SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 10 May 2023

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-2583	Code Injection in GitHub repository jsreport/jsreport prior to 3.11.3.	10.0	More Details
CVE-2023-2564	OS Command Injection in GitHub repository sbs20/scanservjs prior to v2.27.0.	10.0	More Details
CVE-2023-32069	XWiki Platform is a generic wiki platform. Starting in version 3.3-milestone-2 and prior to versions 14.10.4 and 15.0-rc-1, it's possible for a user to execute anything with the right of the author of the XWiki.ClassSheet document. This has been patched in XWiki 15.0-rc-1 and 14.10.4. There are no known workarounds.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30899	A vulnerability has been identified in Siveillance Video 2020 R2 (All versions < V20.2 HotfixRev14), Siveillance Video 2020 R3 (All versions < V20.3 HotfixRev12), Siveillance Video 2021 R1 (All versions < V21.1 HotfixRev12), Siveillance Video 2021 R2 (All versions < V21.2 HotfixRev8), Siveillance Video 2022 R1 (All versions < V22.1 HotfixRev7), Siveillance Video 2022 R2 (All versions < V22.2 HotfixRev5), Siveillance Video 2022 R3 (All versions < V22.3 HotfixRev2), Siveillance Video 2023 R1 (All versions < V23.1 HotfixRev1). The Management Server component of affected applications deserializes data without sufficient validations. This could allow an authenticated remote attacker to execute code on the affected system.	9.9	More Details
CVE-2023-22651	Improper Privilege Management vulnerability in SUSE Rancher allows Privilege Escalation. A failure in the update logic of Rancher's admission Webhook may lead to the misconfiguration of the Webhook. This component enforces validation rules and security checks before resources are admitted into the Kubernetes cluster. The issue only affects users that upgrade from 2.6.x or 2.7.x to 2.7.2. Users that did a fresh install of 2.7.2 (and did not follow an upgrade path) are not affected.	9.9	More Details
CVE-2023-27407	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). The web based management of affected device does not properly validate user input, making it susceptible to command injection. This could allow an authenticated remote attacker to access the underlying operating system as the root user.	9.9	More Details
CVE-2023-30898	A vulnerability has been identified in Siveillance Video 2020 R2 (All versions < V20.2 HotfixRev14), Siveillance Video 2020 R3 (All versions < V20.3 HotfixRev12), Siveillance Video 2021 R1 (All versions < V21.1 HotfixRev12), Siveillance Video 2021 R2 (All versions < V21.2 HotfixRev8), Siveillance Video 2022 R1 (All versions < V22.1 HotfixRev7), Siveillance Video 2022 R2 (All versions < V22.2 HotfixRev5), Siveillance Video 2022 R3 (All versions < V22.3 HotfixRev2), Siveillance Video 2023 R1 (All versions < V23.1 HotfixRev1). The Event Server component of affected applications deserializes data without sufficient validations. This could allow an authenticated remote attacker to execute code on the affected system.	9.9	More Details
CVE-2023-22785	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22784	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2023-25826	Due to insufficient validation of parameters passed to the legacy HTTP query API, it is possible to inject crafted OS commands into multiple parameters and execute malicious code on the OpenTSDB host system. This exploit exists due to an incomplete fix that was made when this vulnerability was previously disclosed as CVE-2020-35476. Regex validation that was implemented to restrict allowed input to the query API does not work as intended, allowing crafted commands to bypass validation.	9.8	More Details
CVE-2023-29693	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function set_tftp_upgrad.	9.8	More Details
CVE-2023-22783	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2023-22782	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2023-30204	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the judge_id parameter at /php-jms/edit_judge.php.	9.8	More Details
CVE-2023-22780	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22779	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2023-22786	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2023-23526	This was addressed with additional checks by Gatekeeper on files downloaded from an iCloud shared-by-me folder. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. A file from an iCloud shared-by-me folder may be able to bypass Gatekeeper.	9.8	More Details
CVE-2023-29696	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function version_set.	9.8	More Details
CVE-2023-30092	SourceCodester Online Pizza Ordering System v1.0 is vulnerable to SQL Injection via the QTY parameter.	9.8	More Details
CVE-2022-4118	The Bitcoin / AltCoin Payment Gateway for WooCommerce & Multivendor store / shop WordPress plugin through 1.7.1 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by authenticated users	9.8	More Details
CVE-2023-27953	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory.	9.8	More Details
CVE-2023-28201	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, Safari 16.4, iOS 16.4 and iPadOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, tvOS 16.4. A remote user may be able to cause unexpected app termination or arbitrary code execution.	9.8	More Details
CVE-2023-24941	Windows Network File System Remote Code Execution Vulnerability	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24943	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-26379	Insufficient input validation of mailbox data in the SMU may allow an attacker to coerce the SMU to corrupt SMRAM, potentially leading to a loss of integrity and privilege escalation.	9.8	More Details
CVE-2023-20520	Improper access control settings in ASP Bootloader may allow an attacker to corrupt the return address causing a stack-based buffer overrun potentially leading to arbitrary code execution.	9.8	More Details
CVE-2021-46760	A malicious or compromised UApp or ABL can send a malformed system call to the bootloader, which may result in an out-of-bounds memory access that may potentially lead to an attacker leaking sensitive information or achieving code execution.	9.8	More Details
CVE-2023-1650	The AI ChatBot WordPress plugin before 4.4.7 unserializes user input from cookies via an AJAX action available to unauthenticated users, which could allow them to perform PHP Object Injection when a suitable gadget is present on the blog	9.8	More Details
CVE-2023-22781	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2020-23966	SQL Injection vulnerability in victor cms 1.0 allows attackers to execute arbitrary commands via the post parameter to /post.php in a crafted GET request.	9.8	More Details
CVE-2023-2531	Improper Restriction of Excessive Authentication Attempts in GitHub repository azuracast/azuracast prior to 0.18.3.	9.8	More Details
CVE-2022-47757	In imo.im 2022.11.1051, a path traversal vulnerability delivered via an unsanitized deeplink can force the application to write a file into the application's data directory. This may allow an attacker to save a shared library under a special directory which the app uses to dynamically load modules. Loading the library can lead to arbitrary code execution.	9.8	More Details
CVE-2023-30077	Judging Management System v1.0 by oretnom23 was discovered to vulnerable to SQL injection via /php-jms/review_result.php? mainevent_id=, mainevent_id.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30331	An issue in the render function of beetl v3.15.0 allows attackers to execute server-side template injection (SSTI) via a crafted payload.	9.8	More Details
CVE-2023-29827	ejs v3.1.9 is vulnerable to server-side template injection. If the ejs file is controllable, template injection can be implemented through the configuration settings of the closeDelimiter parameter. NOTE: this is disputed by the vendor because the render function is not intended to be used with untrusted input.	9.8	More Details
CVE-2023-30203	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the event_id parameter at /php-jms/result_sheet.php.	9.8	More Details
CVE-2023-20126	A vulnerability in the web-based management interface of Cisco SPA112 2-Port Phone Adapters could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to a missing authentication process within the firmware upgrade function. An attacker could exploit this vulnerability by upgrading an affected device to a crafted version of firmware. A successful exploit could allow the attacker to execute arbitrary code on the affected device with full privileges. Cisco has not released firmware updates to address this vulnerability.	9.8	More Details
CVE-2023-23059	An issue was discovered in GeoVision GV-Edge Recording Manager 2.2.3.0 for windows, which contains improper permissions within the default installation and allows attackers to execute arbitrary code and gain escalated privileges.	9.8	More Details
CVE-2023-30264	CLTPHP <=6.0 is vulnerable to Unrestricted Upload of File with Dangerous Type via application/admin/controller/Template.php:update.	9.8	More Details
CVE-2023-30268	CLTPHP <=6.0 is vulnerable to Improper Input Validation.	9.8	More Details
CVE-2023-25754	Privilege Context Switching Error vulnerability in Apache Software Foundation Apache Airflow.This issue affects Apache Airflow: before 2.6.0.	9.8	More Details
CVE-2023-30328	An issue in the helper tool of Mailbutler GmbH Shimo VPN Client for macOS v5.0.4 allows attackers to bypass authentication via PID re-use.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28316	A security vulnerability has been discovered in the implementation of 2FA on the rocket.chat platform, where other active sessions are not invalidated upon activating 2FA. This could potentially allow an attacker to maintain access to a compromised account even after 2FA is enabled.	9.8	More Details
CVE-2023-30122	An arbitrary file upload vulnerability in the component /admin/ajax.php?action=save_menu of Online Food Ordering System v2.0 allows attackers to execute arbitrary code via uploading a crafted PHP file.	9.8	More Details
CVE-2023-30013	TOTOLINK X5000R V9.1.0u.6118_B20201102 and V9.1.0u.6369_B20230113 contain a command insertion vulnerability in setting/setTracerouteCfg. This vulnerability allows an attacker to execute arbitrary commands through the "command" parameter.	9.8	More Details
CVE-2023-31039	Security vulnerability in Apache bRPC <1.5.0 on all platforms allows attackers to execute arbitrary code via ServerOptions::pid_file. An attacker that can influence the ServerOptions pid_file parameter with which the bRPC server is started can execute arbitrary code with the permissions of the bRPC process. Solution: 1. upgrade to bRPC >= 1.5.0, download link: https://dist.apache.org/repos/dist/release/brpc/1.5.0/ https://dist.apache.org/repos/dist/release/brpc/1.5.0/ 2. If you are using an old version of bRPC and hard to upgrade, you can apply this patch: https://github.com/apache/brpc/pull/2218 https://github.com/apache/brpc/pull/2218	9.8	More Details
CVE-2023-30018	Judging Management System v1.0 is vulnerable to SQL Injection. via /php-jms/review_se_result.php?mainevent_id=.	9.8	More Details
CVE-2023-30185	CRMEB v4.4 to v4.6 was discovered to contain an arbitrary file upload vulnerability via the component \attachment\SystemAttachmentServices.php.	9.8	More Details
CVE-2023-29944	Metersphere v1.20.20-lts-79d354a6 is vulnerable to Remote Command Execution. The system command reverse-shell can be executed at the custom code snippet function of the metersphere system workbench	9.8	More Details
CVE-2023-31047	In Django 3.2 before 3.2.19, 4.x before 4.1.9, and 4.2 before 4.2.1, it was possible to bypass validation when using one form field to upload multiple files. This multiple upload has never been supported by forms.FileField or forms.ImageField (only the last uploaded file was validated). However, Django's "Uploading multiple files" documentation suggested otherwise.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30053	TOTOLINK A7100RU V7.4cu.2313_B20191024 is vulnerable to Command Injection.	9.8	More Details
CVE-2023-30054	TOTOLINK A7100RU V7.4cu.2313_B20191024 has a Command Injection vulnerability. An attacker can obtain a stable root shell through a specially constructed payload.	9.8	More Details
CVE-2023-30242	NS-ASG v6.3 was discovered to contain a SQL injection vulnerability via the component /admin/add_ikev2.php.	9.8	More Details
CVE-2023-30090	Semcms Shop v4.2 was discovered to contain an arbitrary file uplaod vulnerability via the component SEMCMS_Upfile.php. This vulnerability allows attackers to execute arbitrary code via uploading a crafted PHP file.	9.8	More Details
CVE-2023-30135	Tenda AC18 v15.03.05.19(6318_)_cn was discovered to contain a command injection vulnerability via the deviceName parameter in the setUsbUnload function.	9.8	More Details
CVE-2023-2478	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.9.7, all versions starting from 15.10 before 15.10.6, all versions starting from 15.11 before 15.11.2. Under certain conditions, a malicious unauthorized GitLab user may use a GraphQL endpoint to attach a malicious runner to any project.	9.6	More Details
CVE-2023-27958	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory.	9.1	More Details
CVE-2023-28762	SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an authenticated attacker with administrator privileges to get the login token of any logged-in BI user over the network without any user interaction. The attacker can impersonate any user on the platform resulting into accessing and modifying data. The attacker can also make the system partially or entirely unavailable.	9.1	More Details
CVE-2021-46753	Failure to validate the length fields of the ASP (AMD Secure Processor) sensor fusion hub headers may allow an attacker with a malicious Uapp or ABL to map the ASP sensor fusion hub region and overwrite data structures leading to a potential loss of confidentiality and integrity.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46754	Insufficient input validation in the ASP (AMD Secure Processor) bootloader may allow an attacker with a compromised Uapp or ABL to coerce the bootloader into exposing sensitive information to the SMU (System Management Unit) resulting in a potential loss of confidentiality and integrity.	9.1	More Details
CVE-2021-46756	Insufficient validation of inputs in SVC_MAP_USER_STACK in the ASP (AMD Secure Processor) bootloader may allow an attacker with a malicious Uapp or ABL to send malformed or invalid syscall to the bootloader resulting in a potential denial of service and loss of integrity.	9.1	More Details
CVE-2023-31123	`effectindex/tripreporter` is a community-powered, universal platform for submitting and analyzing trip reports. Prior to commit bd80ba833b9023d39ca22e29874296c8729dd53b, any user with an account on an instance of `effectindex/tripreporter`, e.g. `subjective.report`, may be affected by an improper password verification vulnerability. The vulnerability allows any user with a password matching the password requirements to log in as any user. This allows access to accounts / data loss of the user. This issue is patched in commit bd80ba833b9023d39ca22e29874296c8729dd53b. No action necessary for users of `subjective.report`, and anyone running their own instance should update to this commit or newer as soon as possible. As a workaround, someone running their own instance may apply the patch manually.	9.1	More Details
CVE-2023-31126	`org.xwiki.commons:xwiki-commons-xml` is an XML library used by the open-source wiki platform XWiki. The HTML sanitizer, introduced in version 14.6-rc-1, allows the injection of arbitrary HTML code and thus cross-site scripting via invalid data attributes. This vulnerability does not affect restricted cleaning in HTMLCleaner as there attributes are cleaned and thus characters like `/` and `>` are removed in all attribute names. This problem has been patched in XWiki 14.10.4 and 15.0 RC1 by making sure that data attributes only contain allowed characters. There are no known workarounds apart from upgrading to a version including the fix.	9.0	More Details
CVE-2023-32071	XWiki Platform is a generic wiki platform. Starting in versions 2.2-milestone-1 and prior to versions 14.4.8, 14.10.4, and 15.0-rc-1, it's possible to execute javascript with the right of any user by leading him to a special URL on the wiki targeting a page which contains an attachment. This has been patched in XWiki 15.0-rc-1, 14.10.4, and 14.4.8. The easiest possible workaround is to edit file `<xwiki app>/templates/importinline.vm` and apply the modification described in commit 28905f7f518cc6f21ea61fe37e9e1ed97ef36f01.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31127	libspdm is a sample implementation that follows the DMTF SPDM specifications. A vulnerability has been identified in SPDM session establishment in libspdm prior to version 2.3.1. If a device supports both DHE session and PSK session with mutual authentication, the attacker may be able to establish the session with `KEY_EXCHANGE` and `PSK_FINISH` to bypass the mutual authentication. This is most likely to happen when the Requester begins a session using one method (DHE, for example) and then uses the other method's finish (PSK_FINISH in this example) to establish the session. The session hashes would be expected to fail in this case, but the condition was not detected. This issue only impacts the SPDM responder, which supports `KEY_EX_CAP=1 and `PSK_CAP=10b` at same time with mutual authentication requirement. The SPDM requester is not impacted. The SPDM responder is not impacted if `KEY_EX_CAP=0` or `PSK_CAP=0` or `PSK_CAP=01b`. The SPDM responder is not impacted if mutual authentication is not required. libspdm 1.0, 2.0, 2.1, 2.2, 2.3 are all impacted. Older branches are not maintained, but users of the 2.3 branch may receive a patch in version 2.3.2. The SPDM specification (DSP0274) does not contain this vulnerability.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-0768	The Avirato hotels online booking engine WordPress plugin through 5.0.5 does not validate and escape some of its shortcode attributes before using them in SQL statement/s, which could allow any authenticated users, such as subscriber to perform SQL Injection attacks.	8.8	More Details
