of Service (DoS). Since this is a timing issue (race condition), the successful exploitation of this vulnerability is outside the attacker's control.Â However, continued receipt and processing of this packet may create a sustained Denial of Service (DoS) condition. On all Junos OS and Junos OS Evolved platforms with BGP multipath enabled, a specific multipath calculation removes the original next hop from the multipath lead routes nexthop-set. When this change happens, multipath relies on certain internal timing to record the update.Â Under certain circumstance and with specific timing, this could result in an rpd crash. This issue only affects systems with BGP multipath enabled. This issue affects: Junos OS: * All versions of 21.1 * from 21.2 before 21.2R3-S7, * from 21.4 before 21.4R3-S6, * from 22.1 before 22.1R3-S5, * from 22.2 before 22.2R3-S3, * from 22.3 before 22.3R3-S2, * from 22.4 before 22.4R3, * from 23.2 before 23.2R2. Junos OS Evolved: * All versions of 21.1-EVO, * All versions of 21.2-EVO, * from 21.4-EVO before 21.4R3-S6-EVO, * from 22.1-EVO before 22.1R3-S5-EVO, * from 22.2-EVO before 22.2R3-S3-EVO, * from 22.3-EVO before 22.3R3-S2-EVO, * from 22.4-EVO before 22.4R3-EVO, * from 23.2-EVO before 23.2R2-EVO. Versions of Junos OS before 21.1R1 are unaffected by this vulnerability. Versions of Junos OS Evolved before 21.1R1-EVO are unaffected by this vulnerability.	2024-07-10	5.9	CVE-2024-39554
Juniper Networks--Junos OS	An Improper Check for Unusual or Exceptional Conditions vulnerability in the flow daemon (flowd) of Juniper Networks Junos OS on SRX4600 and SRX5000 Series allows an attacker to send TCP packets with SYN/FIN or SYN/RST flags, bypassing the expected blocking of these packets. A TCP packet with SYN/FIN or SYN/RST should be dropped in flowd. However, when no-syn-check and Express PathÂ are enabled, these TCP packets are unexpectedly transferred to the downstream network. This issue affects Junos OS on SRX4600 and SRX5000 Series: * All versions before 21.2R3-S8, * from 21.4 before 21.4R3-S7, * from 22.1 before 22.1R3-S6, * from 22.2 before 22.2R3-S4, * from 22.3 before 22.3R3-S3, * from 22.4 before 22.4R3-S2, * from 23.2 before 23.2R2, * from 23.4 before 23.4R1-S1, 23.4R2.	2024-07-10	5.8	CVE-2024-39561
khoj-ai--khoj	Khoj is an application that creates personal AI agents. The Khoj Obsidian, Desktop and Web clients inadequately sanitize the AI model's response and user inputs. This can trigger Cross Site Scripting (XSS) via Prompt Injection from untrusted documents either indexed by the user on Khoj or read by Khoj from the internet when the user invokes the /online command. This vulnerability is fixed in 1.13.0.	2024-07-08	5.9	CVE-2024-25639
leap13--Premium Addons for Elementor	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Animated Text widget in all versions up to, and including, 4.10.36 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.	2024-07-12	6.4	CVE-2024-6495
m_uysl--WP Total Branding Complete branding solution for WordPress	The WP Total Branding - Complete branding solution for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.2 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.	2024-07-12	5.5	CVE-2024-6625

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mardojai--Simple Alert Boxes	The Simple Alert Boxes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Alert shortcode in all versions up to, and including, 1.4.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-09	6.4	CVE-2024-5937
metagauss--ProfileGrid User Profiles, Groups and Communities	The ProfileGrid - User Profiles, Groups and Communities plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.8.9 via the 'pm_upload_image' function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change the profile picture of any user.	2024-07-10	4.3	CVE-2024-6410
mhuertos--phpLDAPadmin	A vulnerability classified as critical was found in mhuertos phpLDAPadmin up to 665dbc2690ebeb5392d38f1fece0a654225a0b38. Affected by this vulnerability is the function makeHttpRequest of the file htdocs/js/ajax_functions.js. The manipulation leads to http request smuggling. The attack can be launched remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named dd6e9583a2eb2ca085583765e8a63df5904cb036. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-270523.	2024-07-11	6.3	CVE-2016-15039
microsoft -- 365_apps	Microsoft Outlook Spoofing Vulnerability	2024-07-09	6.5	CVE-2024-38020
microsoft -- azure_kinect_software_development_kit	Azure Kinect SDK Remote Code Execution Vulnerability	2024-07-09	6.4	CVE-2024-38086
microsoft -- windows_10_1507	Microsoft Windows Server Backup Elevation of Privilege Vulnerability	2024-07-09	6.7	CVE-2024-38013
microsoft -- windows_10_1507	Windows Line Printer Daemon Service Denial of Service Vulnerability	2024-07-09	6.5	CVE-2024-38027
microsoft -- windows_10_1507	Windows Themes Spoofing Vulnerability	2024-07-09	6.5	CVE-2024-38030
microsoft -- windows_10_1507	Windows Network Driver Interface Specification (NDIS) Denial of Service Vulnerability	2024-07-09	6.5	CVE-2024-38048
microsoft -- windows_10_1507	BitLocker Security Feature Bypass Vulnerability	2024-07-09	6.8	CVE-2024-38058
microsoft -- windows_10_1507	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	6.8	CVE-2024-38065
microsoft -- windows_10_1507	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	2024-07-09	6.5	CVE-2024-38101

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10_1507	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	2024-07-09	6.5	CVE-2024-38102
microsoft -- windows_10_1507	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	2024-07-09	6.5	CVE-2024-38105
microsoft -- windows_10_1507	Microsoft Message Queuing Information Disclosure Vulnerability	2024-07-09	5.5	CVE-2024-38017
microsoft -- windows_10_1507	Microsoft Windows Codecs Library Information Disclosure Vulnerability	2024-07-09	5.5	CVE-2024-38055
microsoft -- windows_10_1507	Microsoft Windows Codecs Library Information Disclosure Vulnerability	2024-07-09	5.5	CVE-2024-38056
microsoft -- windows_10_1607	Windows Kernel Information Disclosure Vulnerability	2024-07-09	5.5	CVE-2024-38041
microsoft -- windows_server_2008	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	2024-07-09	5.9	CVE-2024-38099
Microsoft-- Windows 10 Version 1809	Windows iSCSI Service Denial of Service Vulnerability	2024-07-09	5.3	CVE-2024-35270
Microsoft-- Windows 10 Version 1809	Windows Remote Access Connection Manager Information Disclosure Vulnerability	2024-07-09	4.7	CVE-2024-30071
Microsoft-- Windows Server 2022	Secure Boot Security Feature Bypass Vulnerability	2024-07-09	6.8	CVE-2024-26184
Milan Petrovic--GD Rating System	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Milan Petrovic GD Rating System allows PHP Local File Inclusion.This issue affects GD Rating System: from n/a through 3.6.	2024-07-12	5.3	CVE-2024-38709
mommyheather -- advanced_backups	Mommy Heather Advanced Backups up to v3.5.3 allows attackers to write arbitrary files via restoring a crafted back up.	2024-07-09	5.5	CVE-2024-39118
monospace -- directus	Directus is a real-time API and App dashboard for managing SQL database content. There was already a reported SSRF vulnerability via file import. It was fixed by resolving all DNS names and checking if the requested IP is an internal IP address. However it is possible to bypass this security measure and execute a SSRF using redirects. Directus allows redirects when importing file from the URL and does not check the result URL. Thus, it is possible to execute a request to an internal IP, for example to 127.0.0.1. However, it is blind SSRF, because Directus also uses response interception technique to get the information about the connect from the socket directly and it does not show a response if the IP address is internal. This vulnerability is fixed in 10.9.3.	2024-07-08	5	CVE-2024-39699

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Mozilla--Firefox	CSP violations generated links in the console tab of the developer tools, pointing to the violating resource. This caused a DNS prefetch which leaked that a CSP violation happened. This vulnerability affects Firefox < 128.	2024-07-09	5.3	CVE-2024-6612 security@mozilla.org security@mozilla.org
mythemeshop -- url_shortener	The URL Shortener by Myhop WordPress plugin through 1.0.17 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	2024-07-09	4.8	CVE-2024-5802
MyThemeShop-- SociallyViral	Cross-Site Request Forgery (CSRF) vulnerability in MyThemeShop SociallyViral.This issue affects SociallyViral: from n/a through 1.0.10.	2024-07-12	4.3	CVE-2024-37938
N/A--Cliengo Chatbot	Cross-Site Request Forgery (CSRF) vulnerability in Cliengo - Chatbot.This issue affects Cliengo - Chatbot: from n/a through 3.0.1.	2024-07-09	5.4	CVE-2024-37923
N/A-- easyappointments	A BOLA vulnerability in POST /customers allows a low privileged user to create a low privileged user (customer) in the system. This results in unauthorized data manipulation.	2024-07-09	5	CVE-2023-3290
n/a--n/a	An issue was discovered on Renesas SmartBond DA14691, DA14695, DA14697, and DA14699 devices. The bootrom function responsible for validating the Flash Product Header directly uses a user-controllable size value (Length of Flash Config Section) to control a read from the QSPI device into a fixed sized buffer, resulting in a buffer overflow and execution of arbitrary code.	2024-07-10	6.8	CVE-2024-25076
n/a--n/a	A vulnerability was discovered in Samsung Mobile Processor Exynos 850, Exynos 9610, Exynos 980, Exynos 1280, Exynos 1380, Exynos 1330, Exynos W920, and Exynos W930 where it does not properly check a pointer address, which can lead to a Information disclosure.	2024-07-09	6	CVE-2024-27363
n/a--n/a	A vulnerability was discovered in the slsi_handle_nan_rx_event_log_ind function in Samsung Mobile Processor Exynos 1380 and Exynos 1480 related to no input validation check on tag_len for rx coming from userspace, which can lead to heap overwrite.	2024-07-09	6.7	CVE-2024-27385
n/a--n/a	A vulnerability was discovered in the slsi_handle_nan_rx_event_log_ind function in Samsung Mobile Processor Exynos 1380 and Exynos 1480 related to no input validation check on tag_len for tx coming from userspace, which can lead to heap overwrite.	2024-07-09	6.7	CVE-2024-27386
n/a--n/a	Cross Site Scripting vulnerability in Creativeitem Academy LMS Learning Management System v.6.8.1 allows a remote attacker to execute arbitrary code and obtain sensitive information via the string parameter.	2024-07-09	6.1	CVE-2024-38959
n/a--n/a	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/memberOnline_deal.php?mudi=del&dataType=&dataID=6	2024-07-10	6.3	CVE-2024-40328
n/a--n/a	idccms v1.35 is vulnerable to Cross Site Scripting (XSS) within the 'Image Advertising Management.'	2024-07-10	6.1	CVE-2024-40336
n/a--n/a	A vulnerability was discovered in Samsung Mobile Processor Exynos 980, Exynos 990, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, and Exynos 2400 that involves a time-of-check to time-of-use (TOCTOU) race condition, which can lead to a Denial of Service.	2024-07-09	5.1	CVE-2024-27361
n/a--n/a	A vulnerability was discovered in SS in Samsung Mobile Processor, Wearable Processor, and Modems with versions Exynos 9820, Exynos 9825, Exynos 980, Exynos 990, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 2400, Exynos 9110, Exynos W920, Exynos W930,	2024-07-09	5.3	CVE-2024-28068

