SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 13 December 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-2023-4122	Student Information System v1.0 is vulnerable to an Insecure File Upload vulnerability on the 'photo' parameter of my-profile page, allowing an authenticated attacker to obtain Remote Code Execution on the server hosting the application.	9.9	More Details
CVE-2023-48930	xinhu xinhuoa 2.2.1 contains a File upload vulnerability.	9.8	More Details
CVE-2023-50002	Tenda W30E V16.01.0.12(4843) was discovered to contain a stack overflow via the function formRebootMeshNode.	9.8	More Details
CVE-2023-40301	NETSCOUT nGeniusPULSE 3.8 has a Command Injection Vulnerability.	9.8	More Details
CVE-2023-22524	Certain versions of the Atlassian Companion App for MacOS were affected by a remote code execution vulnerability. An attacker could utilize WebSockets to bypass Atlassian Companion's blocklist and MacOS Gatekeeper to allow execution of code.	9.8	More Details
CVE-2023-49404	Tenda W30E V16.01.0.12(4843) was discovered to contain a stack overflow via the function formAdvancedSetListSet.	9.8	More Details
CVE-2023-49405	Tenda W30E V16.01.0.12(4843) was discovered to contain a stack overflow via the function UploadCfg.	9.8	More Details
CVE-2023-49406	Tenda W30E V16.01.0.12(4843) was discovered to contain a Command Execution vulnerability via the function /goform/telnet.	9.8	More Details
CVE-2023-49408	Tenda AX3 V16.03.12.11 was discovered to contain a stack overflow via the function set_device_name.	9.8	More Details
CVE-2023-49409	Tenda AX3 V16.03.12.11 was discovered to contain a Command Execution vulnerability via the function /goform/telnet.	9.8	More Details
CVE-2023-49411	Tenda W30E V16.01.0.12(4843) contains a stack overflow vulnerability via the function formDeleteMeshNode.	9.8	More Details
CVE-2023-5008	Student Information System v1.0 is vulnerable to an unauthenticated SQL Injection vulnerability on the 'regno' parameter of index.php page, allowing an external attacker to dump all the contents of the database contents and bypass the login control.	9.8	More Details
CVE-2023-43742	An authentication bypass in Zultys MX-SE, MX-SE II, MX-E, MX-Virtual, MX250, and MX30 with firmware versions prior to 17.0.10 patch 17161 and 16.04 patch 16109 allows an unauthenticated attacker to obtain an administrative session via a protection mechanism failure in the authentication function. In normal operation, the Zultys MX Administrator Windows client connects to port 7505 and attempts authentication, submitting the administrator username and password to the server. Upon authentication failure, the server sends a login failure message prompting the client to disconnect. However, if the client ignores the failure message instead and attempts to continue, the server does not forcibly close the connection and processes all subsequent requests from the client as if authentication had been successful.	9.8	More Details
CVE-2023-48929	Franklin Fueling Systems System Sentinel AnyWare (SSA) version 1.6.24.492 is vulnerable to Session Fixation. The 'sid' parameter in the group_status.asp resource allows an attacker to escalate privileges and obtain sensitive information.	9.8	More Details
CVE-2023-49007	In Netgear Orbi RBR750 firmware before V7.2.6.21, there is a stack-based buffer overflow in /usr/sbin/httpd.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49443	DoraCMS v2.1.8 was discovered to re-use the same code for verification of valid usernames and passwords. This vulnerability allows attackers to gain access to the application via a bruteforce attack.	9.8	More Details
CVE-2023-48423	In dhcp4_SetPDNAddress of dhcp4_Main.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-46498	An issue in EverShop NPM versions before v.1.0.0-rc.8 allows a remote attacker to obtain sensitive information and execute arbitrary code via the /deleteCustomer/route.json file.	9.8	More Details
CVE-2023-46932	Heap Buffer Overflow vulnerability in GPAC version 2.3-DEV-rev617-g671976fcc-master, allows attackers to execute arbitrary code and cause a denial of service (DoS) via str2ulong class in src/media_tools/avilib.c in gpac/MP4Box.	9.8	More Details
CVE-2023-47254	An OS Command Injection in the CLI interface on DrayTek Vigor167 version 5.2.2, allows remote attackers to execute arbitrary system commands and escalate privileges via any account created within the web interface.	9.8	More Details