CVE-2023-24958	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X-Force ID: 246320.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31038	SQL injection in Log4cxx when using the ODBC appender to send log messages to a database. No fields sent to the database were properly escaped for SQL injection. This has been the case since at least version 0.9.0(released 2003-08-06) Note that Log4cxx is a C++ framework, so only C++ applications are affected. Before version 1.1.0, the ODBC appender was automatically part of Log4cxx if the library was found when compiling the library. As of version 1.1.0, this must be both explicitly enabled in order to be compiled in. Three preconditions must be met for this vulnerability to be possible: 1. Log4cxx compiled with ODBC support(before version 1.1.0, this was auto-detected at compile time) 2. ODBCAppender enabled for logging messages to, generally done via a config file 3. User input is logged at some point. If your application does not have user input, it is unlikely to be affected. Users are recommended to upgrade to version 1.1.0 which properly binds the parameters to the SQL statement, or migrate to the new DBAppender class which supports an ODBC connection in addition to other databases. Note that this fix does require a configuration file update, as the old configuration files will not configure properly. An example is shown below, and more information may be found in the Log4cxx documentation on the ODBCAppender. Example of old configuration snippet: <appender name="SqlODBCAppender" class="ODBCAppender"> <param name="sql" value="INSERT INTO logs (message) VALUES ('%m')" /> ... other params here ... </appender> The migrated configuration snippet with new ColumnMapping parameters: <appender name="SqlODBCAppender" class="ODBCAppender"> <param name="sql" value="INSERT INTO logs (message) VALUES (?)" /> <param name="ColumnMapping" value="message"/> ... other params here ... </appender>	8.8	More Details
CVE-2023-0603	The Sloth Logo Customizer WordPress plugin through 2.0.2 does not have CSRF check when updating its settings, 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	8.8	More Details
CVE-2023-1031	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the application via CSTI in the `settings` endpoint and first_name parameter.	8.8	More Details
CVE-2023-29842	ChurchCRM 4.5.4 endpoint /EditEventTypes.php is vulnerable to Blind SQL Injection (Time-based) via the EN_tyid POST parameter.	8.8	More Details
CVE-2023-31976	libming v0.4.8 was discovered to contain a stack buffer overflow via the function makeswf_preprocess at /util/makeswf_utils.c.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1094	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the application via CSTI in the `people:id/food` endpoint and food parameter.	8.8	More Details
CVE-2022-4259	Due to improper input validation in the Alerts controller, a SQL injection vulnerability in Nozomi Networks Guardian and CMC allows an authenticated attacker to execute arbitrary SQL queries on the DBMS used by the web application.	8.8	More Details
CVE-2023-23532	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, iOS 15.7.6 and iPadOS 15.7.6. An app may be able to break out of its sandbox.	8.8	More Details
CVE-2022-32885	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5, Safari 15.6. Processing maliciously crafted web content may lead to arbitrary code execution	8.8	More Details
CVE-2023-31415	Kibana version 8.7.0 contains an arbitrary code execution flaw. An attacker with All privileges to the Uptime/Synthetics feature could send a request that will attempt to execute JavaScript code. This could lead to the attacker executing arbitrary commands on the host system with permissions of the Kibana process.	8.8	More Details
CVE-2023-31414	Kibana versions 8.0.0 through 8.7.0 contain an arbitrary code execution flaw. An attacker with write access to Kibana yaml or env configuration could add a specific payload that will attempt to execute JavaScript code. This could lead to the attacker executing arbitrary commands on the host system with permissions of the Kibana process.	8.8	More Details
CVE-2023-24947	Windows Bluetooth Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-2520	A vulnerability was found in Caton Prime 2.1.2.51.e8d7225049(202303031001) and classified as critical. This issue affects some unknown processing of the file cgi-bin/tools_ping.cgi?action=Command of the component Ping Handler. The manipulation of the argument Destination leads to command injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-228011. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2023-2551	PHP Remote File Inclusion in GitHub repository unilogies/bumsys prior to 2.1.1.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27934	A memory initialization issue was addressed. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4. A remote attacker may be able to cause unexpected app termination or arbitrary code execution.	8.8	More Details
CVE-2023-2552	Cross-Site Request Forgery (CSRF) in GitHub repository unilogies/bumsys prior to 2.1.1.	8.8	More Details
CVE-2023-30065	MitraStar GPT-2741GNAC-N2 with firmware BR_g5.9_1.11(WVK.0)b32 was discovered to contain a remote code execution (RCE) vulnerability in the ping function.	8.8	More Details
CVE-2021-46769	Insufficient syscall input validation in the ASP Bootloader may allow a privileged attacker to execute arbitrary DMA copies, which can lead to code execution.	8.8	More Details
CVE-2023-31099	Zoho ManageEngine OPManager through 126323 allows an authenticated user to achieve remote code execution via probe servers.	8.8	More Details
CVE-2023-27568	SQL injection vulnerability inSpryker Commerce OS 0.9 that allows for access to sensitive data via customer/order?orderSearchForm[searchText]=	8.8	More Details
CVE-2023-2461	Use after free in OS Inputs in Google Chrome on ChromeOS prior to 113.0.5672.63 allowed a remote attacker who convinced a user to enage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-24507	AgilePoint NX v8.0 SU2.2 & SU2.3 – Insecure File Upload - Vulnerability allows insecure file upload, by an unspecified request.	8.8	More Details
CVE-2021-28999	SQL Injection vulnerability in CMS Made Simple through 2.2.15 allows remote attackers to execute arbitrary commands via the m1_sortby parameter to modules/News/function.admin_articlestab.php.	8.8	More Details
CVE-2020-23363	Cross Site Request Forgery (CSRF) vulnerability found in Verytops Verydows all versions that allows an attacker to execute arbitrary code via a crafted script.	8.8	More Details
CVE-2020-36065	Cross Site Request Forgery (CSRF) vulnerability in FlyCms 1.0 allows attackers to add arbitrary administrator accounts via system/admin/admin_save.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-22755	File upload vulnerability in MCMS 5.0 allows attackers to execute arbitrary code via a crafted thumbnail. A different vulnerability than CVE-2022-31943.	8.8	More Details
CVE-2023-25832	There is a cross-site-request forgery vulnerability in Esri Portal for ArcGIS Versions 11.0 and below that may allow an attacker to trick an authorized user into executing unwanted actions.	8.8	More Details
CVE-2023-20046	A vulnerability in the key-based SSH authentication feature of Cisco StarOS Software could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied credentials. An attacker could exploit this vulnerability by sending a valid low-privileged SSH key to an affected device from a host that has an IP address that is configured as the source for a high-privileged user account. A successful exploit could allow the attacker to log in to the affected device through SSH as a high-privileged user. There are workarounds that address this vulnerability.	8.8	More Details
CVE-2021-46773	Insufficient input validation in ABL may enable a privileged attacker to corrupt ASP memory, potentially resulting in a loss of integrity or code execution.	8.8	More Details
CVE-2020-18131	Cross Site Request Forgery (CSRF) vulnerability in Bluethrust Clan Scripts v4 allows attackers to escilate privledges to an arbitrary account via a crafted request to /members/console.php?cID=5.	8.8	More Details
CVE-2023-2575	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stack-based Buffer Overflow vulnerability, which can be triggered by authenticated users via a crafted POST request.	8.8	More Details
CVE-2023-2574	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the device name input field, which can be triggered by authenticated users via a crafted POST request.	8.8	More Details
CVE-2023-2573	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the NTP server input field, which can be triggered by authenticated users via a crafted POST request.	8.8	More Details
CVE-2022-3405	Code execution and sensitive information disclosure due to excessive privileges assigned to Acronis Agent. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 29486, Acronis Cyber Backup 12.5 (Windows, Linux) before build 16545.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27935	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected app termination or arbitrary code execution.	8.8	More Details
CVE-2023-27944	This issue was addressed with a new entitlement. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to break out of its sandbox.	8.6	More Details
CVE-2022-46720	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1. An app may be able to break out of its sandbox	8.6	More Details
CVE-2023-27967	The issue was addressed with improved memory handling. This issue is fixed in Xcode 14.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges.	8.6	More Details
CVE-2023-21491	Improper access control vulnerability in ThemeManager prior to SMR May-2023 Release 1 allows local attackers to write arbitrary files with system privilege.	8.5	More Details
CVE-2022-45048	Authenticated users with appropriate privileges can create policies having expressions that can exploit code execution vulnerability. This issue affects Apache Ranger: 2.3.0. Users are recommended to update to version 2.4.0.	8.4	More Details
CVE-2023-21501	Improper input validation vulnerability in mPOS fiserve trustlet prior to SMR May-2023 Release 1 allows local attackers to execute arbitrary code.	8.2	More Details
CVE-2023-30744	In SAP AS NetWeaver JAVA - versions SERVERCORE 7.50, J2EE-FRMW 7.50, CORE-TOOLS 7.50, an unauthenticated attacker can attach to an open interface and make use of an open naming and directory API to instantiate an object which has methods which can be called without further authorization and authentication. A subsequent call to one of these methods can read or change the state of existing services without any effect on availability.	8.2	More Details
CVE-2021-26365	Certain size values in firmware binary headers could trigger out of bounds reads during signature validation, leading to denial of service or potentially limited leakage of information about out-of-bounds memory contents.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25827	Due to insufficient validation of parameters reflected in error messages by the legacy HTTP query API and the logging endpoint, it is possible to inject and execute malicious JavaScript within the browser of a targeted OpenTSDB user. This issue shares the same root cause as CVE-2018-13003, a reflected XSS vulnerability with the suggestion endpoint.	8.2	More Details
CVE-2023-21499	Out-of-bounds write vulnerability in TA_Communication_mpos_encrypt_pin in mPOS TUI trustlet prior to SMR May-2023 Release 1 allows local attackers to execute arbitrary code.	8.2	More Details
CVE-2023-30399	Insecure permissions in the settings page of GARO Wallbox GLB/GTB/GTC before v189 allows attackers to redirect users to a crafted update package link via a man-in-the-middle attack.	8.1	More Details
CVE-2021-40331	An Incorrect Permission Assignment for Critical Resource vulnerability was found in the Apache Ranger Hive Plugin. Any user with SELECT privilege on a database can alter the ownership of the table in Hive when Apache Ranger Hive Plugin is enabled This issue affects Apache Ranger Hive Plugin: from 2.0.0 through 2.3.0. Users are recommended to upgrade to version 2.4.0 or later.	8.1	More Details
CVE-2023-24903	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-31178	AgilePoint NX v8.0 SU2.2 & SU2.3 – Arbitrary File Delete Vulnerability allows arbitrary file deletion, by an unspecified request.	8.1	More Details
CVE-2023-28283	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-28656	NGINX Management Suite may allow an authenticated attacker to gain access to configuration objects outside of their assigned environment. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.1	More Details
CVE-2023-31182	EasyTor Applications – Authorization Bypass - EasyTor Applications may allow authorization bypass via unspecified method.	8.1	More Details
CVE-2023-29325	Windows OLE Remote Code Execution Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30860	WWBN AVideo is an open source video platform. In AVideo prior to version 12.4, a normal user can make a Meeting Schedule where the user can invite another user in that Meeting, but it does not properly sanitize the malicious characters when creating a Meeting Room. This allows attacker to insert malicious scripts. Since any USER including the ADMIN can see the meeting room that was created by the attacker this can lead to cookie hijacking and takeover of any accounts. Version 12.4 contains a patch for this issue.	8.0	More Details
CVE-2022-48243	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2022-48384	In srtd service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2023-31982	Sngrep v1.6.0 was discovered to contain a heap buffer overflow via the function capture_packet_reasm_ip at /src/capture.c.	7.8	More Details
CVE-2022-48388	In powerEx service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2023-31981	Sngrep v1.6.0 was discovered to contain a stack buffer overflow via the function packet_set_payload at /src/packet.c.	7.8	More Details
CVE-2023-27999	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in FortiADC 7.2.0, 7.1.0 through 7.1.1 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands.	7.8	More Details
CVE-2023-25438	An issue was discovered in Genomedics MilleGP5 5.9.2, allows remote attackers to execute arbitrary code and gain escalated privileges via modifying specific files.	7.8	More Details
CVE-2022-48368	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2023-31979	Catdoc v0.95 was discovered to contain a global buffer overflow via the function process_file at /src/reader.c.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31284	illumos illumos-gate before 676abcb has a stack buffer overflow in /dev/net, leading to privilege escalation via a stat on a long file name in /dev/net.	7.8	More Details
CVE-2022-48245	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2022-48246	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2022-48250	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2022-48249	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2023-29462	An arbitrary code execution vulnerability contained in Rockwell Automation's Arena Simulation software was reported that could potentially allow a malicious user to commit unauthorized arbitrary code to the software by using a memory buffer overflow in the heap. potentially resulting in a complete loss of confidentiality, integrity, and availability.	7.8	More Details
CVE-2023-29461	An arbitrary code execution vulnerability contained in Rockwell Automation's Arena Simulation software was reported that could potentially allow a malicious user to commit unauthorized arbitrary code to the software by using a memory buffer overflow in the heap. potentially resulting in a complete loss of confidentiality, integrity, and availability.	7.8	More Details
CVE-2022-48244	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2023-30986	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 3), Solid Edge SE2023 (All versions < V223.0 Update 2). Affected applications contain a memory corruption vulnerability while parsing specially crafted STP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19561)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48248	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2022-44433	In phoneEx service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2023-30237	CyberGhostVPN Windows Client before v8.3.10.10015 was discovered to contain a DLL injection vulnerability via the component Dashboard.exe.	7.8	More Details
CVE-2022-48247	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2023-29460	An arbitrary code execution vulnerability contained in Rockwell Automation's Arena Simulation software was reported that could potentially allow a malicious user to commit unauthorized arbitrary code to the software by using a memory buffer overflow potentially resulting in a complete loss of confidentiality, integrity, and availability.	7.8	More Details
CVE-2023-27965	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, Studio Display Firmware Update 16.4. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-48383	.In srtd service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2023-27936	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to cause unexpected system termination or write kernel memory.	7.8	More Details
CVE-2023-27949	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2023-24946	Windows Backup Service Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27946	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2023-30257	A buffer overflow in the component /proc/ftxxxx-debug of FiiO M6 Build Number v1.0.4 allows attackers to escalate privileges to root.	7.8	More Details