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Exynos Modem 5123, and Exynos Modem 5300 that involves a NULL pointer dereference which can cause abnormal termination of a mobile phone via a manipulated packet.			
n/a--n/a	In Silverpeas Core <= 6.3.5, inside of mes agendas a user can create a new event and add it to his calendar. The user can also add other users to the event from the same domain, including administrator. A normal user can create an event with XSS payload inside "Titre" and "Description" parameters and add the administrator or any user to the event. When the other user (victim) visits his own profile (even without clicking on the event) the payload will be executed on the victim side.	2024-07-09	5.4	CVE-2024-39031
n/a--n/a	An issue was discovered in Django 5.0 before 5.0.7 and 4.2 before 4.2.14. The django.contrib.auth.backends.ModelBackend.authenticate() method allows remote attackers to enumerate users via a timing attack involving login requests for users with an unusable password.	2024-07-10	5.3	CVE-2024-39329
n/a--n/a	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/userLevel_deal.php?mudi=add.	2024-07-09	5.9	CVE-2024-40035
n/a--n/a	idccms v1.35 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/userScore_deal.php?mudi=rev	2024-07-09	5.3	CVE-2024-40038
NetApp--SnapCenter	SnapCenter versions prior to 5.0p1 are susceptible to a vulnerability which could allow an authenticated attacker to discover plaintext credentials.	2024-07-09	5.7	CVE-2024-21993
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-ports/add/.	2024-07-09	6.1	CVE-2024-38972
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-ports/{id}/edit/.	2024-07-09	6.1	CVE-2024-40726
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/console-server-ports/add/.	2024-07-09	6.1	CVE-2024-40727
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/console-server-ports/{id}/edit/.	2024-07-09	6.1	CVE-2024-40728
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/interfaces/add/.	2024-07-09	6.1	CVE-2024-40729
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/interfaces/{id}/edit/.	2024-07-09	6.1	CVE-2024-40730
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/rear-ports/{id}/edit/.	2024-07-09	6.1	CVE-2024-40731
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/rear-ports/add/.	2024-07-09	6.1	CVE-2024-40732
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/front-ports/{id}/edit/.	2024-07-09	6.1	CVE-2024-40733

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/front-ports/add/.	2024-07-09	6.1	CVE-2024-40734
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-outlets/{id}/edit/.	2024-07-09	6.1	CVE-2024-40735
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-outlets/add.	2024-07-09	6.1	CVE-2024-40736
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/console-ports/add.	2024-07-09	6.1	CVE-2024-40737
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/console-ports/{id}/edit/.	2024-07-09	6.1	CVE-2024-40738
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-feeds/add.	2024-07-09	6.1	CVE-2024-40739
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter at /dcim/power-feeds/{id}/edit/.	2024-07-09	6.1	CVE-2024-40740
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the circuit ID parameter at /circuits/circuits/{id}/edit/.	2024-07-09	6.1	CVE-2024-40741
netbox -- netbox	A cross-site scripting (XSS) vulnerability in netbox v4.0.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the circuit ID parameter at /circuits/circuits/add.	2024-07-09	6.1	CVE-2024-40742
Netgear--WN604	A vulnerability was found in Netgear WN604 up to 20240710. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /downloadFile.php of the component Web Interface. The manipulation of the argument file with the input config leads to information disclosure. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-271052. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-10	5.3	CVE-2024-6646
nhibernate--nhibernate-core	NHibernate is an object-relational mapper for the .NET framework. A SQL injection vulnerability exists in some types implementing ILiteralType.ObjectToSQLString. Callers of these methods are exposed to the vulnerability, which includes mappings using inheritance with discriminator values; HQL queries referencing a static field of the application; users of the SqlInsertBuilder and SqlUpdateBuilder utilities, calling their AddColumn overload taking a literal value; and any direct use of the ObjectToSQLString methods for building SQL queries on the user side. This vulnerability is fixed in 5.4.9 and 5.5.2.	2024-07-08	5.9	CVE-2024-39677
Ninja Team--FileBird Document Library	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ninja Team FileBird Document Library.This issue affects FileBird Document Library: from n/a through 2.0.6.	2024-07-10	5.3	CVE-2024-37504
Nuvoton--NPCM7xx (Poleg) BootBlock	Nuvoton - CWE-305: Authentication Bypass by Primary Weakness An attacker with write access to the SPI-Flash on an NPCM7xx BMC subsystem that uses the Nuvoton BootBlock reference code can modify the u-boot image header on flash parsed by the BootBlock which could lead to arbitrary code execution.	2024-07-11	6.7	CVE-2024-38433

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openclarity--kubeclarity	KubeClarity is a tool for detection and management of Software Bill Of Materials (SBOM) and vulnerabilities of container images and filesystems. A time/boolean SQL Injection is present in the following resource `/api/applicationResources` via the following parameter `packageID`. As it can be seen in backend/pkg/database/id_view.go, while building the SQL Query the `fmt.Sprintf` function is used to build the query string without the input having first been subjected to any validation. This vulnerability is fixed in 2.23.1.	2024-07-12	6.5	CVE-2024-39909
opensearch-project--observability	OpenSearch Observability is collection of plugins and applications that visualize data-driven events. An issue in the OpenSearch observability plugins allows unintended access to private tenant resources like notebooks. The system did not properly check if the user was the resource author when accessing resources in a private tenant, leading to potential data being revealed. The patches are included in OpenSearch 2.14.	2024-07-09	5.4	CVE-2024-39901
opensearch-project--reporting	OpenSearch Dashboards Reports allows 'Report Owner' export and share reports from OpenSearch Dashboards. An issue in the OpenSearch reporting plugin allows unintended access to private tenant resources like notebooks. The system did not properly check if the user was the resource author when accessing resources in a private tenant, leading to potential data being revealed. The patches are included in OpenSearch 2.14.	2024-07-09	5.4	CVE-2024-39900
optemiz--XPlainer WooCommerce Product FAQ [WooCommerce Accordion FAQ Plugin]	The XPlainer - WooCommerce Product FAQ [WooCommerce Accordion FAQ Plugin] plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ffw_activate_template' function in all versions up to, and including, 1.6.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to store cross-site scripting that will trigger when viewing the dashboard templates or accessing FAQs.	2024-07-09	6.4	CVE-2024-5669
optemiz--XPlainer WooCommerce Product FAQ [WooCommerce Accordion FAQ Plugin]	The XPlainer - WooCommerce Product FAQ [WooCommerce Accordion FAQ Plugin plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several functions in all versions up to, and including, 1.6.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to add new and update existing FAQs, FAQ lists, and modify FAQ associations with products.	2024-07-09	4.3	CVE-2024-5704
pandavideo--Panda Video	The Panda Video plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 1.4.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-09	6.4	CVE-2024-5457
Patreon--Patreon WordPress	Authentication Bypass by Spoofing vulnerability in Patreon Patreon WordPress allows Functionality Misuse.This issue affects Patreon WordPress: from n/a through 1.9.0.	2024-07-09	5.3	CVE-2024-37430
Pauple--Table & Contact Form 7 Database Tablesome	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Pauple Table & Contact Form 7 Database - Tablesome.This issue affects Table & Contact Form 7 Database - Tablesome: from n/a through 1.0.33.	2024-07-10	5.3	CVE-2024-37498
payflex -- payment_gateway	The Payflex Payment Gateway plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the payment_callback() function in all versions up to, and including, 2.5.0. This makes it possible for unauthenticated attackers to update the status of orders, which can potentially lead to revenue loss.	2024-07-11	5.3	CVE-2024-0619
petesheppard84--Extensions for	The Extensions for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's EE Events and EE Flipbox widgets in all versions up to,	2024-07-09	6.4	CVE-2024-4868