CVE-2023-48417	Missing Permission checks resulting in unauthorized access and Manipulation in KeyChainActivity Application	9.8	More Details
CVE-2023-48424	U-Boot shell vulnerability resulting in Privilege escalation in a production device	9.8	More Details
CVE-2023-48425	U-Boot vulnerability resulting in persistent Code Execution	9.8	More Details
CVE-2023-6181	An oversight in BCB handling of reboot reason that allows for persistent code execution	9.8	More Details
CVE-2023-49417	TOTOLink A7000R V9.1.0u.6115_B20201022 has a stack overflow vulnerability via setOpModeCfg.	9.8	More Details
CVE-2023-49418	TOTOLink A7000R V9.1.0u.6115_B20201022has a stack overflow vulnerability via setIpPortFilterRules.	9.8	More Details
CVE-2023-50245	OpenEXR-viewer is a viewer for OpenEXR files with detailed metadata probing. Versions prior to 0.6.1 have a memory overflow vulnerability. This issue is fixed in version 0.6.1.	9.8	More Details
CVE-2023-46454	In GL.iNET GL-AR300M routers with firmware v4.3.7, it is possible to inject arbitrary shell commands through a crafted package name in the package information functionality.	9.8	More Details
CVE-2023-46456	In GL.iNET GL-AR300M routers with firmware 3.216 it is possible to inject arbitrary shell commands through the OpenVPN client file upload functionality.	9.8	More Details
CVE-2023-6593	Client side permission bypass in Devolutions Remote Desktop Manager 2023.3.4.0 and earlier on iOS allows an attacker that has access to the application to execute entries in a SQL data source without restriction.	9.8	More Details
CVE-2013-2513	The flash_tool gem through 0.6.0 for Ruby allows command execution via shell metacharacters in the name of a downloaded file.	9.8	More Details
CVE-2023-40300	NETSCOUT nGeniusPULSE 3.8 has a Hardcoded Cryptographic Key.	9.8	More Details
CVE-2023-43364	main.py in Searchor before 2.4.2 uses eval on CLI input, which may cause unexpected code execution.	9.8	More Details
CVE-2023-50001	Tenda W30E V16.01.0.12(4843) was discovered to contain a stack overflow via the function formUpgradeMeshOnline.	9.8	More Details
CVE-2023-49428	Tenda AX12 V22.03.01.46 has been discovered to contain a command injection vulnerability in the 'mac' parameter at /goform/SetOnlineDevName.	9.8	More Details
CVE-2023-48849	Ruijie EG Series Routers version EG_3.0(1)B11P216 and before allows unauthenticated attackers to remotely execute arbitrary code due to incorrect filtering.	9.8	More Details
CVE-2023-46773	Permission management vulnerability in the PMS module. Successful exploitation of this vulnerability may cause privilege escalation.	9.8	More Details
CVE-2023-36655	The login REST API in ProLion CryptoSpike 3.0.15P2 (when LDAP or Active Directory is used as the users store) allows a remote blocked user to login and obtain an authentication token by specifying a username with different uppercase/lowercase character combination.	9.8	More Details
CVE-2023-46353	In the module "Product Tag Icons Pro" (ticons) before 1.8.4 from MyPresta.eu for PrestaShop, a guest can perform SQL injection. The method TiconProduct::getTiconByProductAndTicon() has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection.	9.8	More Details
CVE-2023-5761	The Burst Statistics – Privacy-Friendly Analytics for WordPress plugin for WordPress is vulnerable to SQL Injection via the 'url' parameter in versions 1.4.0 to 1.4.6.1 (free) and versions 1.4.0 to 1.5.0 (pro) due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41913	strongSwan before 5.9.12 has a buffer overflow and possible unauthenticated remote code execution via a DH public value that exceeds the internal buffer in charon-tkm's DH proxy. The earliest affected version is 5.3.0. An attack can occur via a crafted IKE_SA_INIT message.	9.8	More Details
CVE-2023-48823	A Blind SQL injection issue in ajax.php in GaatiTrack Courier Management System 1.0 allows an unauthenticated attacker to inject a payload via the email parameter during login.	9.8	More Details
CVE-2023-48860	TOTOLINK N300RT version 3.2.4-B20180730.0906 has a post-authentication RCE due to incorrect access control, allows attackers can bypass front-end security restrictions and execute arbitrary code.	9.8	More Details