CVE-2023-27938	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in GarageBand for macOS 10.4.8. Parsing a maliciously crafted MIDI file may lead to an unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2023-27937	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, tvOS 16.4, watchOS 9.4. Parsing a maliciously crafted plist may lead to an unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2023-24949	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-29343	SysInternals Sysmon for Windows Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-24953	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-23525	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, macOS Big Sur 11.7.5. An app may be able to gain root privileges.	7.8	More Details
CVE-2023-23540	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.8 and iPadOS 15.7.8, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4, macOS Big Sur 11.7.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-29336	Win32k Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23536	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, macOS Big Sur 11.7.5, iOS 15.7.4 and iPadOS 15.7.4, macOS Monterey 12.6.4, tvOS 16.4, watchOS 9.4. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-29340	AV1 Video Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-27957	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2017-11197	In CyberArk Viewfinity 5.5.10.95 and 6.x before 6.1.1.220, a low privilege user can escalate to an administrative user via a bug within the "add printer" option.	7.8	More Details
CVE-2020-22429	redox-os v0.1.0 was discovered to contain a use-after-free bug via the gethostbyaddr() function at /src/header/netdb/mod.rs.	7.8	More Details
CVE-2023-24902	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-31240	An issue found in libming v.0.4.8 allows a local attacker to execute arbitrary code via the parseSWF_IMPORTASSETS function in the parser.c file.	7.8	More Details
CVE-2023-32233	In the Linux kernel through 6.3.1, a use-after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled.	7.8	More Details
CVE-2023-2610	Integer Overflow or Wraparound in GitHub repository vim/vim prior to 9.0.1532.	7.8	More Details
CVE-2023-28181	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, iOS 15.7.6 and iPadOS 15.7.6, macOS Monterey 12.6.4, macOS Big Sur 11.7.7, tvOS 16.4, watchOS 9.4. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27280	OS Command injection vulnerability in mblog 3.5.0 allows attackers to execute arbitrary code via crafted theme when it gets selected.	7.8	More Details
CVE-2023-27970	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-27969	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, tvOS 16.4, watchOS 9.4. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-29341	AV1 Video Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-27959	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-48369	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	7.8	More Details
CVE-2023-24905	Remote Desktop Client Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-27960	This issue was addressed by removing the vulnerable code. This issue is fixed in GarageBand for macOS 10.4.8. An app may be able to gain elevated privileges during the installation of GarageBand.	7.8	More Details
CVE-2023-2534	Improper Authorization vulnerability in OTRS AG OTRS 8 (Websocket API backend) allows any as Agent authenticated attacker to track user behaviour and to gain live insight into overall system usage. User IDs can easily be correlated with real names e. g. via ticket histories by any user. (Fuzzing for garnering other adjacent user/sensitive data). Subscribing to all possible push events could also lead to performance implications on the server side, depending on the size of the installation and the number of active users. (Flooding)This issue affects OTRS: from 8.0.X before 8.0.32.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22787	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point.	7.5	More Details
CVE-2023-30551	Rekor is an open source software supply chain transparency log. Rekor prior to version 1.1.1 may crash due to out of memory (OOM) conditions caused by reading archive metadata files into memory without checking their sizes first. Verification of a JAR file submitted to Rekor can cause an out of memory crash if files within the META-INF directory of the JAR are sufficiently large. Parsing of an APK file submitted to Rekor can cause an out of memory crash if the .SIGN or .PKGINFO files within the APK are sufficiently large. The OOM crash has been patched in Rekor version 1.1.1. There are no known workarounds.	7.5	More Details
CVE-2023-30837	Vyper is a pythonic smart contract language for the EVM. The storage allocator does not guard against allocation overflows in versions prior to 0.3.8. An attacker can overwrite the owner variable. This issue was fixed in version 0.3.8.	7.5	More Details
CVE-2023-32290	The myMail app through 14.30 for iOS sends cleartext credentials in a situation where STARTTLS is expected by a server.	7.5	More Details
CVE-2023-24506	Milesight NCR/camera version 71.8.0.6-r5 exposes credentials through an unspecified request.	7.5	More Details
CVE-2023-29350	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	7.5	More Details
CVE-2021-31239	An issue found in SQLite SQLite3 v.3.35.4 that allows a remote attacker to cause a denial of service via the appendvfs.c function.	7.5	More Details
CVE-2023-32235	Ghost before 5.42.1 allows remote attackers to read arbitrary files within the active theme's folder via /assets/built%2F..%2F..%2F/ directory traversal. This occurs in frontend/web/middleware/static-theme.js.	7.5	More Details
CVE-2023-25289	Directory Traversal vulnerability in virtualreception Digital Receptie version win7sp1_rtm.101119-1850 6.1.7601.1.0.65792 in embedded web server, allows attacker to gain sensitive information via a crafted GET request.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27963	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Monterey 12.6.4, tvOS 16.4, watchOS 9.4. A shortcut may be able to use sensitive data with certain actions without prompting the user.	7.5	More Details
CVE-2023-31133	Ghost is an app for new-media creators with tools to build a website, publish content, send newsletters, and offer paid subscriptions to members. Prior to version 5.46.1, due to a lack of validation when filtering on the public API endpoints, it is possible to reveal private fields via a brute force attack. Ghost(Pro) has already been patched. Maintainers can find no evidence that the issue was exploited on Ghost(Pro) prior to the patch being added. Self-hosters are impacted if running Ghost a version below v5.46.1. v5.46.1 contains a fix for this issue. As a workaround, add a block for requests to `/ghost/api/content/*` where the `filter` query parameter contains `password` or `email`.	7.5	More Details
CVE-2023-30282	PrestaShop scexportcustomers <= 3.6.1 is vulnerable to Incorrect Access Control. Due to a lack of permissions' control, a guest can access exports from the module which can lead to leak of personal information from customer table.	7.5	More Details
CVE-2023-30243	Beijing Netcon NS-ASG Application Security Gateway v6.3 is vulnerable to SQL Injection via TunnelId that allows access to sensitive information.	7.5	More Details
CVE-2023-31129	The Contiki-NG operating system versions 4.8 and prior can be triggered to dereference a NULL pointer in the message handling code for IPv6 router solicitiations. Contiki-NG contains an implementation of IPv6 Neighbor Discovery (ND) in the module `os/net/ipv6/uip-nd6.c`. The ND protocol includes a message type called Router Solicitation (RS), which is used to locate routers and update their address information via the SLLAO (Source Link-Layer Address Option). If the indicated source address changes, a given neighbor entry is set to the STALE state. The message handler does not check for RS messages with an SLLAO that indicates a link-layer address change that a neighbor entry can actually be created for the indicated address. The resulting pointer is used without a check, leading to the dereference of a NULL pointer of type `uip_ds6_nbr_t`. The problem has been patched in the `develop` branch of Contiki-NG, and will be included in the upcoming 4.9 release. As a workaround, users can apply Contiki-NG pull request #2271 to patch the problem directly.	7.5	More Details
CVE-2023-31181	WJJ Software - InnoKB Server, InnoKB/Console 2.2.1 - CWE-22: Path Traversal	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31478	An issue was discovered on GL.iNet devices before 3.216. An API endpoint reveals information about the Wi-Fi configuration, including the SSID and key.	7.5	More Details
CVE-2023-32111	In SAP PowerDesigner (Proxy) - version 16.7, an attacker can send a crafted request from a remote host to the proxy machine and crash the proxy server, due to faulty implementation of memory management causing a memory corruption. This leads to a high impact on availability of the application.	7.5	More Details
CVE-2022-30995	Sensitive information disclosure due to improper authentication. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 29486, Acronis Cyber Backup 12.5 (Windows, Linux) before build 16545.	7.5	More Details
CVE-2021-46755	Failure to unmap certain SysHub mappings in error paths of the ASP (AMD Secure Processor) bootloader may allow an attacker with a malicious bootloader to exhaust the SysHub resources resulting in a potential denial of service.	7.5	More Details
CVE-2017-20184	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Carlo Gavazzi Powersoft up to version 2.1.1.1 allows an unauthenticated, remote attacker to download any file from the affected device.	7.5	More Details
CVE-2023-31137	MaraDNS is open-source software that implements the Domain Name System (DNS). In version 3.5.0024 and prior, a remotely exploitable integer underflow vulnerability in the DNS packet decompression function allows an attacker to cause a Denial of Service by triggering an abnormal program termination. The vulnerability exists in the `decomp_get_rddata` function within the `Decompress.c` file. When handling a DNS packet with an Answer RR of qtype 16 (TXT record) and any qclass, if the `rdlength` is smaller than `rdata`, the result of the line `Decompress.c:886` is a negative number `len = rdlength - total;`. This value is then passed to the `decomp_append_bytes` function without proper validation, causing the program to attempt to allocate a massive chunk of memory that is impossible to allocate. Consequently, the program exits with an error code of 64, causing a Denial of Service. One proposed fix for this vulnerability is to patch `Decompress.c:887` by breaking `if(len <= 0)`, which has been incorporated in version 3.5.0036 via commit bab062bde40b2ae8a91eecd522e84d8b993bab58.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27378	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2022-23818	Insufficient input validation on the model specific register: VM_HSAVE_PA may potentially lead to loss of SEV-SNP guest memory integrity.	7.5	More Details
CVE-2023-22640	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests.	7.5	More Details
CVE-2021-46764	Improper validation of DRAM addresses in SMU may allow an attacker to overwrite sensitive memory locations within the ASP potentially resulting in a denial of service.	7.5	More Details
CVE-2021-46763	Insufficient input validation in the SMU may enable a privileged attacker to write beyond the intended bounds of a shared memory buffer potentially leading to a loss of integrity.	7.5	More Details
CVE-2021-46749	Insufficient bounds checking in ASP (AMD Secure Processor) may allow for an out of bounds read in SMI (System Management Interface) mailbox checksum calculation triggering a data abort, resulting in a potential denial of service.	7.5	More Details
CVE-2021-26406	Insufficient validation in parsing Owner's Certificate Authority (OCA) certificates in SEV (AMD Secure Encrypted Virtualization) and SEV-ES user application can lead to a host crash potentially resulting in denial of service.	7.5	More Details
CVE-2023-31476	An issue was discovered on GL.iNet devices running firmware before 3.216. There is an arbitrary file write in which an empty file can be created almost anywhere on the filesystem, as long as the filename and path is no more than 6 characters (the working directory is /www).	7.5	More Details
CVE-2023-31490	An issue found in Frrouting bgpd v.8.4.2 allows a remote attacker to cause a denial of service via the bgp_attr_psid_sub() function.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24898	Windows SMB Denial of Service Vulnerability	7.5	More Details
CVE-2023-31474	An issue was discovered on GL.iNet devices before 3.216. Through the software installation feature, it is possible to inject arbitrary parameters in a request to cause opkg to obtain a list of files in a specific directory, by using the regex feature in a package name.	7.5	More Details
CVE-2023-31472	An issue was discovered on GL.iNet devices before 3.216. There is an arbitrary file write in which an empty file can be created anywhere on the filesystem. This is caused by a command injection vulnerability with a filter applied.	7.5	More Details
CVE-2023-24901	Windows NFS Portmapper Information Disclosure Vulnerability	7.5	More Details
CVE-2023-29335	Microsoft Word Security Feature Bypass Vulnerability	7.5	More Details
CVE-2023-24939	Server for NFS Denial of Service Vulnerability	7.5	More Details
CVE-2023-24940	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability	7.5	More Details
CVE-2023-24942	Remote Procedure Call Runtime Denial of Service Vulnerability	7.5	More Details
CVE-2023-29163	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2023-29994	In NanoMQ v0.15.0-0, Heap overflow occurs in read_byte function of mqtt_code.c.	7.5	More Details
CVE-2023-20524	An attacker with a compromised ASP could possibly send malformed commands to an ASP on another CPU, resulting in an out of bounds write, potentially leading to a loss a loss of integrity.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29995	In NanoMQ v0.15.0-0, a Heap overflow occurs in copyn_utf8_str function of mqtt_parser.c	7.5	More Details
CVE-2021-46794	Insufficient bounds checking in ASP (AMD Secure Processor) may allow for an out of bounds read in SMI (System Management Interface) mailbox checksum calculation triggering a data abort, resulting in a potential denial of service.	7.5	More Details
CVE-2023-32113	SAP GUI for Windows - version 7.70, 8.0, allows an unauthorized attacker to gain NTLM authentication information of a victim by tricking it into clicking a prepared shortcut file. Depending on the authorizations of the victim, the attacker can read and modify potentially sensitive information after successful exploitation.	7.5	More Details
CVE-2021-44283	A buffer overflow in the component /Enclave.cpp of Electronics and Telecommunications Research Institute ShieldStore commit 58d455617f99705f0ffd8a27616abdf77bdc1bdc allows attackers to cause an information leak via a crafted structure from an untrusted operating system.	7.5	More Details
CVE-2023-2156	A flaw was found in the networking subsystem of the Linux kernel within the handling of the RPL protocol. This issue results from the lack of proper handling of user-supplied data, which can lead to an assertion failure. This may allow an unauthenticated remote attacker to create a denial of service condition on the system.	7.5	More Details
CVE-2021-46765	Insufficient input validation in ASP may allow an attacker with a compromised SMM to induce out-of-bounds memory reads within the ASP, potentially leading to a denial of service.	7.5	More Details
CVE-2023-29996	In NanoMQ v0.15.0-0, segment fault with Null Pointer Dereference occurs in the process of decoding subinfo_decode and unsubinfo_decode.	7.5	More Details
CVE-2023-28127	A path traversal vulnerability exists in Avalanche version 6.3.x and below that when exploited could result in possible information disclosure.	7.5	More Details
CVE-2023-30056	A session takeover vulnerability exists in FICO Origination Manager Decision Module 4.8.1 due to insufficient protection of the JSESSIONID cookie.	7.5	More Details
CVE-2023-24948	Windows Bluetooth Driver Elevation of Privilege Vulnerability	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26356	A TOCTOU in ASP bootloader may allow an attacker to tamper with the SPI ROM following data read to memory potentially resulting in S3 data corruption and information disclosure.	7.4	More Details
CVE-2023-24461	An improper certificate validation vulnerability exists in the BIG-IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.4	More Details
CVE-2023-2519	A vulnerability has been found in Caton CTP Relay Server 1.2.9 and classified as critical. This vulnerability affects unknown code of the file /server/api/v1/login of the component API. The manipulation of the argument username/password leads to sql injection. The attack can be initiated remotely. VDB-228010 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2023-2523	A vulnerability was found in Weaver E-Office 9.5. It has been rated as critical. Affected by this issue is some unknown functionality of the file App/Ajax/ajax.php?action=mobile_upload_save. The manipulation of the argument upload_quwan leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-228014 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2023-28068	Dell Command Monitor, versions 10.9 and prior, contains an improper folder permission vulnerability. A local authenticated malicious user can potentially exploit this vulnerability leading to privilege escalation by writing to a protected directory when Dell Command Monitor is installed to a non-default path	7.3	More Details
CVE-2016-15031	A vulnerability was found in PHP-Login 1.0. It has been declared as critical. This vulnerability affects the function checkLogin of the file login/scripts/class.loginscript.php of the component POST Parameter Handler. The manipulation of the argument myusername leads to sql injection. The attack can be initiated remotely. Upgrading to version 2.0 is able to address this issue. The patch is identified as 0083ec652786ddbb81335ea20da590df40035679. It is recommended to upgrade the affected component. VDB-228022 is the identifier assigned to this vulnerability.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2594	A vulnerability, which was classified as critical, was found in SourceCodester Food Ordering Management System 1.0. Affected is an unknown function of the component Registration. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-228396.	7.3	More Details