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Elementor	and including, 2.0.31 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
photoweblog--OSM OpenStreetMap	The OSM - OpenStreetMap plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'osm_map' shortcode in all versions up to, and including, 6.0.2 due to insufficient input sanitization and output escaping on user supplied attributes such as 'theme'. 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.	2024-07-09	6.4	CVE-2024-3603
pickplugins--Product Designer	The Product Designer plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the product_designer_ajax_delete_attach_id() function in all versions up to, and including, 1.0.33. This makes it possible for unauthenticated attackers to delete arbitrary attachments.	2024-07-09	5.3	CVE-2024-3608
Ping Identity--PingFederate	The deploy directory in PingFederate runtime nodes is reachable to unauthorized users.	2024-07-09	5.3	CVE-2024-22377
plugin-devs --blog\,_posts_and_category_filter_for_elementor	The Blog, Posts and Category Filter for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Post and Category Filter widget in all versions up to, and including, 1.0.3 due to insufficient input sanitization and output escaping on user supplied 'post_types' attribute. 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.	2024-07-09	5.4	CVE-2024-4667
PrivateBin--PrivateBin	PrivateBin is an online pastebin where the server has zero knowledge of pasted data. In v1.5, PrivateBin introduced the YOURLS server-side proxy. The idea was to allow using the YOURLs URL shortener without running the YOURLs instance without authentication and/or exposing the authentication token to the public, allowing anyone to shorten any URL. With the proxy mechanism, anyone can shorten any URL pointing to the configured PrivateBin instance. The vulnerability allowed other URLs to be shortened, as long as they contain the PrivateBin instance, defeating the limit imposed by the proxy. This vulnerability is fixed in 1.7.4.	2024-07-09	5.3	CVE-2024-39899
project-zot--zot	zot is an OCI image registry. Prior to 2.1.0, the cache driver `GetBlob()` allows read access to any blob without access control check. If a Zot `accessControl` policy allows users read access to some repositories but restricts read access to other repositories and `dedupe` is enabled (it is enabled by default), then an attacker who knows the name of an image and the digest of a blob (that they do not have read access to), they may maliciously read it via a second repository they do have read access to. This attack is possible because [`ImageStore.CheckBlob()` calls `checkCacheBlob()`](https://github.com/project-zot/zot/blob/v2.1.0-rc2/pkg/storage/imagestore/imagestore.go#L1158-L1159) to find the blob a global cache by searching for the digest. If it is found, it is copied to the user requested repository with `copyBlob()`. The attack may be mitigated by configuring "dedupe": false in the "storage" settings. The vulnerability is fixed in 2.1.0.	2024-07-09	4.3	CVE-2024-39897
publiccms --publiccms	PublicCMS v4.0.202302.e was discovered to contain an arbitrary file content replacement vulnerability via the component /admin/cmsTemplate/replace.	2024-07-12	6.5	CVE-2024-40547
RadiusTheme--ShopBuilder Elementor WooCommerce	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in RadiusTheme ShopBuilder - Elementor WooCommerce Builder Addons allows Path Traversal.This issue affects ShopBuilder - Elementor WooCommerce Builder Addons: from n/a through 2.1.12.	2024-07-09	6.5	CVE-2024-37520

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Builder Addons				
randombit--botan	Botan is a C++ cryptography library. X.509 certificates can identify elliptic curves using either an object identifier or using explicit encoding of the parameters. Prior to 3.5.0 and 2.19.5, checking name constraints in X.509 certificates is quadratic in the number of names and name constraints. An attacker who presented a certificate chain which contained a very large number of names in the SubjectAlternativeName, signed by a CA certificate which contained a large number of name constraints, could cause a denial of service. The problem has been addressed in Botan 3.5.0 and a partial backport has also been applied and is included in Botan 2.19.5.	2024-07-08	5.3	CVE-2024-34702
randombit--botan	Botan is a C++ cryptography library. X.509 certificates can identify elliptic curves using either an object identifier or using explicit encoding of the parameters. A bug in the parsing of name constraint extensions in X.509 certificates meant that if the extension included both permitted subtrees and excluded subtrees, only the permitted subtree would be checked. If a certificate included a name which was permitted by the permitted subtree but also excluded by excluded subtree, it would be accepted. Fixed in versions 3.5.0 and 2.19.5.	2024-07-08	5.3	CVE-2024-39312
realmag777--WPCS	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in realmag777 WPCS allows Code Injection.This issue affects WPCS: from n/a through 1.2.0.3.	2024-07-12	6.5	CVE-2024-38700
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in OpenJPEG. A resource exhaustion can occur in the opj_t1_decode_cblks function in tcd.c through a crafted image file, causing a denial of service.	2024-07-13	6.5	CVE-2023-39329
Red Hat--Red Hat Enterprise Linux 6	A vulnerability was found in OpenJPEG similar to CVE-2019-6988. This flaw allows an attacker to bypass existing protections and cause an application crash through a maliciously crafted file.	2024-07-09	5.5	CVE-2023-39328
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in OpenJPEG. Maliciously constructed pictures can cause the program to enter a large loop and continuously print warning messages on the terminal.	2024-07-13	4.3	CVE-2023-39327
Red Hat--Red Hat JBoss Enterprise Application Platform 8	A vulnerability was found in Undertow. This issue requires enabling the learning-push handler in the server's config, which is disabled by default, leaving the maxAge config in the handler unconfigured. The default is -1, which makes the handler vulnerable. If someone overwrites that config, the server is not subject to the attack. The attacker needs to be able to reach the server with a normal HTTP request.	2024-07-08	5.3	CVE-2024-3653
redhat -- directory_server	A flaw was found in the 389 Directory Server. This flaw allows an unauthenticated user to cause a systematic server crash while sending a specific extended search request, leading to a denial of service.	2024-07-09	6.5	CVE-2024-6237
rensas -- arm-trusted-firmware	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in Renesas arm-trusted-firmware allows Local Execution of Code. This vulnerability is associated with program files https://github.Com/renesas-rcar/arm-trusted-firmware/blob/rcar_gen3_v2.5/drivers/renesas/common/io/i... https://github.Com/renesas-rcar/arm-trusted-firmware/blob/rcar_gen3_v2.5/drivers/renesas/common/io/io_rcar.C . In line 313 "addr_loaded_cnt" is checked not to be "CHECK_IMAGE_AREA_CNT" (5) or larger, this check does not halt the function. Immediately after (line 317) there will be an overflow in the buffer and the value of "dst" will be written to the area immediately after the buffer, which is "addr_loaded_cnt". This will allow an	2024-07-08	6.7	CVE-2024-6563

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to freely control the value of "addr_loaded_cnt" and thus control the destination of the write immediately after (line 318). The write in line 318 will then be fully controlled by said attacker, with whichever address and whichever value ("len") they desire.			
rensas -- arm-trusted-firmware	Buffer overflow in "rcar_dev_init" due to using due to using untrusted data (rcar_image_number) as a loop counter before verifying it against RCAR_MAX_BL3X_IMAGE. This could lead to a full bypass of secure boot.	2024-07-08	6.7	CVE-2024-6564
rico-macchi--WP Links Page	The WP Links Page plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'wplf_ajax_update_screenshots' function in all versions up to, and including, 4.9.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to regenerate the link's thumbnail image.	2024-07-13	4.3	CVE-2024-6465
samsung -- android	Use of implicit intent for sensitive communication in Samsung Messages prior to SMR Jul-2024 Release 1 allows local attackers to get sensitive information. User interaction is required for triggering this vulnerability.	2024-07-08	5.5	CVE-2024-34602
samsung -- android	Improper access control in Samsung Message prior to SMR Jul-2024 Release 1 allows local attackers to access location data.	2024-07-08	5.5	CVE-2024-34603
SAP_SE--SAP Business Warehouse - Business Planning and Simulation	SAP Business Warehouse - Business Planning and Simulation application does not sufficiently encode user controlled inputs, resulting in Reflected Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker can cause low impact on the confidentiality and integrity of the application.	2024-07-09	6.1	CVE-2024-39594
SAP_SE--SAP Business Warehouse - Business Planning and Simulation	SAP Business Warehouse - Business Planning and Simulation application does not sufficiently encode user-controlled inputs, resulting in Stored Cross-Site Scripting (XSS) vulnerability. This vulnerability allows users to modify website content and on successful exploitation, an attacker can cause low impact to the confidentiality and integrity of the application.	2024-07-09	5.4	CVE-2024-39595
SAP_SE--SAP Business Workflow (WebFlow Services)	WebFlow Services of SAP Business Workflow allows an authenticated attacker to enumerate accessible HTTP endpoints in the internal network by specially crafting HTTP requests. On successful exploitation this can result in information disclosure. It has no impact on integrity and availability of the application.	2024-07-09	5	CVE-2024-34689
SAP_SE--SAP CRM WebClient UI	Due to insufficient input validation, SAP CRM WebClient UI allows an unauthenticated attacker to craft a URL link which embeds a malicious script. When a victim clicks on this link, the script will be executed in the victim's browser giving the attacker the ability to access and/or modify information with no effect on availability of the application.	2024-07-09	6.1	CVE-2024-37173
SAP_SE--SAP CRM WebClient UI	Custom CSS support option in SAP CRM WebClient UI does not sufficiently encode user-controlled inputs resulting in Cross-Site Scripting vulnerability. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application.	2024-07-09	6.1	CVE-2024-37174
SAP_SE--SAP CRM WebClient UI	SAP CRM (WebClient UI Framework) allows an authenticated attacker to enumerate accessible HTTP endpoints in the internal network by specially crafting HTTP requests. On successful exploitation this can result in information disclosure. It has no impact on integrity and availability of the application.	2024-07-09	5	CVE-2024-39598
SAP_SE--SAP CRM WebClient UI	SAP CRM WebClient does not perform necessary authorization check for an authenticated user, resulting in escalation of privileges. This could allow an attacker to access some sensitive information.	2024-07-09	4.3	CVE-2024-37175