CVE-2023-50164	An attacker can manipulate file upload params to enable paths traversal and under some circumstances this can lead to uploading a malicious file which can be used to perform Remote Code Execution. Users are recommended to upgrade to versions Struts 2.5.33 or Struts 6.3.0.2 or greater to fix this issue.	9.8	More Details
CVE-2023-35039	Improper Restriction of Excessive Authentication Attempts vulnerability in Be Devious Web Development Password Reset with Code for WordPress REST API allows Authentication Abuse.This issue affects Password Reset with Code for WordPress REST API: from n/a through 0.0.15.	9.8	More Details
CVE-2023-50000	Tenda W30E V16.01.0.12(4843) was discovered to contain a stack overflow via the function formResetMeshNode.	9.8	More Details
CVE-2023-39169	The affected devices use publicly available default credentials with administrative privileges.	9.8	More Details
CVE-2023-49425	Tenda AX12 V22.03.01.46 was discovered to contain a stack overflow via the deviceList parameter at /goform/setMacFilterCfg .	9.8	More Details
CVE-2023-49426	Tenda AX12 V22.03.01.46 was discovered to contain a stack overflow via the list parameter at /goform/SetStaticRouteCfg.	9.8	More Details
CVE-2023-49424	Tenda AX12 V22.03.01.46 was discovered to contain a stack overflow via the list parameter at /goform/SetVirtualServerCfg.	9.8	More Details
CVE-2023-49437	Tenda AX12 V22.03.01.46 has been discovered to contain a command injection vulnerability in the 'list' parameter at /goform/SetNetControlList.	9.8	More Details
CVE-2023-49434	Tenda AX9 V22.03.01.46 has been found to contain a stack overflow vulnerability in the 'list' parameter at /goform/SetNetControlList.	9.8	More Details
CVE-2023-49999	Tenda W30E V16.01.0.12(4843) was discovered to contain a command injection vulnerability via the function setUmountUSBPartition.	9.8	More Details
CVE-2023-49410	Tenda W30E V16.01.0.12(4843) was discovered to contain a stack overflow via the function via the function set_wan_status.	9.8	More Details
CVE-2023-49403	Tenda W30E V16.01.0.12(4843) was discovered to contain a command injection vulnerability via the function setFixTools.	9.8	More Details
CVE-2023-49402	Tenda W30E V16.01.0.12(4843) was discovered to contain a stack overflow via the function localMsg.	9.8	More Details
CVE-2023-49429	Tenda AX9 V22.03.01.46 was discovered to contain a SQL command injection vulnerability in the 'setDeviceInfo' feature through the 'mac' parameter at /goform/setModules.	9.8	More Details
CVE-2023-49435	Tenda AX9 V22.03.01.46 is vulnerable to command injection.	9.8	More Details
CVE-2023-49436	Tenda AX9 V22.03.01.46 has been discovered to contain a command injection vulnerability in the 'list' parameter at /goform/SetNetControlList.	9.8	More Details
CVE-2023-49433	Tenda AX9 V22.03.01.46 has been found to contain a stack overflow vulnerability in the 'list' parameter at /goform/SetVirtualServerCfg.	9.8	More Details
CVE-2023-49432	Tenda AX9 V22.03.01.46 has been found to contain a stack overflow vulnerability in the 'deviceList' parameter at /goform/setMacFilterCfg.	9.8	More Details
CVE-2023-49431	Tenda AX9 V22.03.01.46 has been discovered to contain a command injection vulnerability in the 'mac' parameter at /goform/SetOnlineDevName.	9.8	More Details
CVE-2023-49430	Tenda AX9 V22.03.01.46 has been found to contain a stack overflow vulnerability in the 'list' parameter at /goform/SetStaticRouteCfg.	9.8	More Details
CVE-2023-35618	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	9.6	More Details
CVE-2023-36019	Microsoft Power Platform Connector Spoofing Vulnerability	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36649	Insertion of sensitive information in the centralized (Grafana) logging system in ProLion CryptoSpike 3.0.15P2 allows remote attackers to impersonate other users in web management and the REST API by reading JWT tokens from logs (as a Granafa authenticated user) or from the Loki REST API without authentication.	9.1	More Details
CVE-2023-49583	SAP BTP Security Services Integration Library ([Node.js] @sap/xssec - versions < 3.6.0, allow under certain conditions an escalation of privileges. On successful exploitation, an unauthenticated attacker can obtain arbitrary permissions within the application.	9.1	More Details