CVE-2023-22788	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2023-28742	When DNS is provisioned, an authenticated remote command execution vulnerability exists in DNS iQuery mesh. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.2	More Details
CVE-2023-1347	The Customizer Export/Import WordPress plugin before 0.9.6 unserializes user input provided via the settings, which could allow high privilege users such as admin to perform PHP Object Injection when a suitable gadget is present	7.2	More Details
CVE-2023-28832	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The web based management of affected devices does not properly validate user input, making it susceptible to command injection. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	7.2	More Details
CVE-2023-2554	External Control of File Name or Path in GitHub repository unilogies/bumsys prior to 2.2.0.	7.2	More Details
CVE-2023-24955	Microsoft SharePoint Server Remote Code Execution Vulnerability	7.2	More Details
CVE-2023-29963	S-CMS v5.0 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the component /admin/ajax.php.	7.2	More Details
CVE-2023-1408	The Video List Manager WordPress plugin through 1.7 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28128	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.3.x and below that could allow an attacker to achieve a remove code execution.	7.2	More Details
CVE-2023-2114	The NEX-Forms WordPress plugin before 8.4 does not properly escape the `table` parameter, which is populated with user input, before concatenating it to an SQL query.	7.2	More Details
CVE-2021-28998	File upload vulnerability in CMS Made Simple through 2.2.15 allows remote authenticated attackers to gain a webshell via a crafted phar file.	7.2	More Details
CVE-2023-22790	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2023-22789	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2022-47439	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Rocket Apps Open Graphite plugin <= 1.6.0 versions.	7.1	More Details
CVE-2022-45065	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Squirrly SEO Plugin by Squirrly SEO plugin <= 12.1.20 versions.	7.1	More Details
CVE-2023-23790	Cross-Site Request Forgery (CSRF) vulnerability in Pods Framework Team Pods – Custom Content Types and Fields plugin <= 2.9.10.2 versions.	7.1	More Details
CVE-2023-2460	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to bypass file access checks via a crafted HTML page. (Chromium security severity: Medium)	7.1	More Details
CVE-2022-46799	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution Easy Testimonial Slider and Form plugin <= 1.0.15 versions.	7.1	More Details
CVE-2021-26397	Insufficient address validation, may allow an attacker with a compromised ABL and UApp to corrupt sensitive memory locations potentially resulting in a loss of integrity or availability.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1385	Improper JPAKE implementation allows offline PIN brute-forcing due to the initialization of random values to a known value, which leads to unauthorized authentication to amzn.lightning services. This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS 7.6.3.3.	7.1	More Details
CVE-2023-21489	Heap out-of-bounds write vulnerability in bootloader prior to SMR May-2023 Release 1 allows a physical attacker to execute arbitrary code.	7.1	More Details
CVE-2023-24904	Windows Installer Elevation of Privilege Vulnerability	7.1	More Details
CVE-2023-23830	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ProfilePress Membership Team ProfilePress plugin <= 4.5.4 versions.	7.1	More Details
CVE-2022-47449	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in RexTheme Cart Lift – Abandoned Cart Recovery for WooCommerce and EDD plugin <= 3.1.5 versions.	7.1	More Details
CVE-2023-30743	Due to improper neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This blocks user's interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user's information through phishing attack.	7.1	More Details
CVE-2023-31138	DHIS2 Core contains the service layer and Web API for DHIS2, an information system for data capture. Starting in the 2.36 branch and prior to versions 2.37.9.1, 2.38.3.1, and 2.39.1.2, using object model traversal in the payload of a PATCH request, authenticated users with write access to an object may be able to modify related objects that they should not have access to. DHIS2 implementers should upgrade to a supported version of DHIS2 to receive a patch: 2.37.9.1, 2.38.3.1, or 2.39.1.2. It is possible to work around this issue by blocking all PATCH requests on a reverse proxy, but this may cause some issues with the functionality of built-in applications using legacy PATCH requests.	7.1	More Details
CVE-2023-28724	NGINX Management Suite default file permissions are set such that an authenticated attacker may be able to modify sensitive files on NGINX Instance Manager and NGINX API Connectivity Manager. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22710	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in chilidevs Return and Warranty Management System for WooCommerce plugin <= 1.2.3 versions.	7.1	More Details
CVE-2022-46858	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Amin A.Rezapour Product Specifications for Woocommerce plugin <= 0.6.0 versions.	7.1	More Details
CVE-2022-46864	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Umair Saleem Woocommerce Custom Checkout Fields Editor With Drag & Drop plugin <= 0.1 versions.	7.1	More Details
CVE-2020-23362	Insecure Permissons vulnerability found in Shop_CMS YerShop all versions allows a remote attacker to escalate privileges via the cover_id parameter.	7.1	More Details
CVE-2023-25961	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Catch Themes Darcie theme <= 1.1.5 versions.	7.1	More Details
CVE-2023-27968	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory.	7.1	More Details
CVE-2022-46822	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in JC Development Team WooCommerce JazzCash Gateway Plugin plugin <= 2.0 versions.	7.1	More Details
CVE-2023-24899	Windows Graphics Component Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-2182	An issue has been discovered in GitLab EE affecting all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. Under certain conditions when OpenID Connect is enabled on an instance, it may allow users who are marked as 'external' to become 'regular' users thus leading to privilege escalation for those users.	6.8	More Details
CVE-2023-30550	MeterSphere is an open source continuous testing platform, covering functions such as test tracking, interface testing, UI testing, and performance testing. This IDOR vulnerability allows the administrator of a project to modify other projects under the workspace. An attacker can obtain some operating permissions. The issue has been fixed in version 2.9.0.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46775	Improper input validation in ABL may enable an attacker with physical access, to perform arbitrary memory overwrites, potentially leading to a loss of integrity and code execution.	6.8	More Details
CVE-2023-1965	An issue has been discovered in GitLab EE affecting all versions starting from 14.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. Lack of verification on RelayState parameter allowed a maliciously crafted URL to obtain access tokens granted for 3rd party Group SAML SSO logins. This feature isn't enabled by default.	6.8	More Details
CVE-2023-21493	Improper access control vulnerability in SemShareFileProvider prior to SMR May-2023 Release 1 allows local attackers to access protected data.	6.8	More Details
CVE-2023-26203	A use of hard-coded credentials vulnerability [CWE-798] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions may allow an authenticated attacker to access to the database via shell commands.	6.7	More Details
CVE-2023-21509	Out-of-bounds Write vulnerability while processing BC_TUI_CMD_UPDATE_SCREEN in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2023-28070	Alienware Command Center Application, versions 5.5.43.0 and prior, contain an improper access control vulnerability. A local malicious user could potentially exploit this vulnerability during installation or update process leading to privilege escalation.	6.7	More Details
CVE-2023-32269	An issue was discovered in the Linux kernel before 6.1.11. In net/netrom/af_netrom.c, there is a use-after-free because accept is also allowed for a successfully connected AF_NETROM socket. However, in order for an attacker to exploit this, the system must have netrom routing configured or the attacker must have the CAP_NET_ADMIN capability.	6.7	More Details
CVE-2023-21508	Out-of-bounds Write vulnerability while processing BC_TUI_CMD_SEND_RESOURCE_DATA command in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2023-2513	A use-after-free vulnerability was found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for extended attributes. This flaw could allow a privileged local user to cause a system crash or other undefined behaviors.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21506	Out-of-bounds Write vulnerability while processing BC_TUI_CMD_SEND_RESOURCE_DATA_ARRAY command in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2023-24932	Secure Boot Security Feature Bypass Vulnerability	6.7	More Details
CVE-2023-27933	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, macOS Monterey 12.6.4, tvOS 16.4, watchOS 9.4. An app with root privileges may be able to execute arbitrary code with kernel privileges.	6.7	More Details
CVE-2023-29338	Visual Studio Code Spoofing Vulnerability	6.6	More Details
CVE-2023-23664	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in ConvertBox ConvertBox Auto Embed WordPress plugin <= 1.0.19 versions.	6.5	More Details
CVE-2022-46844	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in PixelGrade PixFields plugin <= 0.7.0 versions.	6.5	More Details
CVE-2022-41640	Auth. (subscriber+) Stored Cross-Site Scripting (XSS) vulnerability in Rymera Web Co Wholesale Suite plugin <= 2.1.5 versions.	6.5	More Details
CVE-2022-4537	The Hide My WP Ghost – Security Plugin plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 5.0.18. This is due to insufficient restrictions on where the IP Address information is being retrieved for request logging and login restrictions. Attackers can supply the X-Forwarded-For header with with a different IP Address that will be logged and can be used to bypass settings that may have blocked out an IP address from logging in.	6.5	More Details
CVE-2023-23862	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Vertical scroll recent post plugin <= 14.0 versions.	6.5	More Details
CVE-2023-24950	Microsoft SharePoint Server Spoofing Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23894	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Surbma Surbma	GDPR Proof Cookie Consent & Notice Bar plugin <= 17.5.3 versions.	6.5	More Details
CVE-2023-31179	AgilePoint NX v8.0 SU2.2 & SU2.3 - Path traversal - Vulnerability allows path traversal and downloading files from the server, by an unspecified request.	6.5	More Details
CVE-2023-24408	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Ecwid Ecommerce Ecwid Ecommerce Shopping Cart plugin <= 6.11.4 versions.	6.5	More Details
CVE-2023-28493	Auth (subscriber+) Reflected Cross-Site Scripting (XSS) vulnerability in Macho Themes NewsMag theme <= 2.4.4 versions.	6.5	More Details
CVE-2023-30855	Pimcore is an open source data and experience management platform. Versions of Pimcore prior to 10.5.18 are vulnerable to path traversal. The impact of this path traversal and arbitrary extension is limited to creation of arbitrary files and appending data to existing files. When combined with the SQL Injection, the exported data `RESTRICTED DIFFUSION 9 / 9` can be controlled and a webshell can be uploaded. Attackers can use that to execute arbitrary PHP code on the server with the permissions of the webserver. Users may upgrade to version 10.5.18 to receive a patch or, as a workaround, apply the patch manually.	6.5	More Details
CVE-2023-32060	DHIS2 Core contains the service layer and Web API for DHIS2, an information system for data capture. Starting in the 2.35 branch and prior to versions 2.36.13, 2.37.8, 2.38.2, and 2.39.0, when the Category Option Combination Sharing settings are configured to control access to specific tracker program events or program stages, the `/trackedEntityInstances` and `/events` API endpoints may include all events regardless of the sharing settings applied to the category option combinations. When this specific configuration is present, users may have access to events which they should not be able to see based on the sharing settings of the category options. The events will not appear in the user interface for web-based Tracker Capture or Capture applications, but if the Android Capture App is used they will be displayed to the user. Versions 2.36.13, 2.37.8, 2.38.2, and 2.39.0 contain a fix for this issue. No workaround is known.	6.5	More Details
CVE-2023-28182	The issue was addressed with improved authentication. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP-only authentication on a device.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28180	A denial-of-service issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. A user in a privileged network position may be able to cause a denial-of-service.	6.5	More Details
CVE-2023-23528	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in tvOS 16.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted Bluetooth packet may result in disclosure of process memory.	6.5	More Details
CVE-2023-27954	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, Safari 16.4, iOS 16.4 and iPadOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, tvOS 16.4, watchOS 9.4. A website may be able to track sensitive user information.	6.5	More Details
CVE-2023-24944	Windows Bluetooth Driver Information Disclosure Vulnerability	6.5	More Details
CVE-2023-29324	Windows MSHTML Platform Security Feature Bypass Vulnerability	6.5	More Details
CVE-2023-24954	Microsoft SharePoint Server Information Disclosure Vulnerability	6.5	More Details
CVE-2023-31125	Engine.IO is the implementation of transport-based cross-browser/cross-device bi-directional communication layer for Socket.IO. An uncaught exception vulnerability was introduced in version 5.1.0 and included in version 4.1.0 of the `socket.io` parent package. Older versions are not impacted. A specially crafted HTTP request can trigger an uncaught exception on the Engine.IO server, thus killing the Node.js process. This impacts all the users of the `engine.io` package, including those who use depending packages like `socket.io`. This issue was fixed in version 6.4.2 of Engine.IO. There is no known workaround except upgrading to a safe version.	6.5	More Details
CVE-2023-2459	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to bypass permission restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2023-29659	A Segmentation fault caused by a floating point exception exists in libheif 1.15.1 using crafted heif images via the heif::Fraction::round() function in box.cc, which causes a denial of service.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-22334	Cross Site Request Forgery (CSRF) vulnerability in beescms v4 allows attackers to delete the administrator account via crafted request to /admin/admin_admin.php.	6.5	More Details
CVE-2023-25798	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Olevmedia Olevmedia Shortcodes plugin <= 1.1.9 versions.	6.5	More Details
CVE-2022-43681	An out-of-bounds read exists in the BGP daemon of FRRouting FRR through 8.4. When sending a malformed BGP OPEN message that ends with the option length octet (or the option length word, in case of an extended OPEN message), the FRR code reads of out of the bounds of the packet, throwing a SIGABRT signal and exiting. This results in a bgpd daemon restart, causing a Denial-of-Service condition.	6.5	More Details
CVE-2022-40318	An issue was discovered in bgpd in FRRouting (FRR) through 8.4. By crafting a BGP OPEN message with an option of type 0xff (Extended Length from RFC 9072), attackers may cause a denial of service (assertion failure and daemon restart, or out-of-bounds read). This is possible because of inconsistent boundary checks that do not account for reading 3 bytes (instead of 2) in this 0xff case. NOTE: this behavior occurs in bgp_open_option_parse in the bgp_open.c file, a different location (with a different attack vector) relative to CVE-2022-40302.	6.5	More Details
CVE-2022-40302	An issue was discovered in bgpd in FRRouting (FRR) through 8.4. By crafting a BGP OPEN message with an option of type 0xff (Extended Length from RFC 9072), attackers may cause a denial of service (assertion failure and daemon restart, or out-of-bounds read). This is possible because of inconsistent boundary checks that do not account for reading 3 bytes (instead of 2) in this 0xff case.	6.5	More Details
CVE-2023-23708	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Themeisle Visualizer: Tables and Charts Manager for WordPress plugin <= 3.9.4 versions.	6.5	More Details
CVE-2023-23820	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in ProfilePress Membership Team ProfilePress plugin <= 4.5.4 versions.	6.5	More Details
CVE-2023-23874	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Metaphor Creations Ditty plugin <= 3.0.32 versions.	6.5	More Details
CVE-2023-23876	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in TMS-Plugins wpDataTables plugin <= 2.1.49 versions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25982	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Eirudo Simple YouTube Responsive plugin <= 2.5 versions.	6.5	More Details
CVE-2023-24400	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Humanity.Co Cookie Notice & Compliance for GDPR / CCPA plugin <= 2.4.6 versions.	6.5	More Details