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SAP_SE--SAP Enable Now	Due to missing authorization checks, SAP Enable Now allows an author to escalate privileges to access information which should otherwise be restricted. On successful exploitation, the attacker can cause limited impact on confidentiality of the application.	2024-07-09	4.3	CVE-2024-39596
SAP_SE--SAP GUI for Windows	Under certain conditions, the memory of SAP GUI for Windows contains the password used to log on to an SAP system, which might allow an attacker to get hold of the password and impersonate the affected user. As a result, it has a high impact on the confidentiality but there is no impact on the integrity and availability.	2024-07-09	5	CVE-2024-39600
SAP_SE--SAP Landscape Management	SAP Landscape Management allows an authenticated user to read confidential data disclosed by the REST Provider Definition response. Successful exploitation can cause high impact on confidentiality of the managed entities.	2024-07-09	6.9	CVE-2024-39593
SAP_SE--SAP NetWeaver Application Server for ABAP and ABAP Platform	Under certain conditions SAP NetWeaver Application Server for ABAP and ABAP Platform allows an attacker to access remote-enabled function module with no further authorization which would otherwise be restricted, the function can be used to read non-sensitive information with low impact on confidentiality of the application.	2024-07-09	4.1	CVE-2024-37180
SAP_SE--SAP NetWeaver Application Server for ABAP and ABAP Platform	Due to a Protection Mechanism Failure in SAP NetWeaver Application Server for ABAP and ABAP Platform, a developer can bypass the configured malware scanner API because of a programming error. This leads to a low impact on the application's confidentiality, integrity, and availability.	2024-07-09	4.7	CVE-2024-39599
SAP_SE--SAP NetWeaver Knowledge Management XMLEditor	Due to weak encoding of user-controlled input in SAP NetWeaver Knowledge Management XMLEditor which allows malicious scripts can be executed in the application, potentially leading to a Cross-Site Scripting (XSS) vulnerability. This has no impact on the availability of the application but it has a low impact on its confidentiality and integrity.	2024-07-09	6.1	CVE-2024-34685
SAP_SE--SAP S/4HANA Finance (Advanced Payment Management)	SAP S/4HANA Finance (Advanced Payment Management) does not perform necessary authorization check for an authenticated user, resulting in escalation of privileges. As a result, it has a low impact to confidentiality and availability but there is no impact on the integrity.	2024-07-09	5.4	CVE-2024-37172
SAP_SE--SAP Transportation Management (Collaboration Portal)	SAP Transportation Management (Collaboration Portal) allows an attacker with non-administrative privileges to send a crafted request from a vulnerable web application. This will trigger the application handler to send a request to an unintended service, which may reveal information about that service. The information obtained could be used to target internal systems behind firewalls that are normally inaccessible to an attacker from the external network, resulting in a Server-Side Request Forgery vulnerability. There is no effect on integrity or availability of the application.	2024-07-09	5	CVE-2024-37171
Saturday Drive--Ninja Forms	Improper Control of Generation of Code ('Code Injection') vulnerability in Saturday Drive Ninja Forms allows Code Injection.This issue affects Ninja Forms: from n/a through 3.8.4.	2024-07-09	5.4	CVE-2024-37934
schneider-electric--ecostruxure_foxboro_dcs_control_co	CWE-129: Improper Validation of Array Index vulnerability exists that could cause local denial-of-service when a malicious actor with local user access crafts a script/program using an IOCTL call in the Foxboro.sys driver.	2024-07-11	5.5	CVE-2024-5680 cybersecurity@se.com

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
re_services				
schneider-electric--modicon_m241_firmware	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause a vulnerability leading to a cross-site scripting condition where attackers can have a victim's browser run arbitrary JavaScript when they visit a page containing the injected payload.	2024-07-11	6.1	CVE-2024-6528 cybersecurity@se.com
ServiceNow--Now Platform	ServiceNow has addressed a sensitive file read vulnerability that was identified in the Washington DC, Vancouver, and Utah Now Platform releases. This vulnerability could allow an administrative user to gain unauthorized access to sensitive files on the web application server.Â The vulnerability is addressed in the listed patches and hot fixes, which were released during the June 2024 patching cycle. If you have not done so already, we recommend applying security patches relevant to your instance as soon as possible.	2024-07-10	4.9	CVE-2024-5178
SERVIT Software Solutions--affiliate-toolkit	Insertion of Sensitive Information into Log File vulnerability in SERVIT Software Solutions.This issue affects affiliate-toolkit: from n/a through 3.4.4.	2024-07-10	5.3	CVE-2024-37205
Siemens--RUGGEDCOM RMC8388 V5.X	A vulnerability has been identified in RUGGEDCOM RMC8388 V5.X (All versions < V5.9.0), RUGGEDCOM RMC8388NC V5.X (All versions < V5.9.0), RUGGEDCOM RS416NCv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416PNCv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416Pv2 V5.X (All versions < V5.9.0), RUGGEDCOM RS416v2 V5.X (All versions < V5.9.0), RUGGEDCOM RS900 (32M) V5.X (All versions < V5.9.0), RUGGEDCOM RS900G (32M) V5.X (All versions < V5.9.0), RUGGEDCOM RS900GNC(32M) V5.X (All versions < V5.9.0), RUGGEDCOM RS900NC(32M) V5.X (All versions < V5.9.0), RUGGEDCOM RSG2100 (32M) V5.X (All versions < V5.9.0), RUGGEDCOM RSG2100NC(32M) V5.X (All versions < V5.9.0), RUGGEDCOM RSG2288 V5.X (All versions < V5.9.0), RUGGEDCOM RSG2288NC V5.X (All versions < V5.9.0), RUGGEDCOM RSG2300 V5.X (All versions < V5.9.0), RUGGEDCOM RSG2300NC V5.X (All versions < V5.9.0), RUGGEDCOM RSG2300P V5.X (All versions < V5.9.0), RUGGEDCOM RSG2300PNC V5.X (All versions < V5.9.0), RUGGEDCOM RSG2488 V5.X (All versions < V5.9.0), RUGGEDCOM RSG2488NC V5.X (All versions < V5.9.0), RUGGEDCOM RSG907R (All versions < V5.9.0), RUGGEDCOM RSG908C (All versions < V5.9.0), RUGGEDCOM RSG909R (All versions < V5.9.0), RUGGEDCOM RSG910C (All versions < V5.9.0), RUGGEDCOM RSG920P V5.X (All versions < V5.9.0), RUGGEDCOM RSG920PNC V5.X (All versions < V5.9.0), RUGGEDCOM RSL910 (All versions < V5.9.0), RUGGEDCOM RSL910NC (All versions < V5.9.0), RUGGEDCOM RST2228 (All versions < V5.9.0), RUGGEDCOM RST2228P (All versions < V5.9.0), RUGGEDCOM RST916C (All versions < V5.9.0), RUGGEDCOM RST916P (All versions < V5.9.0). The affected products with IP forwarding enabled wrongly make available certain remote services in non-managed VLANs, even if these services are not intentionally activated. An attacker could leverage this vulnerability to create a remote shell to the affected system.	2024-07-09	6.6	CVE-2024-38278
Siemens--RUGGEDCOM RST2228	A vulnerability has been identified in RUGGEDCOM RST2228 (All versions < V5.9.0), RUGGEDCOM RST2228P (All versions < V5.9.0). The web server of the affected systems leaks the MACSEC key in clear text to a logged in user. An attacker with the credentials of a low privileged user could retrieve the MACSEC key and access (decrypt) the ethernet frames sent by authorized recipients.	2024-07-09	4.3	CVE-2023-52238
Siemens--SIMATIC Energy Manager Basic	A vulnerability has been identified in SIMATIC Energy Manager Basic (All versions < V7.5), SIMATIC Energy Manager PRO (All versions < V7.5), SIMATIC IPC DiagBase (All versions), SIMATIC IPC DiagMonitor (All versions), SIMIT V10 (All versions), SIMIT V11 (All versions < V11.1). Unified Automation .NET based OPC UA Server SDK before 3.2.2 used in Siemens products are affected by a similar vulnerability as documented in CVE-2023-27321 for the OPC Foundation UA .NET Standard	2024-07-09	5.3	CVE-2023-52891

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	implementation. A successful attack may lead to high load situation and memory exhaustion, and may block the server.			
Siemens--SIMATIC PCS 7 V9.1	A vulnerability has been identified in SIMATIC PCS 7 V9.1 (All versions), SIMATIC WinCC Runtime Professional V18 (All versions), SIMATIC WinCC Runtime Professional V19 (All versions < V19 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 23), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 17), SIMATIC WinCC V8.0 (All versions < V8.0 Update 5). The affected products do not properly handle certain requests to their web application, which may lead to the leak of privileged information. This could allow an unauthenticated remote attacker to retrieve information such as users and passwords.	2024-07-09	5.9	CVE-2024-30321
Siemens--SIMATIC STEP 7 Safety V16	A vulnerability has been identified in SIMATIC STEP 7 Safety V16 (All versions < V16 Update 7), SIMATIC STEP 7 Safety V17 (All versions < V17 Update 7), SIMATIC STEP 7 Safety V18 (All versions < V18 Update 2), SIMATIC STEP 7 V16 (All versions < V16 Update 7), SIMATIC STEP 7 V17 (All versions < V17 Update 7), SIMATIC STEP 7 V18 (All versions < V18 Update 2), SIMATIC WinCC Unified V16 (All versions < V16 Update 7), SIMATIC WinCC Unified V17 (All versions < V17 Update 7), SIMATIC WinCC Unified V18 (All versions < V18 Update 2), SIMATIC WinCC V16 (All versions < V16.7), SIMATIC WinCC V17 (All versions < V17.7), SIMATIC WinCC V18 (All versions < V18 Update 2), SIMOCODE ES V16 (All versions < V16 Update 7), SIMOCODE ES V17 (All versions < V17 Update 7), SIMOCODE ES V18 (All versions < V18 Update 2), SIMOTION SCOUT TIA V5.4 SP1 (All versions), SIMOTION SCOUT TIA V5.4 SP3 (All versions), SIMOTION SCOUT TIA V5.5 SP1 (All versions), SINAMICS Startdrive V16 (All versions), SINAMICS Startdrive V17 (All versions), SINAMICS Startdrive V18 (All versions), SIRIUS Safety ES V17 (All versions < V17 Update 7), SIRIUS Safety ES V18 (All versions < V18 Update 2), SIRIUS Soft Starter ES V17 (All versions < V17 Update 7), SIRIUS Soft Starter ES V18 (All versions < V18 Update 2), Soft Starter ES V16 (All versions < V16 Update 7), TIA Portal Cloud V3.0 (All versions < V18 Update 2). Affected applications do not properly restrict the .NET BinaryFormatter when deserializing hardware configuration profiles. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application. This is the same issue that exists for .NET BinaryFormatter https://docs.microsoft.com/en-us/visualstudio/code-quality/ca2300.	2024-07-09	6.5	CVE-2023-32735
Siemens--SIMATIC STEP 7 Safety V18	A vulnerability has been identified in SIMATIC STEP 7 Safety V18 (All versions < V18 Update 2). Affected applications do not properly restrict the .NET BinaryFormatter when deserializing user-controllable input. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application. This is the same issue that exists for .NET BinaryFormatter https://docs.microsoft.com/en-us/visualstudio/code-quality/ca2300.	2024-07-09	6.3	CVE-2023-32737
Siemens--SINEMA Remote Connect Client	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.2 HF1). The system service of affected applications is vulnerable to command injection due to missing server side input sanitation when loading VPN configurations. This could allow an administrative remote attacker running a corresponding SINEMA Remote Connect Server to execute arbitrary code with system privileges on the client system.	2024-07-09	6.6	CVE-2024-39569
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected products allow to upload certificates. An authenticated attacker could upload a crafted certificates leading to a permanent denial-of-service situation. In order to recover from such an attack, the offending certificate needs to be removed manually.	2024-07-09	6.5	CVE-2024-39869
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected applications can be configured to allow users to manage own users. A local authenticated user with this privilege could use this modify users outside of their own scope as well as to escalate privileges.	2024-07-09	6.3	CVE-2024-39870