CVE-2023-50422	SAP BTP Security Services Integration Library ([Java] cloud-security-services-integration-library) - versions below 2.17.0 and versions from 3.0.0 to before 3.3.0, allow under certain conditions an escalation of privileges. On successful exploitation, an unauthenticated attacker can obtain arbitrary permissions within the application.	9.1	More Details
CVE-2023-50423	SAP BTP Security Services Integration Library ([Python] sap-xssec) - versions < 4.1.0, allow under certain conditions an escalation of privileges. On successful exploitation, an unauthenticated attacker can obtain arbitrary permissions within the application.	9.1	More Details
CVE-2023-50424	SAP BTP Security Services Integration Library ([Golang] github.com/sap/cloud-security-client-go) - versions < 0.17.0, allow under certain conditions an escalation of privileges. On successful exploitation, an unauthenticated attacker can obtain arbitrary permissions within the application.	9.1	More Details
CVE-2023-39172	The affected devices transmit sensitive information unencrypted allowing a remote unauthenticated attacker to capture and modify network traffic.	9.1	More Details
CVE-2023-50429	IzyBat Orange casiers before 20230803_1 allows getEnsemble.php ensemble SQL injection.	9.1	More Details
CVE-2023-40302	NETSCOUT nGeniusPULSE 3.8 has Weak File Permissions Vulnerability	9.1	More Details

OTHER VULNERABILITIES

CVE Number	
CVE-2023-48225	Laf is a cloud development platform. Prior to version 1.0.0-beta.13, the control of LAF app enV is not strict enough, and in certain scenarios of privatization environmen env was found from the database and directly inserted into the template, resulting in controllability here. Sensitive information in the secret and configmap can be read
CVE-2023-6580	A vulnerability, which was classified as critical, was found in D-Link DIR-846 FW100A53DBR. This affects an unknown part of the file /HNAP1/ of the component QoS F vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-33413	The configuration functionality in the Intelligent Platform Management Interface (IPMI) baseboard management controller (BMC) implementation on Supermicro X11 an
CVE-2023-49465	Libde265 v1.0.14 was discovered to contain a heap-buffer-overflow vulnerability in the derive_spatial_luma_vector_prediction function at motion.cc.
CVE-2023-49464	libheif v1.17.5 was discovered to contain a segmentation violation via the function UncompressedImageCodec::get_luma_bits_per_pixel_from_configuration_unci.
CVE-2023-49463	libheif v1.17.5 was discovered to contain a segmentation violation via the function find_exif_tag at /libheif/exif.cc.
CVE-2023-49462	libheif v1.17.5 was discovered to contain a segmentation violation via the component /libheif/exif.cc.
CVE-2023-49460	libheif v1.17.5 was discovered to contain a segmentation violation via the function UncompressedImageCodec::decode_uncompressed_image.
CVE-2023-39909	Ericsson Network Manager before 23.2 mishandles Access Control and thus unauthenticated low-privilege users can access the NCM application.
CVE-2023-33412	The web interface in the Intelligent Platform Management Interface (IPMI) baseboard management controller (BMC) implementation on Supermicro X11 and M11 base
CVE-2023-49468	Libde265 v1.0.14 was discovered to contain a global buffer overflow vulnerability in the read_coding_unit function at slice.cc.

CVE Number	
CVE-2023-48841	Appointment Scheduler 3.0 is vulnerable to CSV Injection via a Language > Labels > Export action.
CVE-2023-48835	Car Rental Script v3.0 is vulnerable to CSV Injection via a Language > Labels > Export action.
CVE-2023-48830	Shuttle Booking Software 2.0 is vulnerable to CSV Injection in the Languages section via an export.
CVE-2023-48826	Time Slots Booking Calendar 4.0 is vulnerable to CSV Injection via the unique ID field of the Reservations List.
CVE-2023-48207	Availability Booking Calendar 5.0 allows CSV injection via the unique ID field in the Reservations list component.
CVE-2020-10676	In Rancher 2.x before 2.6.13 and 2.7.x before 2.7.4, an incorrectly applied authorization check allows users who have certain access to a namespace to move that nam
CVE-2023-35630	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability
CVE-2023-49467	Libde265 v1.0.14 was discovered to contain a heap-buffer-overflow vulnerability in the derive_combined_bipredictive_merging_candidates function at motion.cc.