CVE-2022-45818	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WP OnlineSupport, Essential Plugin Hero Banner Ultimate plugin <= 1.3.4 versions.	6.5	More Details
CVE-2023-22637	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions in License Management would permit an authenticated attacker to trigger remote code execution via crafted licenses.	6.5	More Details
CVE-2023-23668	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in GiveWP plugin <= 2.25.1 versions.	6.5	More Details
CVE-2022-45812	Auth. (subscriber+) Stored Cross-Site Scripting (XSS) vulnerability in Martin Lees Exxp plugin <= 2.6.8 versions.	6.5	More Details
CVE-2023-22713	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress Download Manager Gutenberg Blocks by WordPress Download Manager plugin <= 2.1.8 versions.	6.5	More Details
CVE-2023-0485	An issue has been discovered in GitLab affecting all versions starting from 13.11 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. It was possible that a project member demoted to a user role to read project updates by doing a diff with a pre-existing fork.	6.5	More Details
CVE-2023-0522	The Enable/Disable Auto Login when Register WordPress plugin through 1.1.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23470	IBM i 7.2, 7.3, 7.4, and 7.5 could allow an authenticated privileged administrator to gain elevated privileges in non-default configurations, as a result of improper SQL processing. By using a specially crafted SQL operation, the administrator could exploit the vulnerability to perform additional administrator operations. IBM X-Force ID: 244510.	6.4	More Details
CVE-2023-2069	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0 before 13.0.1. A user with the role of developer could use the import project feature to leak CI/CD variables.	6.4	More Details
CVE-2023-2524	A vulnerability classified as critical has been found in Control iD RHiD 23.3.19.0. This affects an unknown part of the file /v2/#/. The manipulation leads to direct request. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-228015. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-2596	A vulnerability was found in SourceCodester Online Reviewer System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /reviewer/system/system/admins/manage/users/user-update.php of the component GET Parameter Handler. The manipulation of the argument user_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-228398 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-30740	SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an authenticated attacker to access sensitive information which is otherwise restricted. On successful exploitation, there could be a high impact on confidentiality, limited impact on integrity and availability of the application.	6.3	More Details
CVE-2023-2595	A vulnerability has been found in SourceCodester Billing Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file ajax_service.php of the component POST Parameter Handler. The manipulation of the argument drop_services 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-228397 was assigned to this vulnerability.	6.3	More Details
CVE-2023-27945	This issue was addressed with improved entitlements. This issue is fixed in Xcode 14.3, macOS Big Sur 11.7.7, macOS Monterey 12.6.6. A sandboxed app may be able to collect system logs.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27966	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3. An app may be able to break out of its sandbox.	6.3	More Details
CVE-2023-30434	IBM Storage Scale (IBM Spectrum Scale 5.1.0.0 through 5.1.2.9, 5.1.3.0 through 5.1.6.1 and IBM Elastic Storage Systems 6.1.0.0 through 6.1.2.5, 6.1.3.0 through 6.1.6.0) could allow a local user to cause a kernel panic. IBM X-Force ID: 252187.	6.2	More Details
CVE-2023-0514	The Membership Database WordPress plugin through 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	6.1	More Details
CVE-2023-30741	Due to insufficient input validation, SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an unauthenticated attacker to redirect users to untrusted site using a malicious link. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	6.1	More Details
CVE-2023-0948	The Japanized For WooCommerce WordPress plugin before 2.5.8 does not escape generated URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting	6.1	More Details
CVE-2023-1011	The AI ChatBot WordPress plugin before 4.4.5 does not escape most of its settings before outputting them back in the dashboard, and does not have a proper CSRF check, allowing attackers to make a logged in admin set XSS payloads in them.	6.1	More Details
CVE-2023-30093	A cross-site scripting (XSS) vulnerability in Open Networking Foundation ONOS from version v1.9.0 to v2.7.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the url parameter of the API documentation dashboard.	6.1	More Details
CVE-2023-30334	AsmBB v2.9.1 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities via the MiniMag.asm and bbcode.asm libraries.	6.1	More Details
CVE-2021-46759	Improper syscall input validation in AMD TEE (Trusted Execution Environment) may allow an attacker with physical access and control of a Uapp that runs under the bootloader to reveal the contents of the ASP (AMD Secure Processor) bootloader accessible memory to a serial port, resulting in a potential loss of integrity.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0421	The Cloud Manager WordPress plugin through 1.0 does not sanitise and escape the query param ricerca before outputting it in an admin panel, allowing unauthenticated attackers to trick a logged in admin to trigger a XSS payload by clicking a link.	6.1	More Details
CVE-2023-31406	Due to insufficient input validation, SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an unauthenticated attacker to redirect users to untrusted site using a malicious link. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	6.1	More Details
CVE-2023-25831	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim’s browser.	6.1	More Details
CVE-2023-2582	A prototype pollution vulnerability exists in Strikingly CMS which can result in reflected cross-site scripting (XSS) in affected applications and sites built with Strikingly. The vulnerability exists because of Strikingly JavaScript library parsing the URL fragment allows access to the __proto__ or constructor properties and the Object prototype. By leveraging an embedded gadget like jQuery, an attacker who convinces a victim to visit a specially crafted link could achieve arbitrary javascript execution in the context of the user's browser.	6.1	More Details
CVE-2023-31180	WJJ Software - InnoKB Server, InnoKB/Console 2.2.1 - Reflected cross-site scripting (RXSS) through an unspecified request.	6.1	More Details
CVE-2023-25829	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 11.0 and 10.9.1 that may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks.	6.1	More Details
CVE-2023-24744	Cross Site Scripting (XSS) vulnerability in Rediker Software AdminPlus 6.1.91.00 allows remote attackers to run arbitrary code via the onload function within the application DOM.	6.1	More Details
CVE-2023-25830	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim’s browser.	6.1	More Details
CVE-2020-21038	Open redirect vulnerability in typecho 1.1-17.10.30-release via the referer parameter to Login.php.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19660	Cross Site Scripting (XSS) pandao editor.md 1.5.0 allows attackers to execute arbitrary code via crafted linked url values.	6.1	More Details
CVE-2020-18282	Cross-site scripting (XSS) vulnerability in NoneCms 1.3.0 allows remote attackers to inject arbitrary web script or HTML via feedback feature.	6.1	More Details
CVE-2023-31801	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the skills wheel parameter.	6.1	More Details
CVE-2023-31144	Craft CMS is a content management system. Starting in version 3.0.0 and prior to versions 3.8.4 and 4.4.4, a malformed title in the feed widget can deliver a cross-site scripting payload. This issue is fixed in version 3.8.4 and 4.4.4.	6.1	More Details
CVE-2023-30742	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker.	6.1	More Details
CVE-2023-1806	The WP Inventory Manager WordPress plugin before 2.1.0.12 does not sanitise and escape the message 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 administrators.	6.1	More Details
CVE-2020-18280	Cross Site Scripting vulnerability found in Phodal CMD v.1.0 allows a local attacker to execute arbitrary code via the EMBED SRC function.	6.1	More Details
CVE-2023-21496	Active Debug Code vulnerability in ActivityManagerService prior to SMR May-2023 Release 1 allows attacker to use debug function via setting debug level.	6.1	More Details
CVE-2023-1660	The AI ChatBot WordPress plugin before 4.4.9 does not have authorisation and CSRF in a function hooked to init, allowing unauthenticated users to update some settings, leading to Stored XSS due to the lack of escaping when outputting them in the admin dashboard	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31183	Cybonet PineApp Mail Secure A reflected cross-site scripting (XSS) vulnerability was identified in the product, using an unspecified endpoint.	6.1	More Details
CVE-2023-21500	Double free validation vulnerability in setPinPadImages in mPOS TUI trustlet prior to SMR May-2023 Release 1 allows local attackers to access the trustlet memory.	6.0	More Details
CVE-2023-21498	Improper input validation vulnerability in setPartnerTAInfo in mPOS TUI trustlet prior to SMR May-2023 Release 1 allows local attackers to overwrite the trustlet memory.	6.0	More Details
CVE-2023-27993	A relative path traversal [CWE-23] in Fortinet FortiADC version 7.2.0 and before 7.1.1 allows a privileged attacker to delete arbitrary directories from the underlying file system via crafted CLI commands.	6.0	More Details
CVE-2023-29104	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to overwrite any file the Linux user `ccuser` has write access to, or to download any file the Linux user `ccuser` has read-only access to.	6.0	More Details
CVE-2023-25796	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Include WP BaiDu Submit plugin <= 1.2.1 versions.	5.9	More Details
CVE-2023-28126	An authentication bypass vulnerability exists in Avalanche versions 6.3.x and below that could allow an attacker to gain access by exploiting the SetUser method or can exploit the Race Condition in the authentication message.	5.9	More Details
CVE-2023-23875	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Himanshu Bing Site Verification plugin using Meta Tag plugin <= 1.0 versions.	5.9	More Details
CVE-2023-23881	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in GreenTreeLabs Circles Gallery plugin <= 1.0.10 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31143	mage-ai is an open-source data pipeline tool for transforming and integrating data. Those who use Mage starting in version 0.8.34 and prior to 0.8.72 with user authentication enabled may be affected by a vulnerability. The terminal could be accessed by users who are not signed in or do not have editor permissions. Version 0.8.72 contains a fix for this issue.	5.9	More Details
CVE-2023-25021	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in FareHarbor FareHarbor for WordPress plugin <= 3.6.6 versions.	5.9	More Details
CVE-2023-25977	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in 9seeds.Com CPT – Speakers plugin <= 1.1 versions.	5.9	More Details
CVE-2022-47434	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in PB SEO Friendly Images plugin <= 4.0.5 versions.	5.9	More Details
CVE-2023-25052	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Teplitsa Yandex.News Feed by Teplitsa plugin <= 1.12.5 versions.	5.9	More Details
CVE-2023-26017	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in BlueGlass Jobs for WordPress plugin <= 2.5.10.2 versions.	5.9	More Details
CVE-2023-23793	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Eightweb Interactive Read More Without Refresh plugin <= 3.1 versions.	5.9	More Details
CVE-2023-26285	IBM MQ 9.2 CD, 9.2 LTS, 9.3 CD, and 9.3 LTS could allow a remote attacker to cause a denial of service due to an error processing invalid data. IBM X-Force ID: 248418.	5.9	More Details
CVE-2023-25452	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Michael Pretty (prettyboymp) CMS Press plugin <= 0.2.3 versions.	5.9	More Details
CVE-2023-28169	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in CoreFortress Easy Event calendar plugin <= 1.0 versions.	5.9	More Details
CVE-2023-23732	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Joel James Disqus Conditional Load plugin <= 11.0.6 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23733	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Joel James Lazy Social Comments plugin <= 2.0.4 versions.	5.9	More Details
CVE-2022-47437	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Branko Borilovic WSB Brands plugin <= 1.1.8 versions.	5.9	More Details
CVE-2023-29105	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device is vulnerable to a denial of service while parsing a random (non-JSON) MQTT payload. This could allow an attacker who can manipulate the communication between the MQTT broker and the affected device to cause a denial of service (DoS).	5.9	More Details
CVE-2023-23734	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in David Voswinkel Userlike – WordPress Live Chat plugin <= 2.2 versions.	5.9	More Details
CVE-2023-24376	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Nico Graff WP Simple Events plugin <= 1.0 versions.	5.9	More Details
CVE-2023-23883	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in David Gwyer WP Content Filter plugin <= 3.0.1 versions.	5.9	More Details
CVE-2023-23884	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kanban for WordPress Kanban Boards for WordPress plugin <= 2.5.20 versions.	5.9	More Details
CVE-2023-24372	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in USB Memory Direct Simple Custom Author Profiles plugin <= 1.0.0 versions.	5.9	More Details
CVE-2023-23647	Auth. (author+) Stored Cross-Site Scripting (XSS) vulnerability in Sk. Abul Hasan Team Member – Team with Slider plugin <= 4.4 versions.	5.9	More Details
CVE-2023-26010	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPMobile.App plugin <= 11.18 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26012	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Denzel Chia l Phire Design Custom Login Page plugin <= 2.0 versions.	5.9	More Details
CVE-2023-24900	Windows NTLM Security Support Provider Information Disclosure Vulnerability	5.9	More Details
CVE-2023-23863	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Black and White Digital Ltd TreePress – Easy Family Trees & Ancestor Profiles plugin <= 2.0.22 versions.	5.9	More Details
CVE-2023-25458	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in GMO Internet Group, Inc. TypeSquare Webfonts for ConoHa plugin <= 2.0.3 versions.	5.9	More Details
CVE-2023-23785	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in DgCult Exquisite PayPal Donation plugin <= v2.0.0 versions.	5.9	More Details
CVE-2023-28125	An improper authentication vulnerability exists in Avalanche Premise versions 6.3.x and below that could allow an attacker to gain access to the server by registering to receive messages from the server and perform an authentication bypass.	5.9	More Details
CVE-2023-26016	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Tauhidul Alam Simple Portfolio Gallery plugin <= 0.1 versions.	5.9	More Details
CVE-2023-25783	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alex Moss FireCask Like & Share Button plugin <= 1.1.5 versions.	5.9	More Details
CVE-2023-22372	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.9	More Details
CVE-2023-23808	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Sergey Panasenko Sponsors Carousel plugin <= 4.02 versions.	5.9	More Details
CVE-2023-23809	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Moris Dov Stock market charts from finviz plugin <= 1.0.1 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25784	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Bon Plan Gratos Sticky Ad Bar plugin <= 1.3.1 versions.	5.9	More Details
CVE-2021-46792	Time-of-check Time-of-use (TOCTOU) in the BIOS2PSP command may allow an attacker with a malicious BIOS to create a race condition causing the ASP bootloader to perform out-of-bounds SRAM reads upon an S3 resume event potentially leading to a denial of service.	5.9	More Details
CVE-2023-25962	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Biplob Adhikari Accordion – Multiple Accordion or FAQs Builder plugin <= 2.3.0 versions.	5.9	More Details
CVE-2023-25491	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Samuel Marshall JCH Optimize plugin <= 3.2.2 versions.	5.9	More Details
CVE-2023-25979	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Video Gallery by Total-Soft Video Gallery plugin <= 1.7.6 versions.	5.9	More Details
CVE-2023-25786	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Thom Stark Eyes Only: User Access Shortcode plugin <= 1.8.2 versions.	5.9	More Details
CVE-2022-46852	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WP Table Builder plugin <= 1.4.6 versions.	5.9	More Details
CVE-2023-25792	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in XiaoMac WP Open Social plugin <= 5.0 versions.	5.9	More Details
CVE-2023-25787	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Wbolt team WP资源下载管理 plugin <= 1.3.9 versions.	5.9	More Details
CVE-2023-25797	Auth. Stored Cross-Site Scripting (XSS) vulnerability in Mr.Vibe vSlider Multi Image Slider for WordPress plugin <= 4.1.2 versions.	5.9	More Details
CVE-2023-26519	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alex Benfica Publish to Schedule plugin <= 4.5.4 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25934	DELL ECS prior to 3.8.0.2 contains an improper verification of cryptographic signature vulnerability. A network attacker with an ability to intercept the request could potentially exploit this vulnerability to modify the body data of the request.	5.9	More Details