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected applications do not properly separate the rights to edit device settings and to edit settings for communication relations. This could allow an authenticated attacker with the permission to manage devices to gain access to participant groups that the attacked does not belong to.	2024-07-09	6.3	CVE-2024-39871
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). The affected application allows authenticated, low privilege users with the 'Manage own remote connections' permission to retrieve details about other users and group memberships.	2024-07-09	4.3	CVE-2024-39875
Siemens--SINEMA Remote Connect Server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2 SP1). Affected applications do not properly handle log rotation. This could allow an unauthenticated remote attacker to cause a denial of service condition through resource exhaustion on the device.	2024-07-09	4	CVE-2024-39876
Siemens--SIPROTEC 5 6MD84 (CP300)	A vulnerability has been identified in SIPROTEC 5 6MD84 (CP300) (All versions < V9.64), SIPROTEC 5 6MD85 (CP200) (All versions), SIPROTEC 5 6MD85 (CP300) (All versions < V9.64), SIPROTEC 5 6MD86 (CP200) (All versions), SIPROTEC 5 6MD86 (CP300) (All versions < V9.64), SIPROTEC 5 6MD89 (CP300) (All versions < V9.64), SIPROTEC 5 6MU85 (CP300) (All versions < V9.64), SIPROTEC 5 7KE85 (CP200) (All versions), SIPROTEC 5 7KE85 (CP300) (All versions < V9.64), SIPROTEC 5 7SA82 (CP100) (All versions), SIPROTEC 5 7SA82 (CP150) (All versions < V9.65), SIPROTEC 5 7SA84 (CP200) (All versions), SIPROTEC 5 7SA86 (CP200) (All versions), SIPROTEC 5 7SA86 (CP300) (All versions < V9.65), SIPROTEC 5 7SA87 (CP200) (All versions), SIPROTEC 5 7SA87 (CP300) (All versions < V9.65), SIPROTEC 5 7SD82 (CP100) (All versions), SIPROTEC 5 7SD82 (CP150) (All versions < V9.65), SIPROTEC 5 7SD84 (CP200) (All versions), SIPROTEC 5 7SD86 (CP200) (All versions), SIPROTEC 5 7SD86 (CP300) (All versions < V9.65), SIPROTEC 5 7SD87 (CP200) (All versions), SIPROTEC 5 7SD87 (CP300) (All versions < V9.65), SIPROTEC 5 7SJ81 (CP100) (All versions < V8.89), SIPROTEC 5 7SJ81 (CP150) (All versions < V9.65), SIPROTEC 5 7SJ82 (CP100) (All versions < V8.89), SIPROTEC 5 7SJ82 (CP150) (All versions < V9.65), SIPROTEC 5 7SJ85 (CP200) (All versions), SIPROTEC 5 7SJ85 (CP300) (All versions < V9.65), SIPROTEC 5 7SJ86 (CP200) (All versions), SIPROTEC 5 7SJ86 (CP300) (All versions < V9.65), SIPROTEC 5 7SK82 (CP100) (All versions < V8.89), SIPROTEC 5 7SK82 (CP150) (All versions < V9.65), SIPROTEC 5 7SK85 (CP200) (All versions), SIPROTEC 5 7SK85 (CP300) (All versions < V9.65), SIPROTEC 5 7SL82 (CP100) (All versions), SIPROTEC 5 7SL82 (CP150) (All versions < V9.65), SIPROTEC 5 7SL86 (CP200) (All versions), SIPROTEC 5 7SL86 (CP300) (All versions < V9.65), SIPROTEC 5 7SL87 (CP200) (All versions), SIPROTEC 5 7SL87 (CP300) (All versions < V9.65), SIPROTEC 5 7SS85 (CP200) (All versions), SIPROTEC 5 7SS85 (CP300) (All versions < V9.64), SIPROTEC 5 7ST85 (CP200) (All versions), SIPROTEC 5 7ST85 (CP300) (All versions < V9.64), SIPROTEC 5 7ST86 (CP300) (All versions < V9.64), SIPROTEC 5 7SX82 (CP150) (All versions < V9.65), SIPROTEC 5 7SX85 (CP300) (All versions < V9.65), SIPROTEC 5 7UM85 (CP300) (All versions < V9.64), SIPROTEC 5 7UT82 (CP100) (All versions), SIPROTEC 5 7UT82 (CP150) (All versions < V9.65), SIPROTEC 5 7UT85 (CP200) (All versions), SIPROTEC 5 7UT85 (CP300) (All versions < V9.65), SIPROTEC 5 7UT86 (CP200) (All versions), SIPROTEC 5 7UT86 (CP300) (All versions < V9.65), SIPROTEC 5 7UT87 (CP200) (All versions), SIPROTEC 5 7UT87 (CP300) (All versions < V9.65), SIPROTEC 5 7VE85 (CP300) (All versions < V9.64), SIPROTEC 5 7VK87 (CP200) (All versions), SIPROTEC 5 7VK87 (CP300) (All versions < V9.65), SIPROTEC 5 7VU85 (CP300) (All versions < V9.64), SIPROTEC 5 Communication Module ETH-BA-2EL (Rev.1) (All versions < V9.62 installed on CP150 and CP300 devices), SIPROTEC 5 Communication Module ETH-BA-2EL (Rev.1) (All versions installed on CP200 devices), SIPROTEC 5 Communication Module ETH-BA-2EL (Rev.1) (All versions < V8.89 installed on CP100 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (Rev. 1) (All versions installed on CP200 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (Rev. 1) (All versions < V9.62 installed on CP150 and CP300 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (Rev. 1) (All versions < V8.89 installed on CP100 devices), SIPROTEC 5 Communication	2024-07-09	5.9	CVE-2024-38867

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Module ETH-BD-2FO (All versions < V9.62), SIPROTEC 5 Compact 7SX800 (CP050) (All versions < V9.64). The affected devices are supporting weak ciphers on several ports (443/tcp for web, 4443/tcp for DIGSI 5 and configurable port for syslog over TLS). This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over to and from those ports.			
sirv--Image Optimizer, Resizer and CDN Sirv	The Image Optimizer, Resizer and CDN - Sirv plugin for WordPress is vulnerable to unauthorized plugin settings modification due to missing capability checks on the plugin functions in all versions up to, and including, 7.2.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change the connected Sirv account to an attacker-controlled one.	2024-07-11	5.4	CVE-2024-6392
slui--Media Hygiene: Remove or Delete Unused Images and More!	The Media Hygiene: Remove or Delete Unused Images and More! plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the bulk_action_delete and delete_single_image_call AJAX actions in all versions up to, and including, 3.0.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary attachments. A nonce check was added in version 3.0.1, however, it wasn't until version 3.0.2 that a capability check was added.	2024-07-09	4.3	CVE-2024-5855
smashballoon -- feeds_for_youtube	The Feeds for YouTube (YouTube video, channel, and gallery plugin) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'youtube-feed' shortcode in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-11	5.4	CVE-2024-6256
smub--Duplicator Migration & Backup Plugin	The Duplicator plugin for WordPress is vulnerable to information exposure in all versions up to, and including, 1.5.9. 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.	2024-07-11	5.3	CVE-2024-6210
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 Stored Cross-Site Scripting via the 'id' attribute within the plugin's sonaar_audioplayer shortcode in all versions up to, and including, 5.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-10	6.4	CVE-2024-5664
SourceCodester--Employee and Visitor Gate Pass Logging System	A vulnerability has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0 and classified as problematic. Affected by this vulnerability is the function save_users of the file Users.php. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-271057 was assigned to this vulnerability.	2024-07-10	4.3	CVE-2024-6649
squelch--Squelch Tabs and Accordions Shortcodes	The Squelch Tabs and Accordions Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tab' shortcode in all versions up to, and including, 0.4.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-09	6.4	CVE-2024-5946
stellarwp--LearnDash LMS Reports	The LearnDash LMS - Reports plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several functions in all versions up to, and including, 1.8.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update various plugin settings.	2024-07-09	5.4	CVE-2024-5648

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stijnvanderree--Laposta	The Laposta plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.12. This is due to the plugin not preventing direct access to several 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. This plugin is no longer being maintained and has been closed for downloads.	2024-07-13	5.3	CVE-2024-6574
stitionai -- devika	A stored Cross-Site Scripting (XSS) vulnerability exists in the stitionai/devika chat feature, allowing attackers to inject malicious payloads into the chat input. This vulnerability is due to the lack of input validation and sanitization on both the frontend and backend components of the application. Specifically, the application fails to sanitize user input in the chat feature, leading to the execution of arbitrary JavaScript code in the context of the user's browser session. This issue affects all versions of the application. The impact of this vulnerability includes the potential for stolen credentials, extraction of sensitive information from chat logs, projects, and other data accessible through the application.	2024-07-08	6.1	CVE-2024-5711
studiopress--Genesis Blocks	The Genesis Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Sharing block in all versions up to, and including, 3.1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-09	6.4	CVE-2024-3563
Themeum--Tutor LMS	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Themeum Tutor LMS allows Path Traversal.This issue affects Tutor LMS: from n/a through 2.7.1.	2024-07-09	4.9	CVE-2024-37266
timersys--WP Popups WordPress Popup builder	The WP Popups - WordPress Popup builder plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 2.2.0.1. This is due the plugin utilizing mobiledetect without preventing direct access to the 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.	2024-07-12	5.3	CVE-2024-6555
Tobias Conrad--Get Better Reviews for WooCommerce	Missing Authorization vulnerability in Tobias Conrad Get Better Reviews for WooCommerce.This issue affects Get Better Reviews for WooCommerce: from n/a through 4.0.6.	2024-07-12	4.3	CVE-2024-37544
tranbinhcse--Webico Slider Flatsome Addons	The Webico Slider Flatsome Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wbc_image shortcode in all versions up to, and including, 2.0.1 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.	2024-07-09	6.4	CVE-2024-5881
TrustedLogin--TrustedLogin Vendor	Insertion of Sensitive Information into Log File vulnerability in TrustedLogin TrustedLogin Vendor.This issue affects TrustedLogin Vendor: from n/a before 1.1.1.	2024-07-10	5.3	CVE-2024-37270
tyxla--Gravity Forms: Multiple Form Instances	The Gravity Forms: Multiple Form Instances plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 1.1.1. This is due to the plugin 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	2024-07-10	5.3	CVE-2024-6550

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	own, and requires another vulnerability to be present for damage to an affected website.			
Unknown--DN Footer Contacts	The DN Footer Contacts WordPress plugin before 1.6.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	2024-07-09	4.3	CVE-2024-3410
Unknown--Social Media Widget	The Social Media Widget WordPress plugin before 4.0.9 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)	2024-07-12	4.8	CVE-2024-0974
Unknown--socialdriver-framework	The socialdriver-framework WordPress plugin before 2024.04.30 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)	2024-07-12	4.8	CVE-2024-2696
unlimited-elements -- unlimited_elements_for_elementor_\(free_widgets\,_addons\,_templates\)	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'username' parameter in all versions up to, and including, 1.5.112 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above and granted plugin setting edit permissions by an administrator, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-09	5.4	CVE-2024-6169
unlimited-elements -- unlimited_elements_for_elementor_\(free_widgets\,_addons\,_templates\)	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'email' parameter in all versions up to, and including, 1.5.112 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.	2024-07-09	5.4	CVE-2024-6170
unlimited-elements -- unlimited_elements_for_elementor_\(free_widgets\,_addons\,_templates\)	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to IP Address Spoofing in all versions up to, and including, 1.5.112 due to insufficient IP address validation and/or use of user-supplied HTTP headers as a primary method for IP retrieval. This makes it possible for unauthenticated attackers to bypass antispam functionality in the Form Builder widgets.	2024-07-09	5.3	CVE-2024-6171
vaethink -- vaethink	vaeThink 1.0.2 is vulnerable to stored Cross Site Scripting (XSS) in the system backend.	2024-07-09	5.4	CVE-2024-38971
vaethink -- vaethink	vaeThink 1.0.2 is vulnerable to Information Disclosure via the system backend,access management administrator function.	2024-07-09	4.9	CVE-2024-38970
vCita--Online Booking & Scheduling Calendar for WordPress by vcita	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in vCita Online Booking & Scheduling Calendar for WordPress by vcita allows Path Traversal.This issue affects Online Booking & Scheduling Calendar for WordPress by vcita: from n/a through 4.4.2.	2024-07-09	6.5	CVE-2024-37499

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
VolThemes--Patricia Lite	Cross-Site Request Forgery (CSRF) vulnerability in VolThemes Patricia Lite.This issue affects Patricia Lite: from n/a through 1.2.3.	2024-07-12	4.3	CVE-2024-37939
wagtail--wagtail	Wagtail is an open source content management system built on Django. A bug in Wagtail's `parse_query_string` would result in it taking a long time to process suitably crafted inputs. When used to parse sufficiently long strings of characters without a space, `parse_query_string` would take an unexpectedly large amount of time to process, resulting in a denial of service. In an initial Wagtail installation, the vulnerability can be exploited by any Wagtail admin user. It cannot be exploited by end users. If your Wagtail site has a custom search implementation which uses `parse_query_string`, it may be exploitable by other users (e.g. unauthenticated users). Patched versions have been released as Wagtail 5.2.6, 6.0.6 and 6.1.3.	2024-07-11	6.5	CVE-2024-39317
Webmin--Webmin	Cross-site scripting vulnerability exists in session_login.cgi of Webmin versions prior to 1.970 and Usermin versions prior to 1.820. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the user who accessed the website using the product. As a result, a webpage may be altered or sensitive information such as a credential may be disclosed.	2024-07-10	6.1	CVE-2024-36453
witmy--my-springsecurity-plus	A vulnerability has been found in witmy my-springsecurity-plus up to 2024-07-03 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /api/user. The manipulation of the argument params.dataScope leads to sql injection. The attack can be launched 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. The associated identifier of this vulnerability is VDB-271111.	2024-07-11	6.3	CVE-2024-6676
witmy--my-springsecurity-plus	A vulnerability classified as critical has been found in witmy my-springsecurity-plus up to 2024-07-04. Affected is an unknown function of the file /api/role. The manipulation of the argument params.dataScope leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-271152.	2024-07-11	6.3	CVE-2024-6679
witmy--my-springsecurity-plus	A vulnerability classified as critical was found in witmy my-springsecurity-plus up to 2024-07-04. Affected by this vulnerability is an unknown functionality of the file /api/dept/build. The manipulation of the argument params.dataScope leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-271153 was assigned to this vulnerability.	2024-07-11	6.3	CVE-2024-6680
witmy--my-springsecurity-plus	A vulnerability, which was classified as critical, has been found in witmy my-springsecurity-plus up to 2024-07-04. Affected by this issue is some unknown functionality of the file /api/dept. The manipulation of the argument params.dataScope leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-271154 is the identifier assigned to this vulnerability.	2024-07-11	6.3	CVE-2024-6681
wp2speed--WP2Speed Faster Optimize PageSpeed Insights Score 90-100	The WP2Speed Faster - Optimize PageSpeed Insights Score 90-100 plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 1.0.1. This is due to the use of hardcoded credentials to authenticate all the incoming API requests. This makes it possible for unauthenticated attackers to overwrite CSS, update the trial settings, purge the cache, and find attachments.	2024-07-09	5.3	CVE-2024-5810
wpbits--WPBITS Addons For Elementor Page Builder	The WPBITS Addons For Elementor Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several widgets in all versions up to, and including, 1.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2024-07-09	6.4	CVE-2024-4862

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wpkube--Social Sharing Plugin Kiwi	The Social Sharing Plugin - Kiwi plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 2.1.7 via the 'kiwi-nw-pinterest' class. This makes it possible for unauthenticated attackers to view limited content from password protected posts.	2024-07-09	5.3	CVE-2024-3228
wpmudev -- branda	The Branda - White Label WordPress, Custom Login Page Customizer plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.4.18. This is due the plugin utilizing composer without preventing direct access to the 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.	2024-07-11	5.3	CVE-2024-6554
wpmudev--SmartCrawl WordPress SEO checker, SEO analyzer, SEO optimizer	The SmartCrawl WordPress SEO checker, SEO analyzer, SEO optimizer plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.10.8. This is due the plugin utilizing mobiledetect without preventing direct access to the 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.	2024-07-10	5.3	CVE-2024-6556
wppuzzle--Comment Images Reloaded	The Comment Images Reloaded plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the cir_delete_image AJAX action in all versions up to, and including, 2.2.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary media attachments.	2024-07-09	4.3	CVE-2024-5856
wpweb--WooCommerce Social Login	Deserialization of Untrusted Data vulnerability in wpweb WooCommerce Social Login.This issue affects WooCommerce Social Login: from n/a through 2.6.3.	2024-07-09	5.4	CVE-2024-37502
WPZOOM--Beaver Builder Addons by WPZOOM	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WPZOOM Beaver Builder Addons by WPZOOM allows Path Traversal.This issue affects Beaver Builder Addons by WPZOOM: from n/a through 1.3.5.	2024-07-09	4.9	CVE-2024-37464
WuKongOpenSource--Wukong_nocode	A vulnerability was found in WuKongOpenSource Wukong_nocode up to 20230807. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file ExpressionUtil.java of the component AviatorScript Handler. The manipulation leads to deserialization. The attack can be launched 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. The associated identifier of this vulnerability is VDB-271051.	2024-07-10	6.3	CVE-2024-6645
zblogcn -- z-blogphp	A cross-site scripting (XSS) vulnerability in the Backend Theme Management module of Z-BlogPHP v1.7.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	2024-07-08	6.1	CVE-2024-39203
zmops--ArgusDBM	A vulnerability was found in zmops ArgusDBM up to 0.1.0. It has been classified as critical. Affected is the function getDefaultClassLoader of the file CalculateAlarm.java of the component AviatorScript Handler. The manipulation leads to deserialization. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-271050 is the identifier assigned to this vulnerability.	2024-07-10	6.3	CVE-2024-6644

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ZTE--ZXCLOUD IRAI	There is a permissions and access control vulnerability in ZXCLOUD IRAI.An attacker can elevate non-administrator permissions to administrator permissions by modifying the configuration.	2024-07-09	6.3	CVE-2024-22062 psirt@zte.com.cn