CVE-2023-25789	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Tapfiliate plugin <= 3.0.12 versions.	5.9	More Details
CVE-2023-26517	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Jeff Starr Dashboard Widgets Suite plugin <= 3.2.1 versions.	5.9	More Details
CVE-2023-22683	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Themis Solutions, Inc. Clio Grow plugin <= 1.0.0 versions.	5.9	More Details
CVE-2023-30840	Fluid is an open source Kubernetes-native distributed dataset orchestrator and accelerator for data-intensive applications. Starting in version 0.7.0 and prior to version 0.8.6, if a malicious user gains control of a Kubernetes node running fluid csi pod (controlled by the `csi-nodeplugin-fluid` node-daemonset), they can leverage the fluid-csi service account to modify specs of all the nodes in the cluster. However, since this service account lacks `list node` permissions, the attacker may need to use other techniques to identify vulnerable nodes. Once the attacker identifies and modifies the node specs, they can manipulate system-level-privileged components to access all secrets in the cluster or execute pods on other nodes. This allows them to elevate privileges beyond the compromised node and potentially gain full privileged access to the whole cluster. To exploit this vulnerability, the attacker can make all other nodes unschedulable (for example, patch node with taints) and wait for system-critical components with high privilege to appear on the compromised node. However, this attack requires two prerequisites: a compromised node and identifying all vulnerable nodes through other means. Version 0.8.6 contains a patch for this issue. As a workaround, delete the `csi-nodeplugin-fluid` daemonset in `fluid-system` namespace and avoid using CSI mode to mount FUSE file systems. Alternatively, using sidecar mode to mount FUSE file systems is recommended.	5.8	More Details
CVE-2023-1178	An issue has been discovered in GitLab CE/EE affecting all versions from 8.6 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. File integrity may be compromised when source code or installation packages are pulled from a tag or from a release containing a ref to another commit.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21502	Improper input validation vulnerability in FactoryTest application prior to SMR May-2023 Release 1 allows local attackers to get privilege escalation via debugging commands.	5.7	More Details
CVE-2023-21494	Potential buffer overflow vulnerability in auth api in mm_Authentication.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access.	5.6	More Details
CVE-2023-26125	Versions of the package github.com/gin-gonic/gin before 1.9.0 are vulnerable to Improper Input Validation by allowing an attacker to use a specially crafted request via the X-Forwarded-Prefix header, potentially leading to cache poisoning. **Note:** Although this issue does not pose a significant threat on its own it can serve as an input vector for other more impactful vulnerabilities. However, successful exploitation may depend on the server configuration and whether the header is used in the application logic.	5.6	More Details
CVE-2023-21503	Potential buffer overflow vulnerability in mm_LteInterRatManagement.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access.	5.6	More Details
CVE-2023-21504	Potential buffer overflow vulnerability in mm_Plmncoordination.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access.	5.6	More Details
CVE-2023-31974	yasm v1.3.0 was discovered to contain a use after free via the function error at /nasm/nasm-pp.c. Note: Multiple third parties dispute this as a bug and not a vulnerability according to the YASM security policy.	5.5	More Details
CVE-2022-47487	In thermal service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service local denial of service with no additional execution privileges.	5.5	More Details
CVE-2023-31972	yasm v1.3.0 was discovered to contain a use after free via the function pp_getline at /nasm/nasm-pp.c. Note: Multiple third parties dispute this as a bug and not a vulnerability according to the YASM security policy.	5.5	More Details
CVE-2022-38685	In bluetooth service, there is a possible missing permission check. This could lead to local denial of service in bluetooth service with no additional execution privileges needed.	5.5	More Details
CVE-2022-47340	In h265 codec firmware, 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.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44420	In modem, there is a possible missing verification of HashMME value in Security Mode Command. This could local denial of service with no additional execution privileges.	5.5	More Details
CVE-2022-44419	In modem, there is a possible missing verification of NAS Security Mode Command Replay Attacks in LTE. This could local denial of service with no additional execution privileges.	5.5	More Details
CVE-2023-31489	An issue found in Frrouting bgpd v.8.4.2 allows a remote attacker to cause a denial of service via the bgp_capability_llgr() function.	5.5	More Details
CVE-2022-47490	In soter service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	5.5	More Details
CVE-2022-48377	In dialer service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	5.5	More Details
CVE-2022-47492	In soter service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	5.5	More Details
CVE-2023-30083	Buffer Overflow vulnerability found in Libming swftophp v.0.4.8 allows a local attacker to cause a denial of service via the newVar_N in util/decompile.c.	5.5	More Details
CVE-2022-48375	In contacts service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	5.5	More Details
CVE-2022-48378	In engineermode service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	5.5	More Details
CVE-2022-48379	In dialer service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	5.5	More Details
CVE-2023-31973	yasm v1.3.0 was discovered to contain a use after free via the function expand_mmac_params at /nasm/nasm-pp.c. Note: Multiple third parties dispute this as a bug and not a vulnerability according to the YASM security policy.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48371	In dialer service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges.	5.5	More Details
CVE-2022-48370	In dialer service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges.	5.5	More Details
CVE-2022-48242	In telephony service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges.	5.5	More Details
CVE-2022-48241	In telephony service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	5.5	More Details
CVE-2022-48234	In FM service , there is a possible missing params check. This could lead to local denial of service in FM service .	5.5	More Details
CVE-2022-47493	In soter service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	5.5	More Details
CVE-2022-48233	In FM service , there is a possible missing params check. This could lead to local denial of service in FM service .	5.5	More Details
CVE-2022-48232	In FM service , there is a possible missing params check. This could lead to local denial of service in FM service .	5.5	More Details
CVE-2022-48231	In soter service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	5.5	More Details
CVE-2023-30084	An issue found in libming swftophp v.0.4.8 allows a local attacker to cause a denial of service via the stackVal function in util/decompile.c.	5.5	More Details
CVE-2022-48376	In dialer service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	5.5	More Details
CVE-2023-30086	Buffer Overflow vulnerability found in Libtiff V.4.0.7 allows a local attacker to cause a denial of service via the tiffcp function in tiffcp.c.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30087	Buffer Overflow vulnerability found in Cesanta MJS v.1.26 allows a local attacker to cause a denial of service via the mjs_mk_string function in mjs.c.	5.5	More Details
CVE-2023-30088	An issue found in Cesanta MJS v.1.26 allows a local attacker to cause a denial of service via the mjs_execute function in mjs.c.	5.5	More Details
CVE-2023-30085	Buffer Overflow vulnerability found in Libming swftophp v.0.4.8 allows a local attacker to cause a denial of service via the cws2fws function in util/decompile.c.	5.5	More Details
CVE-2023-28200	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2023-24945	Windows iSCSI Target Service Information Disclosure Vulnerability	5.5	More Details
CVE-2023-2609	NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.1531.	5.5	More Details
CVE-2023-28251	Windows Driver Revocation List Security Feature Bypass Vulnerability	5.5	More Details
CVE-2023-23527	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, tvOS 16.4, watchOS 9.4. A user may gain access to protected parts of the file system.	5.5	More Details
CVE-2023-22874	IBM MQ Clients 9.2 CD, 9.3 CD, and 9.3 LTS are vulnerable to a denial of service attack when processing configuration files. IBM X-Force ID: 244216.	5.5	More Details
CVE-2023-29932	llvm-project commit fdbc55a5 was discovered to contain a segmentation fault via the component mlir::IROperand<mlir::OpOperand.	5.5	More Details
CVE-2023-29933	llvm-project commit bd456297 was discovered to contain a segmentation fault via the component mlir::Block::getArgument.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29934	llvm-project commit 6c01b5c was discovered to contain a segmentation fault via the component mlir::Type::getDialect().	5.5	More Details
CVE-2023-29935	llvm-project commit a0138390 was discovered to contain an assertion failure at !replacements.count(op) && "operation was already replaced.	5.5	More Details
CVE-2023-29939	llvm-project commit a0138390 was discovered to contain a segmentation fault via the component mlir::spirv::TargetEnv::TargetEnv(mlir::spirv::TargetEnvAttr).	5.5	More Details
CVE-2023-27962	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2023-27961	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Monterey 12.6.4, watchOS 9.4, macOS Big Sur 11.7.5. Importing a maliciously crafted calendar invitation may exfiltrate user information.	5.5	More Details
CVE-2023-29941	llvm-project commit a0138390 was discovered to contain a segmentation fault via the component matchAndRewriteSortOp<mlir::sparse_tensor::SortOp> (mlir::sparse_tensor::SortOp.	5.5	More Details
CVE-2023-29942	llvm-project commit a0138390 was discovered to contain a segmentation fault via the component mlir::Type::isa<mlir::LLVM::LLVMVoidType.	5.5	More Details
CVE-2023-27956	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, tvOS 16.4, watchOS 9.4. Processing a maliciously crafted image may result in disclosure of process memory.	5.5	More Details
CVE-2023-27955	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, macOS Monterey 12.6.4, tvOS 16.4, macOS Big Sur 11.7.5. An app may be able to read arbitrary files.	5.5	More Details
CVE-2023-23533	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4. An app may be able to modify protected parts of the file system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27951	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An archive may be able to bypass Gatekeeper.	5.5	More Details
CVE-2023-23534	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5. Processing a maliciously crafted image may result in disclosure of process memory.	5.5	More Details
CVE-2023-23535	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, macOS Big Sur 11.7.5, iOS 15.7.4 and iPadOS 15.7.4, macOS Monterey 12.6.6, tvOS 16.4, watchOS 9.4. Processing a maliciously crafted image may result in disclosure of process memory.	5.5	More Details
CVE-2023-23537	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, watchOS 9.4, macOS Big Sur 11.7.5. An app may be able to read sensitive location information.	5.5	More Details
CVE-2023-23538	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2023-27943	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Files downloaded from the internet may not have the quarantine flag applied.	5.5	More Details
CVE-2023-27942	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, tvOS 16.4, watchOS 9.4. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2023-27941	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2023-23542	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2023-27929	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, iOS 16.4 and iPadOS 16.4, watchOS 9.4. Processing a maliciously crafted image may result in disclosure of process memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27932	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, Safari 16.4, iOS 16.4 and iPadOS 16.4, tvOS 16.4, watchOS 9.4. Processing maliciously crafted web content may bypass Same Origin Policy.	5.5	More Details
CVE-2023-28178	A logic issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, macOS Monterey 12.6.4, tvOS 16.4, watchOS 9.4. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2023-27931	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.3, iOS 16.4 and iPadOS 16.4, macOS Big Sur 11.7.3, tvOS 16.4, watchOS 9.4. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2023-28190	A privacy issue was addressed by moving sensitive data to a more secure location. This issue is fixed in macOS Ventura 13.3. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2021-26354	Insufficient bounds checking in ASP may allow an attacker to issue a system call from a compromised ABL which may cause arbitrary memory values to be initialized to zero, potentially leading to a loss of integrity.	5.5	More Details
CVE-2021-26371	A compromised or malicious ABL or UApp could send a SHA256 system call to the bootloader, which may result in exposure of ASP memory to userspace, potentially leading to information disclosure.	5.5	More Details
CVE-2023-28192	A permissions issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to read sensitive location information.	5.5	More Details
CVE-2023-30300	An issue in the component hang.wasm of WebAssembly 1.0 causes an infinite loop.	5.5	More Details
CVE-2023-28189	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to view sensitive information.	5.5	More Details
CVE-2023-29240	An authenticated attacker granted a Viewer or Auditor role on a BIG-IQ can upload arbitrary files using an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0542	The Custom Post Type List Shortcode WordPress plugin through 1.4.4 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.	5.4	More Details
CVE-2023-0268	The Mega Addons For WPBakery Page Builder WordPress plugin before 4.3.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-30619	Tuleap Open ALM is a Libre and Open Source tool for end to end traceability of application and system developments. The title of an artifact is not properly escaped in the tooltip. A malicious user with the capability to create an artifact or to edit a field title could force victim to execute uncontrolled code. This issue has been patched in version 14.7.99.143.	5.4	More Details
CVE-2023-0280	The Ultimate Carousel For Elementor WordPress plugin through 2.1.7 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.	5.4	More Details
CVE-2023-30184	A stored cross-site scripting (XSS) vulnerability in Typecho v1.2.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the url parameter at /index.php/archives/1/comment.	5.4	More Details
CVE-2023-27075	A cross-site scripting vulnerability (XSS) in the component microbin/src/pasta.rs of Microbin v1.2.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2023-1651	The AI ChatBot WordPress plugin before 4.4.9 does not have authorisation and CSRF in the AJAX action responsible to update the OpenAI settings, allowing any authenticated users, such as subscriber to update them. Furthermore, due to the lack of escaping of the settings, this could also lead to Stored XSS	5.4	More Details
CVE-2023-0537	The Product Slider For WooCommerce Lite WordPress plugin through 1.1.7 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	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1905	The WP Popups WordPress plugin before 2.1.5.1 does not properly escape the href attribute of its spu-facebook-page shortcode before outputting it 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. This is due to an insufficient fix of CVE-2023-24003	5.4	More Details
CVE-2023-24957	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246115.	5.4	More Details
CVE-2023-29247	Task instance details page in the UI is vulnerable to a stored XSS.This issue affects Apache Airflow: before 2.6.0.	5.4	More Details
CVE-2023-0267	The Ultimate Carousel For WPBakery Page Builder WordPress plugin through 2.6 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.	5.4	More Details
CVE-2023-22791	A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge-case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive information can occur are complex and depend on factors that are beyond the control of the attacker.	5.4	More Details
CVE-2023-30057	Multiple stored cross-site scripting (XSS) vulnerabilities in FICO Origination Manager Decision Module 4.8.1 allow attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2023-29839	A Stored Cross Site Scripting (XSS) vulnerability exists in multiple pages of Hotel Druid version 3.0.4, which allows arbitrary execution of commands. The vulnerable fields are Surname, Name, and Nickname in the Document function.	5.4	More Details
CVE-2023-30094	A stored cross-site scripting (XSS) vulnerability in TotalJS Flow v10 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the platform name field in the settings module.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30095	A stored cross-site scripting (XSS) vulnerability in TotalJS messenger commit b6cf1c9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the channel description field.	5.4	More Details
CVE-2023-30096	A stored cross-site scripting (XSS) vulnerability in TotalJS messenger commit b6cf1c9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the user information field.	5.4	More Details
CVE-2023-30097	A stored cross-site scripting (XSS) vulnerability in TotalJS messenger commit b6cf1c9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the private task field.	5.4	More Details