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wp_all_export_project -- wp_all_export	The Export any WordPress data to XML/CSV WordPress plugin before 1.3.1 does not escape its Export's Name before outputting it in Manage Exports settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	2021-11-08	3.5	CVE-2021-24708
aimeos--ai-admin-graphql	aimeos/ai-admin-graphql is the Aimeos GraphQL API admin interface. Starting in version 2022.04.1 and prior to versions 2022.10.10, 2023.10.6, and 2024.4.2, improper access control allows a editors to manage own services via GraphQL API which isn't allowed in the JQAdm front end. Versions 2022.10.10, 2023.10.6, and 2024.4.2 contain a patch for the issue.	2024-07-02	3.8	CVE-2024-39324
CodeIgniter--Ecommerce-CodeIgniter-Bootstrap	A vulnerability classified as problematic has been found in CodeIgniter Ecommerce-CodeIgniter-Bootstrap up to 1998845073cf433bc6c250b0354461fbd84d0e03. This affects an unknown part. The manipulation of the argument search_title/catName/sub/name/categorie leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 1b3da45308bb6c3f55247d0e99620b600bd85277. It is recommended to apply a patch to fix this issue. The identifier VDB-270369 was assigned to this vulnerability.	2024-07-05	3.5	CVE-2024-6526
discourse--discourse	Discourse is an open-source discussion platform. Prior to version 3.2.3 on the `stable` branch and version 3.3.0.beta4 on the `beta` and `tests-passed` branches, moderators using the review queue to review users may see a users email address even when the Allow moderators to view email addresses setting is disabled. This issue is patched in version 3.2.3 on the `stable` branch and version 3.3.0.beta4 on the `beta` and `tests-passed` branches. As possible workarounds, either prevent moderators from accessing the review queue or disable the approve suspect users site setting and the must approve users site setting to prevent users from being added to the review queue.	2024-07-03	2.4	CVE-2024-36122
Johnson Controls--Kantech KT1 Door Controller, Rev01	Under certain circumstances, when the controller is in factory reset mode waiting for initial setup, it will broadcast its MAC address, serial number, and firmware version. Once configured, the controller will no longer broadcast this information.	2024-07-04	3.1	CVE-2024-32754
Kodezen Limited--Academy LMS	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Kodezen Limited Academy LMS.This issue affects Academy LMS: from n/a through 2.0.4.	2024-07-06	3.5	CVE-2024-37234
mattermost -- mattermost	Mattermost versions 9.5.x <= 9.5.5 and 9.8.0 fail to sanitize the RemoteClusterFrame payloads before audit logging them which allows a high privileged attacker with access to the audit logs to read message contents.	2024-07-03	2.7	CVE-2024-39353
n/a--n/a	The OpenAI ChatGPT app before 2024-07-05 for macOS opts out of the sandbox, and stores conversations in cleartext in a location accessible to other apps.	2024-07-06	2.3	CVE-2024-40594
n/a--playSMS	A vulnerability was found in playSMS 1.4.3. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /index.php?app=main&inc=feature_inboxgroup&op=list of the component Template Handler. The manipulation of the argument Receiver Number with the input {{`id`}} leads to injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-270278 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-03	2.7	CVE-2024-6470
openharmony -- openharmony	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause apps crash through type confusion.	2024-07-02	3.3	CVE-2024-31071

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openharmony -- openharmony	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause apps crash through type confusion.	2024-07-02	3.3	CVE-2024-36278
Red Hat--Red Hat Enterprise Linux 7	A flaw was found in the cockpit package. This flaw allows an authenticated user to kill any process when enabling the pam_env's user_readenv option, which leads to a denial of service (DoS) attack.	2024-07-03	3.2	CVE-2024-6126
samsung -- android	Improper authentication in MTP application prior to SMR Jul-2024 Release 1 allows local attackers to enter MTP mode without proper authentication.	2024-07-02	3.3	CVE-2024-20900
samsung -- android	Improper access control in system property prior to SMR Jul-2024 Release 1 allows local attackers to get device identifier.	2024-07-02	3.3	CVE-2024-34583
samsung -- android	Improper access control in KnoxCustomManagerService prior to SMR Jul-2024 Release 1 allows local attackers to configure Knox privacy policy.	2024-07-02	3.3	CVE-2024-34586
samsung -- flow	Improper verification of intent by broadcast receiver vulnerability in Samsung Flow prior to version 4.9.13.0 allows local attackers to copy image files to external storage.	2024-07-02	3.3	CVE-2024-34600
samsung -- health	Improper input validation in Samsung Health prior to version 6.27.0.113 allows local attackers to write arbitrary document files to the sandbox of Samsung Health. User interaction is required for triggering this vulnerability.	2024-07-02	3.3	CVE-2024-34597
samsung -- tips	Improper input validation in Tips prior to version 6.2.9.4 in Android 14 allows local attacker to send broadcast with Tips' privilege.	2024-07-02	3.3	CVE-2024-34599
y_project--RuoYi	A vulnerability classified as problematic was found in y_project RuoYi up to 4.7.9. Affected by this vulnerability is the function isJsonRequest of the component Content-Type Handler. The manipulation of the argument HttpHeaders.CONTENT_TYPE leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-270343.	2024-07-04	3.5	CVE-2024-6511
ZKTeco--BioTime	A vulnerability was found in ZKTeco BioTime up to 9.5.2. It has been classified as problematic. Affected is an unknown function of the component system-group-add Handler. The manipulation of the argument user with the input <script>alert('XSS')</script> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-270366 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-05	3.5	CVE-2024-6523
Automattic--WooCommerce	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Automattic WooCommerce allows Content Spoofing.This issue affects WooCommerce: from n/a through 8.9.2.	2024-07-09	3.5	CVE-2024-35777
DREAM TRAIN INTERNET INC.--TONE store App	TONE store App version 3.4.2 and earlier contains an issue with unprotected primary channel. Since TONE store App communicates with TONE store website in cleartext, a man-in-the-middle attack may allow an attacker to obtain and/or alter communications of the affected App.	2024-07-10	3.7	CVE-2024-39886
Fortinet--FortiProxy	An incorrect parsing of numbers with different radices vulnerability [CWE-1389] in FortiProxy version 7.4.3 and below, version 7.2.10 and below, version 7.0.17 and below and FortiOS version 7.4.3 and below, version 7.2.8 and below, version 7.0.15 and below IP address validation feature may permit an unauthenticated attacker to bypass the IP blocklist via crafted requests.	2024-07-09	3.4	CVE-2024-26015
Gallagher--Command Centre	Improper output Neutralization for Logs (CWE-117) in the Command Centre APIÂ Diagnostics Endpoint could allow an attacker limited ability to modify Command Centre log files. This issue affects:Â Gallagher Command Centre v9.10 prior to vEL9.10.1268 (MR1).	2024-07-11	3.3	CVE-2024-23194

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gitlab -- gitlab	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.5 prior to 16.11.6, starting from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2 in which a user with `admin_group_member` custom role permission could ban group members.	2024-07-11	2.7	CVE-2024-2880
gitlab -- gitlab	An issue was discovered in GitLab CE/EE affecting all versions starting from 17.0 prior to 17.0.4 and from 17.1 prior to 17.1.2 where a Developer user with `admin_compliance_framework` custom role may have been able to modify the URL for a group namespace.	2024-07-11	2.7	CVE-2024-5257
gitlab -- gitlab	An issue was discovered in GitLab CE/EE affecting all versions starting from 17.0 prior to 17.0.4 and from 17.1 prior to 17.1.2 where a Guest user with `admin_push_rules` permission may have been able to create project-level deploy tokens.	2024-07-11	2.7	CVE-2024-5470
nodejs--undici	Undici is an HTTP/1.1 client, written from scratch for Node.js. Depending on network and process conditions of a `fetch()` request, `response.arrayBuffer()` might include portion of memory from the Node.js process. This has been patched in v6.19.2.	2024-07-08	2	CVE-2024-38372
Photo Gallery Team--Photo Gallery by Ays	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Photo Gallery Team Photo Gallery by Ays allows Code Injection.This issue affects Photo Gallery by Ays: from n/a before 5.7.1.	2024-07-09	3.8	CVE-2024-37442
Ping Identity--PingFederate	A potential JSON injection attack vector exists in PingFederate REST API data stores using the POST method and a JSON request body.	2024-07-09	3.5	CVE-2024-21832
Ping Identity--PingFederate	A cross-site scripting vulnerability exists in the admin console OIDC Policy Management Editor. The impact is contained to admin console users only.	2024-07-09	1.8	CVE-2024-22477
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in NetworkManager. When a system running NetworkManager with DEBUG logs enabled and an interface eth1 configured with LLDP enabled, a malicious user could inject a malformed LLDP packet. NetworkManager would crash, leading to a denial of service.	2024-07-09	3.1	CVE-2024-6501
samsung -- exynos_modem_5300_firmware	A vulnerability in Samsung Exynos Modem 5300 allows a Man-in-the-Middle (MITM) attacker to downgrade the security mode of packets going to the victim, enabling the attacker to send messages to the victim in plaintext.	2024-07-09	3.7	CVE-2024-28067
SAP_SE--SAP Enable Now	Due to missing verification of file type or content, SAP Enable Now allows an authenticated attacker to upload arbitrary files. These files include executables which might be downloaded and executed by the user which could host malware. On successful exploitation an attacker can cause limited impact on confidentiality and Integrity of the application.	2024-07-09	3.3	CVE-2024-34692
Siemens--JT Open	A vulnerability has been identified in JT Open (All versions < V11.5), PLM XML SDK (All versions < V7.1.0.014). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted XML files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-07-09	3.3	CVE-2024-37996
Silicon Labs--Simplicity SDK	Use After Free vulnerability in Silicon Labs Bluetooth SDK on 32 bit, ARM may allow an attacker with precise timing capabilities to intercept a small number of packets intended for a recipient that has left the network.This issue affects Silabs Bluetooth SDK: through 8.0.0.	2024-07-12	3.1	CVE-2023-41093
SourceCodester--Employee and	A vulnerability was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0 and classified as problematic. Affected by this issue is the	2024-07-10	2.4	CVE-2024-6650