CVE-2023-31407	SAP Business Planning and Consolidation - versions 740, 750, allows an authorized attacker to upload a malicious file, resulting in Cross-Site Scripting vulnerability. After successful exploitation, an attacker can cause limited impact on confidentiality and integrity of the application.	5.4	More Details
CVE-2023-1383	An Improper Enforcement of Behavioral Workflow vulnerability in the exchangeDeviceServices function on the amzn.dmgr service allowed an attacker to register services that are only locally accessible. This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS versions prior to 7.6.3.3.	5.4	More Details
CVE-2023-2591	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in GitHub repository nilsteampassnet/teampass prior to 3.0.7.	5.4	More Details
CVE-2023-0526	The Post Shortcode WordPress plugin through 2.0.9 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	5.4	More Details
CVE-2023-31804	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the course category parameters.	5.4	More Details
CVE-2023-25834	Changes to user permissions in Portal for ArcGIS 10.9.1 and below are incompletely applied in specific use cases. This issue may allow users to access content that they are no longer privileged to access.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29188	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data.	5.4	More Details
CVE-2023-31807	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via a crafted payload to the personal notes function.	5.4	More Details
CVE-2023-32066	Time Tracker is an open source time tracking system. The week view plugin in Time Tracker versions 1.22.11.5782 and prior was not escaping titles for notes in week view table. Because of that, it was possible for a logged in user to enter notes with elements of JavaScript. Such script could then be executed in user browser on subsequent requests to week view. This issue is fixed in version 1.22.12.5783. As a workaround, use `htmlspecialchars` when calling `$field->setTitle` on line #245 in the `week.php` file, as happens in version 1.22.12.5783.	5.4	More Details
CVE-2023-30788	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the application via CSTI in the `people/add` endpoint and nickName, description, lastName, middleName and firstName parameter.	5.4	More Details
CVE-2023-31802	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the skype and linedin_url parameters.	5.4	More Details
CVE-2023-31800	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the forum title parameter.	5.4	More Details
CVE-2023-30787	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the application via CSTI in the `people:id/introductions` endpoint and first_met_additional_info parameter.	5.4	More Details
CVE-2023-30790	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the application via CSTI in the `people:id/relationships` endpoint and first_name and last_name parameter.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1265	An issue has been discovered in GitLab affecting all versions starting from 11.9 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. The condition allows for a privileged attacker, under certain conditions, to obtain session tokens from all users of a GitLab instance.	5.4	More Details
CVE-2022-43866	IBM Maximo Asset Management 7.6.1.2 and 7.6.1.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 239436.	5.4	More Details
CVE-2023-30789	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the application via CSTI in the `people:id/work` endpoint and job and company parameter.	5.4	More Details
CVE-2021-31711	Cross Site Scripting vulnerability found in Trippo ResponsiveFilemanager v.9.14.0 and before allows a remote attacker to execute arbitrary code via the sort_by parameter in the dialog.php file.	5.4	More Details
CVE-2023-2516	Cross-site Scripting (XSS) - Stored in GitHub repository nilsteampassnet/teampass prior to 3.0.7.	5.4	More Details
CVE-2023-2553	Cross-site Scripting (XSS) - Stored in GitHub repository unilogies/bumsys prior to 2.2.0.	5.4	More Details
CVE-2023-30216	Insecure permissions in the updateUserInfo function of newbee-mall before commit 1f2c2dfy allows attackers to obtain user account information.	5.4	More Details
CVE-2023-31806	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via a crafted payload to the My Progress function.	5.4	More Details
CVE-2023-0536	The Wp-D3 WordPress plugin through 2.4.1 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.	5.4	More Details
CVE-2023-0155	An issue has been discovered in GitLab CE/EE affecting all versions before 15.8.5, 15.9.4, 15.10.1. Open redirects was possible due to framing arbitrary content on any page allowing user controlled markdown	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21486	Improper export of android application components vulnerability in ImagePreviewActivity in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox.	5.3	More Details
CVE-2023-29106	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint is accessible via REST API without authentication. This could allow an unauthenticated remote attacker to download the files available via the endpoint.	5.3	More Details
CVE-2023-24505	Milesight NCR/camera version 71.8.0.6-r5 discloses sensitive information through an unspecified request.	5.3	More Details
CVE-2023-1894	A Regular Expression Denial of Service (ReDoS) issue was discovered in Puppet Server 7.9.2 certificate validation. An issue related to specifically crafted certificate names significantly slowed down server operations.	5.3	More Details
CVE-2023-29107	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint discloses some undocumented files. This could allow an unauthenticated remote attacker to gain access to additional information resources.	5.3	More Details
CVE-2023-28317	A vulnerability has been discovered in Rocket.Chat, where editing messages can change the original timestamp, causing the UI to display messages in an incorrect order.	5.3	More Details
CVE-2022-43919	IBM MQ 9.2 CD, 9.2 LTS, 9.3 CD, and 9.3 LTS could allow an authenticated attacker with authorization to craft messages to cause a denial of service. IBM X-Force ID: 241354.	5.3	More Details
CVE-2023-30019	imgproxy <=3.14.0 is vulnerable to Server-Side Request Forgery (SSRF) due to a lack of sanitization of the imageURL parameter.	5.3	More Details
CVE-2023-28290	Microsoft Remote Desktop app for Windows Information Disclosure Vulnerability	5.3	More Details
CVE-2022-45860	A weak authentication vulnerability [CWE-1390] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions in device registration page may allow an unauthenticated attacker to perform password spraying attacks with an increased chance of success.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28318	A vulnerability has been discovered in Rocket.Chat, where messages can be hidden regardless of the Message_KeepHistory or Message_ShowDeletedStatus server configuration. This allows users to bypass the intended message deletion behavior, hiding messages and deletion notices.	5.3	More Details
CVE-2023-21485	Improper export of android application components vulnerability in VideoPreviewActivity in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox.	5.3	More Details
CVE-2023-23494	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to cause a denial-of-service.	5.3	More Details
CVE-2023-24594	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.3	More Details
CVE-2023-21404	AXIS OS 11.0.X - 11.3.x use a static RSA key in legacy LUA-components to protect Axis-specific source code. The static RSA key is not used in any other secure communication nor can it be used to compromise the device or any customer data.	5.3	More Details
CVE-2023-21484	Improper access control vulnerability in AppLock prior to SMR May-2023 Release 1 allows local attackers without proper permission to execute a privileged operation.	5.1	More Details
CVE-2022-43877	IBM UrbanCode Deploy (UCD) versions up to 7.3.0.1 could disclose sensitive password information during a manual edit of the agentrelay.properties file. IBM X-Force ID: 240148.	5.1	More Details
CVE-2023-21487	Improper access control vulnerability in Telephony framework prior to SMR May-2023 Release 1 allows local attackers to change a call setting.	5.1	More Details
CVE-2023-31404	Under certain conditions, SAP BusinessObjects Business Intelligence Platform (Central Management Service) - versions 420, 430, allows an attacker to access information which would otherwise be restricted. Some users with specific privileges could have access to credentials of other users. It could let them access data sources which would otherwise be restricted.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0805	An issue has been discovered in GitLab EE affecting all versions starting from 15.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. A malicious group member may continue to have access to the public projects of a public group even after being banned from the public group by the owner.	4.9	More Details
CVE-2023-1979	The Web Stories for WordPress plugin supports the WordPress built-in functionality of protecting content with a password. The content is then only accessible to website visitors after entering the password. In WordPress, users with the "Author" role can create stories, but don't have the ability to edit password protected stories. The vulnerability allowed users with said role to bypass this permission check when trying to duplicate the protected story in the plugin's own dashboard, giving them access to the seemingly protected content. We recommend upgrading to version 1.32 or beyond commit ad49781c2a35c5c92ef704d4b621ab4e5cb77d68 https://github.com/GoogleForCreators/web-stories-wp/commit/ad49781c2a35c5c92ef704d4b621ab4e5cb77d68	4.9	More Details
CVE-2023-31805	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local authenticated attacker to execute arbitrary code via the homepage function.	4.8	More Details
CVE-2023-31141	OpenSearch is open-source software suite for search, analytics, and observability applications. Prior to versions 1.3.10 and 2.7.0, there is an issue with the implementation of fine-grained access control rules (document-level security, field-level security and field masking) where they are not correctly applied to the queries during extremely rare race conditions potentially leading to incorrect access authorization. For this issue to be triggered, two concurrent requests need to land on the same instance exactly when query cache eviction happens, once every four hours. OpenSearch 1.3.10 and 2.7.0 contain a fix for this issue.	4.8	More Details
CVE-2023-2550	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.13.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31140	OpenProject is open source project management software. Starting with version 7.4.0 and prior to version 12.5.4, when a user registers and confirms their first two-factor authentication (2FA) device for an account, existing logged in sessions for that user account are not terminated. Likewise, if an administrators creates a mobile phone 2FA device on behalf of a user, their existing sessions are not terminated. The issue has been resolved in OpenProject version 12.5.4 by actively terminating sessions of user accounts having registered and confirmed a 2FA device. As a workaround, users who register the first 2FA device on their account can manually log out to terminate all other active sessions. This is the default behavior of OpenProject but might be disabled through a configuration option. Double check that this option is not overridden if one plans to employ the workaround.	4.8	More Details
CVE-2023-1649	The AI ChatBot WordPress plugin before 4.5.1 does not sanitise and escape numerous 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)	4.8	More Details
CVE-2023-2427	Cross-site Scripting (XSS) - Reflected in GitHub repository thorsten/phpmyfaq prior to 3.1.13.	4.8	More Details
CVE-2023-30205	A stored cross-site scripting (XSS) vulnerability in DouPHP v1.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the unique_id parameter in /admin/article.php.	4.8	More Details
CVE-2020-18132	Cross Site Scripting (XSS) vulnerability in MIPCMS 3.6.0 allows attackers to execute arbitrary code via the category name field to categoryEdit.	4.8	More Details
CVE-2023-0756	An issue has been discovered in GitLab affecting all versions before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. The main branch of a repository with a specially crafted name allows an attacker to create repositories with malicious code, victims who clone or download these repositories will execute arbitrary code on their systems.	4.8	More Details
CVE-2022-39161	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0, and IBM WebSphere Application Server Liberty, when configured to communicate with the Web Server Plug-ins for IBM WebSphere Application Server, could allow an authenticated user to conduct spoofing attacks. A man-in-the-middle attacker could exploit this vulnerability using a certificate issued by a trusted authority to obtain sensitive information. IBM X-Force ID: 235069.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31799	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the system annnouncements parameter.	4.8	More Details
CVE-2023-31134	Tauri is software for building applications for multi-platform deployment. The Tauri IPC is usually strictly isolated from external websites, but in versions 1.0.0 until 1.0.9, 1.1.0 until 1.1.4, and 1.2.0 until 1.2.5, the isolation can be bypassed by redirecting an existing Tauri window to an external website. This is either possible by an application implementing a feature for users to visit arbitrary websites or due to a bug allowing the open redirect. This allows the external website access to the IPC layer and therefore to all configured and exposed Tauri API endpoints and application specific implemented Tauri commands. This issue has been patched in versions 1.0.9, 1.1.4, and 1.2.5. As a workaround, prevent arbitrary input in redirect features and/or only allow trusted websites access to the IPC.	4.8	More Details
CVE-2023-2566	Cross-site Scripting (XSS) - Stored in GitHub repository openemr/openemr prior to 7.0.1.	4.8	More Details
CVE-2023-0544	The WP Login Box WordPress plugin through 2.0.2 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)	4.8	More Details
CVE-2023-31803	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the resource sequencing parameters.	4.8	More Details
CVE-2023-0894	The Pickup l Delivery l Dine-in date time WordPress plugin through 1.0.9 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)	4.8	More Details
CVE-2023-29354	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2522	A vulnerability was found in Chengdu VEC40G 3.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /send_order.cgi?parameter=access_detect of the component Network Detection. The manipulation of the argument COUNT with the input 3 | netstat -an leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-228013 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2023-27952	A race condition was addressed with improved locking. This issue is fixed in macOS Ventura 13.3. An app may bypass Gatekeeper checks.	4.7	More Details
CVE-2023-21490	Improper access control in GearManagerStub prior to SMR May-2023 Release 1 allows a local attacker to delete applications installed by watchmanager.	4.7	More Details
CVE-2023-20098	A vulnerability in the CLI of Cisco SDWAN vManage Software could allow an authenticated, local attacker to delete arbitrary files. This vulnerability is due to improper filtering of directory traversal character sequences within system commands. An attacker with administrative privileges could exploit this vulnerability by running a system command containing directory traversal character sequences to target an arbitrary file. A successful exploit could allow the attacker to delete arbitrary files from the system, including files owned by root.	4.4	More Details
CVE-2023-1836	A cross-site scripting issue has been discovered in GitLab affecting all versions starting from 5.1 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. When viewing an XML file in a repository in "raw" mode, it can be made to render as HTML if viewed under specific circumstances	4.4	More Details
CVE-2022-48240	In camera driver, 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.	4.4	More Details
CVE-2022-47497	In soter 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.	4.4	More Details
CVE-2023-21497	Use of externally-controlled format string vulnerability in mPOS TUI trustlet prior to SMR May-2023 Release 1 allows local attackers to access the memory address.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48238	In Image filter, 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.	4.4	More Details
CVE-2022-48237	In Image filter, 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.	4.4	More Details
CVE-2022-48236	In MP3 encoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	4.4	More Details
CVE-2022-48235	In MP3 encoder, 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.	4.4	More Details
CVE-2022-47499	In soter 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.	4.4	More Details
CVE-2022-47498	In soter 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.	4.4	More Details
CVE-2022-47496	In soter 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.	4.4	More Details
CVE-2022-47495	In soter 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.	4.4	More Details
CVE-2022-47494	In soter 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.	4.4	More Details
CVE-2022-47491	In soter 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.	4.4	More Details
CVE-2022-47489	In soter 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.	4.4	More Details
CVE-2022-47488	In spipe drive, 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.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47486	In ext4fsfilter driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	4.4	More Details
CVE-2022-47485	In modem control device, 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.	4.4	More Details