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Visitor Gate Pass Logging System	function save_designation of the file /classes/Master.php. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-271058 is the identifier assigned to this vulnerability.			
WpDirectoryKit--WP Directory Kit	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in WpDirectoryKit WP Directory Kit allows Code Injection.This issue affects WP Directory Kit: from n/a through 1.3.6.	2024-07-09	2.7	CVE-2024-37253
Ankitects--Anki	A blocklist bypass vulnerability exists in the LaTeX functionality of Ankitects Anki 24.04. A specially crafted malicious flashcard can lead to an arbitrary file creation at a fixed path. An attacker can share a malicious flashcard to trigger this vulnerability.	2024-07-22	3.1	CVE-2024-32152
Connectivity Standards Alliance--connectedhomeip	An implementation issue in the Connectivity Standards Alliance Matter 1.2 protocol as used in the connectedhomeip SDK allows a third party to disclose information about devices part of the same fabric (footprinting), even though the protocol is designed to prevent access to such information.	2024-07-24	3.5	CVE-2024-3454
GitLab--GitLab	A resource misdirection vulnerability in GitLab CE/EE versions 12.0 prior to 17.0.5, 17.1 prior to 17.1.3, and 17.2 prior to 17.2.1 allows an attacker to craft a repository import in such a way as to misdirect commits.	2024-07-24	2.7	CVE-2024-0231
GitLab--GitLab	An information disclosure vulnerability in GitLab CE/EE in project/group exports affecting all versions from 15.4 prior to 17.0.5, 17.1 prior to 17.1.3, and 17.2 prior to 17.2.1 allows unauthorized users to view the resultant export.	2024-07-24	2.6	CVE-2024-7060
IBM--InfoSphere Information Server	IBM InfoSphere Information Server 11.7 could disclose sensitive user information to another user with physical access to the machine. IBM X-Force ID: 294727.	2024-07-24	2.4	CVE-2024-37533
JetBrains--TeamCity	In JetBrains TeamCity before 2024.07 stored XSS was possible on Show Connection page	2024-07-22	3.5	CVE-2024-41826
JetBrains--TeamCity	In JetBrains TeamCity before 2024.07 an OAuth code for JetBrains Space could be stolen via Space Application connection	2024-07-22	3.5	CVE-2024-41829
JetBrains--TeamCity	In JetBrains TeamCity before 2024.07 comparison of authorization tokens took non-constant time	2024-07-22	2.6	CVE-2024-41828
Lenovo--Tab K10	An improper validation vulnerability was reported in the Lenovo Tab K10 that could allow a specially crafted application to keep the device on.	2024-07-26	2.8	CVE-2024-4786
Octopus Deploy--Octopus Server	In affected versions of Octopus Server under certain conditions, a user with specific role assignments can access restricted project artifacts.	2024-07-25	2.2	CVE-2024-4811 security@octopus.com
thinkst--canarytokens	Canarytokens help track activity and actions on a network. A Cross-Site Scripting vulnerability was identified in the "Cloned Website" Canarytoken, whereby the Canarytoken's creator can attack themselves. The creator of a slow-redirect Canarytoken can insert Javascript into the destination URL of their slow redirect token. When the creator later browses the management page for their own Canarytoken, the Javascript executes. This is a self-XSS. An attacker could create a Canarytoken with this self-XSS, and send the management link to a victim. When they click on it, the Javascript would execute. However, no sensitive information (ex. session information) will be disclosed to the malicious actor. This issue is now	2024-07-23	3.5	CVE-2024-41663

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	patched on Canarytokens.org. Users of self-hosted Canarytokens installations can update by pulling the latest Docker image, or any Docker image after `sha-097d91a`.			
Akana--Akana API Platform	In versions of Akana API Platform prior to 2024.1.0 overly verbose errors can be found in SAML integrations	2024-07-30	3.5	CVE-2024-5250
Apple--iOS and iPadOS	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in iOS 17.6 and iPadOS 17.6, watchOS 10.6, tvOS 17.6, visionOS 1.3, macOS Sonoma 14.6. Processing a maliciously crafted file may lead to unexpected app termination.	2024-07-29	3.3	CVE-2024-40777
Baidu--UEditor	A vulnerability was found in Baidu UEditor 1.4.3.3. It has been classified as problematic. This affects an unknown part of the file /ueditor/php/controller.php?action=uploadfile&encode=utf-8. The manipulation of the argument upfile leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273273 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-01	3.5	CVE-2024-7342
Baidu--UEditor	A vulnerability was found in Baidu UEditor 1.4.2. It has been declared as problematic. This vulnerability affects unknown code of the file /ueditor142/php/controller.php?action=catchimage. The manipulation of the argument source[] leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273274 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-08-01	3.5	CVE-2024-7343
biscuit-auth--biscuit-java	biscuit-java is the java implementation of Biscuit, an authentication and authorization token for microservices architectures. Third-party blocks can be generated without transferring the whole token to the third-party authority. Instead, a ThirdPartyBlock request can be sent, providing only the necessary info to generate a third-party block and to sign it, which includes the public key of the previous block (used in the signature) and the public keys part of the token symbol table (for public key interning in datalog expressions). A third-part block request forged by a malicious user can trick the third-party authority into generating datalog trusting the wrong keypair. This vulnerability is fixed in 4.0.0.	2024-08-01	3	CVE-2024-41948
biscuit-auth--biscuit-rust	biscuit-rust is the Rust implementation of Biscuit, an authentication and authorization token for microservices architectures. Third-party blocks can be generated without transferring the whole token to the third-party authority. Instead, a ThirdPartyBlock request can be sent, providing only the necessary info to generate a third-party block and to sign it, which includes the public key of the previous block (used in the signature) and the public keys part of the token symbol table (for public key interning in datalog expressions). A third-part block request forged by a malicious user can trick the third-party authority into generating datalog trusting the wrong keypair.	2024-08-01	3	CVE-2024-41949
Dell--Data Manager Appliance	DM5500 5.16.0.0, contains an information disclosure vulnerability. A local attacker with high privileges could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed	2024-07-31	3.3	CVE-2024-37135

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Software (DMAS)	credentials to access the vulnerable application with privileges of the compromised account.			
FuelLabs--fuels-ts	fuels-ts is a library for interacting with Fuel v2. The typescript SDK has no awareness of to-be-spent transactions causing some transactions to fail or silently get pruned as they are funded with already used UTXOs. The problem occurs, because the `fund` function in `fuels-ts/packages/account/src/account.ts` gets the needed ressources statelessly with the function `getResourcesToSpend` without taking into consideration already used UTXOs. This issue will lead to unexpected SDK behaviour, such as a transaction not getting included in the `txpool` / in a block or a previous transaction silently getting removed from the `txpool` and replaced with a new one.	2024-07-30	3.1	CVE-2024-41945
Honeywell--PC42t, PC42tp, and PC42d (Common Firmware)	Honeywell PC42t, PC42tp, and PC42d Printers, T10.19.020016 to T10.20.060398, contain a cross-site scripting vulnerability. A(n) attacker could potentially inject malicious code which may lead to information disclosure, session theft, or client-side request forgery. Honeywell recommends updating to the most recent version of this firmware, PC42 Printer Firmware Version 20.6 T10.20.060398.	2024-07-29	3.5	CVE-2024-6620
IBM--Security Directory Integrator	IBM Security Directory Integrator 7.2.0 and IBM Security Verify Directory Integrator 10.0.0 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie. IBM X-Force ID: 228587.	2024-07-30	3.7	CVE-2022-33167
itsourcecode--Online Blood Bank Management System	A vulnerability was found in itsourcecode Online Blood Bank Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /request.php of the component Send Blood Request Page. The manipulation of the argument Address/bloodgroup leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273185 was assigned to this vulnerability.	2024-07-31	3.5	CVE-2024-7303
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0, 9.5.x <= 9.5.6 fail to properly restrict channel creation which allows a malicious remote to create arbitrary channels, when shared channels were enabled.	2024-08-01	3.8	CVE-2024-39837
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0, 9.5.x <= 9.5.6 fail to properly validate synced reactions, when shared channels are enabled, which allows a malicious remote to create arbitrary reactions on arbitrary posts	2024-08-01	2.7	CVE-2024-29977
Mattermost--Mattermost	Mattermost versions 9.9.x <= 9.9.0 and 9.5.x <= 9.5.6 fail to validate the source of sync messages and only allow the correct remote IDs, which allows a malicious remote to set arbitrary RemoteId values for synced users and therefore claim that a user was synced from another remote.	2024-08-01	2.7	CVE-2024-41926
Motorola--Q14 Mesh Router Firmware	A denial-of-service vulnerability could allow an authenticated user to trigger an internal service restart via a specially crafted API request.	2024-07-31	2.7	CVE-2022-4003
Ping Identity--OPENIDM	Improper Input Validation of query search results for private field data in PingIDM OPENIDM (Query Filter module) allows for a potentially efficient brute forcing approach leading to information disclosure.	2024-08-01	2.7	CVE-2024-23600
SourceCodester--Complaints Report Management System	A vulnerability, which was classified as problematic, has been found in SourceCodester Complaints Report Management System 1.0. This issue affects some unknown processing of the file /admin/ajax.php?action=save_settings. The manipulation of the argument name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272621 was assigned to this vulnerability.	2024-07-29	3.5	CVE-2024-7200

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SourceCodester--Establishment Billing Management System	A vulnerability has been found in SourceCodester Establishment Billing Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/ajax.php?action=save_settings. The manipulation of the argument name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273154 is the identifier assigned to this vulnerability.	2024-07-31	3.5	CVE-2024-7285
SourceCodester--Insurance Management System	A vulnerability was found in SourceCodester Insurance Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /Script/admin/core/update_policy of the component Edit Insurance Policy Page. The manipulation of the argument pname leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272805 was assigned to this vulnerability.	2024-07-30	3.5	CVE-2024-7225
SourceCodester--Lot Reservation Management System	A vulnerability, which was classified as problematic, was found in SourceCodester Lot Reservation Management System 1.0. This affects an unknown part of the file /admin/ajax.php?action=save_settings. The manipulation of the argument about leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273153 was assigned to this vulnerability.	2024-07-31	3.5	CVE-2024-7284
SourceCodester--Record Management System	A vulnerability was found in SourceCodester Record Management System 1.0. It has been classified as problematic. This affects an unknown part of the file entry.php. The manipulation of the argument school leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273201 was assigned to this vulnerability.	2024-07-31	3.5	CVE-2024-7309
SourceCodester--Record Management System	A vulnerability was found in SourceCodester Record Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file sort_user.php. The manipulation of the argument sort leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-273202 is the identifier assigned to this vulnerability.	2024-07-31	3.5	CVE-2024-7310
SourceCodester--School Log Management System	A vulnerability was found in SourceCodester School Log Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/ajax.php?action=save_student. The manipulation of the argument name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-272789 was assigned to this vulnerability.	2024-07-30	3.5	CVE-2024-7218
SourceCodester--Simple Realtime Quiz System	A vulnerability has been found in SourceCodester Simple Realtime Quiz System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /ajax.php?action=save_quiz. The manipulation of the argument title leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-273352.	2024-08-01	3.5	CVE-2024-7368
SourceCodester--Tracking Monitoring Management System	A vulnerability was found in SourceCodester Tracking Monitoring Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /ajax.php?action=save_establishment. The manipulation of the argument name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-273338 is the identifier assigned to this vulnerability.	2024-08-01	3.5	CVE-2024-7359
TOTOLINK--LR1200	A vulnerability was found in TOTOLINK LR1200 9.3.1cu.2832. It has been classified as problematic. This affects an unknown part of the file /etc/shadow.sample. The manipulation leads to use of hard-coded password. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-	2024-07-30	2.6	CVE-2024-7216

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	272787. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.			