CVE-2022-47470	In ext4fsfilter driver, there is a possible out of bounds read due to a missing bounds check. This could local denial of service with System execution privileges needed.	4.4	More Details
CVE-2022-47469	In ext4fsfilter driver, there is a possible out of bounds read due to a missing bounds check. This could local denial of service with System execution privileges needed.	4.4	More Details
CVE-2022-47334	In phasecheck server, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	4.4	More Details
CVE-2022-39089	In mlog service, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	4.4	More Details
CVE-2023-21507	Out-of-bounds Read vulnerability while processing BC_TUI_CMD_SEND_RESOURCE_DATA_ARRAY command in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to read arbitrary memory.	4.4	More Details
CVE-2023-21510	Out-of-bounds Read vulnerability while processing BC_TUI_CMD_UPDATE_SCREEN in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to read arbitrary memory.	4.4	More Details
CVE-2023-21511	Out-of-bounds Read vulnerability while processing CMD_COLDWALLET_BTC_SET_PRV_UTXO in bc_core trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to read arbitrary memory.	4.4	More Details
CVE-2022-48239	In camera driver, 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.	4.4	More Details
CVE-2022-22313	IBM QRadar Data Synchronization App 1.0 through 3.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 217370.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48386	the apipe driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed.	4.4	More Details
CVE-2022-48389	In modem control device, 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.	4.4	More Details
CVE-2022-48387	the apipe driver, 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.	4.4	More Details
CVE-2023-21488	Improper access control vulnerablility in Tips prior to SMR May-2023 Release 1 allows local attackers to launch arbitrary activity in Tips.	4.4	More Details
CVE-2022-48372	In bootcp 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.	4.4	More Details
CVE-2022-48373	In tee 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.	4.4	More Details
CVE-2022-48374	In tee 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.	4.4	More Details
CVE-2022-48380	In modem control device, 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.	4.4	More Details
CVE-2022-48381	In modem control device, 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.	4.4	More Details
CVE-2023-21492	Kernel pointers are printed in the log file prior to SMR May-2023 Release 1 allows a privileged local attacker to bypass ASLR.	4.4	More Details
CVE-2022-48382	In log 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.	4.4	More Details
CVE-2022-48385	In cp_dump driver, 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.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28406	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.3	More Details
CVE-2023-2464	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to perform an origin spoof in the security UI via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-1204	An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.1 before 15.10.8, all versions starting from 15.11 before 15.11.7, all versions starting from 16.0 before 16.0.2. A user could use an unverified email as a public email and commit email by sending a specifically crafted request on user update settings.	4.3	More Details
CVE-2023-22691	Cross-Site Request Forgery (CSRF) vulnerability in Tips and Tricks HQ, Ruhul Amin Category Specific RSS feed Subscription plugin <= v2.1 versions.	4.3	More Details
CVE-2023-2466	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to spoof the contents of the security UI via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2023-2463	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2022-43950	A URL redirection to untrusted site ('Open Redirect') vulnerability [CWE-601] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.1 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions may allow an unauthenticated attacker to redirect users to any arbitrary website via a crafted URL.	4.3	More Details
CVE-2023-2465	Inappropriate implementation in CORS in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29103	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device uses a hard-coded password to protect the diagnostic files. This could allow an authenticated attacker to access protected data.	4.3	More Details
CVE-2023-2467	Inappropriate implementation in Prompts in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to bypass permissions restrictions via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2023-1384	The setMediaSource function on the amzn.thin.pl service does not sanitize the "source" parameter allowing for arbitrary javascript code to be run This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS versions prior to 7.6.3.3.	4.3	More Details
CVE-2023-25967	Cross-Site Request Forgery (CSRF) vulnerability in PeepSo Community by PeepSo plugin <= 6.0.2.0 versions.	4.3	More Details
CVE-2023-2468	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed a remote attacker who had compromised the renderer process to obfuscate the security UI via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2023-31139	DHIS2 Core contains the service layer and Web API for DHIS2, an information system for data capture. Starting in the 2.37 branch and prior to versions 2.37.9.1, 2.38.3.1, and 2.39.1.2, Personal Access Tokens (PATs) generate unrestricted session cookies. This may lead to a bypass of other access restrictions (for example, based on allowed IP addresses or HTTP methods). DHIS2 implementers should upgrade to a supported version of DHIS2: 2.37.9.1, 2.38.3.1, or 2.39.1.2. Implementers can work around this issue by adding extra access control validations on a reverse proxy.	4.3	More Details
CVE-2023-2462	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to obfuscate main origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2022-45858	A use of a weak cryptographic algorithm vulnerability [CWE-327] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.0 all versions, 8.8.0 all versions, 8.7.0 all versions may increase the chances of an attacker to have access to sensitive information or to perform man-in-the-middle attacks.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-4914	IBM Cloud Pak System Suite 2.3.3.0 through 2.3.3.5 does not invalidate session after logout which could allow a local user to impersonate another user on the system. IBM X-Force ID: 191290.	4.2	More Details
CVE-2022-45859	An insufficiently protected credentials vulnerability [CWE-522] in FortiNAC-F 7.2.0, FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.0 all versions, 8.7.0 all versions may allow a local attacker with system access to retrieve users' passwords.	4.1	More Details
CVE-2022-38707	IBM Cognos Command Center 10.2.4.1 could allow a local attacker to obtain sensitive information due to insufficient session expiration. IBM X-Force ID: 234179.	4.0	More Details
CVE-2023-21495	Improper access control vulnerability in Knox Enrollment Service prior to SMR May-2023 Release 1 allow attacker install KSP app when device admin is set.	4.0	More Details
CVE-2023-21505	Improper access control in Samsung Core Service prior to version 2.1.00.36 allows attacker to write arbitrary file in sandbox.	4.0	More Details
CVE-2021-46762	Insufficient input validation in the SMU may allow an attacker to corrupt SMU SRAM potentially leading to a loss of integrity or denial of service.	3.9	More Details
CVE-2023-29128	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to write any file with the extension `.db`.	3.8	More Details
CVE-2023-28764	SAP BusinessObjects Platform - versions 420, 430, Information design tool transmits sensitive information as cleartext in the binaries over the network. This could allow an unauthenticated attacker with deep knowledge to gain sensitive information such as user credentials and domain names, which may have a low impact on confidentiality and no impact on the integrity and availability of the system.	3.7	More Details
CVE-2023-31136	PostgresNIO is a Swift client for PostgreSQL. Any user of PostgresNIO prior to version 1.14.2 connecting to servers with TLS enabled is vulnerable to a man-in-the-middle attacker injecting false responses to the client's first few queries, despite the use of TLS certificate verification and encryption. The vulnerability is addressed in PostgresNIO versions starting from 1.14.2. There are no known workarounds for unpatched users.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23543	The issue was addressed with additional restrictions on the observability of app states. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4, watchOS 9.4. A sandboxed app may be able to determine which app is currently using the camera.	3.6	More Details
CVE-2017-20183	A vulnerability was found in External Media without Import Plugin up to 1.0.0 on WordPress. It has been declared as problematic. This vulnerability affects the function print_media_new_panel of the file external-media-without-import.php. The manipulation of the argument url/error/width/height/mime-type leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 1.0.1 is able to address this issue. The patch is identified as 9d2ecd159a6e2e3f710b4f1c28e2714f66502746. It is recommended to upgrade the affected component. VDB-227950 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-2565	A vulnerability has been found in SourceCodester Multi Language Hotel Management Software 1.0 and classified as problematic. This vulnerability affects unknown code of the file ajax.php of the component POST Parameter Handler. The manipulation of the argument complaint_type with the input <script>alert(document.cookie)</script> 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-228172.	3.5	More Details
CVE-2023-2560	A vulnerability was found in jja8 NewBingGoGo up to 2023.5.5.2. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-228167.	3.5	More Details
CVE-2023-2521	A vulnerability was found in NEXTU NEXT-7004N 3.0.1. It has been classified as problematic. Affected is an unknown function of the file /boafrm/formFilter of the component POST Request Handler. The manipulation of the argument url with the input <svg onload=alert(1337)> leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-228012. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-2590	Missing Authorization in GitHub repository answerdev/answer prior to 1.0.9.	3.5	More Details
CVE-2023-29333	Microsoft Access Denial of Service Vulnerability	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23541	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to access information about a user's contacts.	3.3	More Details
CVE-2023-23523	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Photos belonging to the Hidden Photos Album could be viewed without authentication through Visual Lookup.	3.3	More Details
CVE-2023-27928	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, tvOS 16.4, watchOS 9.4, macOS Big Sur 11.7.5. An app may be able to access information about a user's contacts.	3.3	More Details
CVE-2023-27408	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). The `i2c` mutex file is created with the permissions bits of `-rw-rw-rw-`. This file is used as a mutex for multiple applications interacting with i2c. This could allow an authenticated attacker with access to the SSH interface on the affected device to interfere with the integrity of the mutex and the data it protects.	3.3	More Details
CVE-2023-22813	A device API endpoint was missing access controls on Western Digital My Cloud OS 5 iOS and Anroid Mobile Apps, My Cloud Home iOS and Android Mobile Apps, SanDisk ibi iOS and Android Mobile Apps, My Cloud OS 5 Web App, My Cloud Home Web App and the SanDisk ibi Web App. Due to a permissive CORS policy and missing authentication requirement for private IPs, a remote attacker on the same network as the device could obtain device information by convincing a victim user to visit an attacker-controlled server and issue a cross-site request. This issue affects My Cloud OS 5 Mobile App: before 4.21.0; My Cloud Home Mobile App: before 4.21.0; ibi Mobile App: before 4.21.0; My Cloud OS 5 Web App: before 4.26.0-6126; My Cloud Home Web App: before 4.26.0-6126; ibi Web App: before 4.26.0-6126.	3.3	More Details
CVE-2023-31413	Filebeat versions through 7.17.9 and 8.6.2 have a flaw in httpjson input that allows the http request Authorization or Proxy-Authorization header contents to be leaked in the logs when debug logging is enabled.	3.3	More Details
CVE-2023-30985	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 3), Solid Edge SE2023 (All versions < V223.0 Update 2). Affected applications contain an out of bounds read past the end of an allocated buffer while parsing a specially crafted OBJ file. This vulnerability could allow an attacker to disclose sensitive information. (ZDI-CAN-19426)	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31975	yasm v1.3.0 was discovered to contain a memory leak via the function yasm_intnum_copy at /libyasm/intnum.c. Note: Multiple third parties dispute this as a bug and not a vulnerability according to the YASM security policy.	3.3	More Details
CVE-2023-28194	The issue was addressed with improved checks. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to unexpectedly create a bookmark on the Home Screen.	3.3	More Details
CVE-2023-29092	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface.	3.1	More Details
CVE-2022-4376	An issue has been discovered in GitLab affecting all versions before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. Under certain conditions, an attacker may be able to map a private email of a GitLab user to their GitLab account on an instance.	3.1	More Details
CVE-2023-30844	Mutagen provides real-time file synchronization and flexible network forwarding for developers. Prior to versions 0.16.6 and 0.17.1 in `mutagen` and prior to version 0.17.1 in `mutagen-compose`, Mutagen `list` and `monitor` commands are susceptible to control characters that could be provided by remote endpoints. This could cause terminal corruption, either intentional or unintentional, if these characters were present in error messages or file paths/names. This could be used as an attack vector if synchronizing with an untrusted remote endpoint, synchronizing files not under control of the user, or forwarding to/from an untrusted remote endpoint. On very old systems with terminals susceptible to issues such as CVE-2003-0069, the issue could theoretically cause code execution. The problem has been patched in Mutagen v0.16.6 and v0.17.1. Earlier versions of Mutagen are no longer supported and will not be patched. Versions of Mutagen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk.	3.0	More Details
CVE-2023-32112	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system.	2.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27410	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). A heap-based buffer overflow vulnerability was found in the `edgebox_web_app` binary. The binary will crash if supplied with a backup password longer than 255 characters. This could allow an authenticated privileged attacker to cause a denial of service.	2.7	More Details
CVE-2023-27409	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). A path traversal vulnerability was found in the `deviceinfo` binary via the `mac` parameter. This could allow an authenticated attacker with access to the SSH interface on the affected device to read the contents of any file named `address`.	2.5	More Details
CVE-2022-26733	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32806	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32804	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32791	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32779	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-26735	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-26734	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-26729	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-26732	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22645	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-26705	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-26692	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-26689	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-22649	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32808	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32822	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32809	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2023-2540	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-2537	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2022-46728	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-46727	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46719	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-46708	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-46707	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-42857	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-42835	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2023-2536	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2022-42822	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-42804	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-42802	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-42794	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32930	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2535	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2022-32921	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32901	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32884	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32878	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32874	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32873	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32856	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-32850	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2023-2539	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details