CVE-2023-43743	A SQL injection vulnerability in Zultys MX-SE, MX-SE II, MX-E, MX-Virtual, MX250, and MX30 with firmware versions prior to 17.0.10 patch 17161 and 16.04 patch 161
CVE-2023-48859	TOTOLINK A3002RU version 2.0.0-B20190902.1958 has a post-authentication RCE due to incorrect access control, allows attackers to bypass front-end security restr
CVE-2023-32460	Dell PowerEdge BIOS contains an improper privilege management security vulnerability. An unauthenticated local attacker could potentially exploit this vulnerability, lea
CVE-2020-12613	An issue was discovered in BeyondTrust Privilege Management for Windows through 5.6. An attacker can spawn a process with multiple users as part of the security to
CVE-2023-6035	The EazyDocs WordPress plugin before 2.3.4 does not properly sanitize and escape "data" parameter before using it in an SQL statement via an AJAX action, which c
CVE-2023-36646	Incorrect user role checking in multiple REST API endpoints in ProLion CryptoSpike 3.0.15P2 allows a remote attacker with low privileges to execute privileged functior
CVE-2023-49964	An issue was discovered in Hyland Alfresco Community Edition through 7.2.0. By inserting malicious content in the folder.get.html.ftl file, an attacker may perform SSTI
CVE-2023-5500	This vulnerability allows an remote attacker with low privileges to misuse Improper Control of Generation of Code ('Code Injection') to gain full control of the affected de
CVE-2023-5869	A flaw was found in PostgreSQL that allows authenticated database users to execute arbitrary code through missing overflow checks during SQL array value modificati read the server's memory.
CVE-2023-42890	The issue was addressed with improved memory handling. This issue is fixed in Safari 17.2, macOS Sonoma 14.2, watchOS 10.2, iOS 17.2 and iPadOS 17.2, tvOS 17
CVE-2023-36006	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability

CVE Number	
CVE-2023-49797	PyInstaller bundles a Python application and all its dependencies into a single package. A PyInstaller built application, elevated as a privileged process, may be tricked user with higher privileges than the attacker). 3. The user's temporary directory is not locked to that specific user (most likely due to `TMP`/`TEMP` environment variabl was built with Python 3.7.x or earlier which has no protection against Directory Junctions links. The vulnerability has been addressed in PR #7827 which corresponds to
CVE-2023-42910	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2. Processing a maliciously crafted file may
CVE-2023-6709	Improper Neutralization of Special Elements Used in a Template Engine in GitHub repository mlflow/mlflow prior to 2.9.2.
CVE-2023-41117	An issue was discovered in EnterpriseDB Postgres Advanced Server (EPAS) before 11.21.32, 12.x before 12.16.20, 13.x before 13.12.16, 14.x before 14.9.0, and 15.x
CVE-2023-41118	An issue was discovered in EnterpriseDB Postgres Advanced Server (EPAS) before 11.21.32, 12.x before 12.16.20, 13.x before 13.12.16, 14.x before 14.9.0, and 15.x read, write, copy, rename, and delete.
CVE-2023-41119	An issue was discovered in EnterpriseDB Postgres Advanced Server (EPAS) before 11.21.32, 12.x before 12.16.20, 13.x before 13.12.16, 14.x before 14.9.0, and 15.x
CVE-2023-46157	File-Manager in MGT CloudPanel 2.0.0 through 2.3.2 allows the lowest privilege user to achieve OS command injection by changing file ownership and changing file pe
CVE-2023-48123	An issue in Netgate pfSense Plus v.23.05.1 and before and pfSense CE v.2.7.0 allows a remote attacker to execute arbitrary code via a crafted request to the packet_c
CVE-2021-3187	An issue was discovered in BeyondTrust Privilege Management for Mac before 5.7. An authenticated, unprivileged user can elevate privileges by running a malicious s
CVE-2023-35641	Internet Connection Sharing (ICS) Remote Code Execution Vulnerability
CVE-2023-49897	An OS command injection vulnerability exists in AE1021PE firmware version 2.0.9 and earlier and AE1021 firmware version 2.0.9 and earlier. If this vulnerability is expl
CVE-2023-6510	Use after free in Media Capture in Google Chrome prior to 120.0.6099.62 allowed a remote attacker who convinced a user to engage in specific UI interaction to potent
CVE-2023-6509	Use after free in Side Panel Search in Google Chrome prior to 120.0.6099.62 allowed a remote attacker who convinced a user to engage in specific UI interaction to po
CVE-2023-6508	Use after free in Media Stream in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chr
CVE-2023-22522	This Template Injection vulnerability allows an authenticated attacker, including one with anonymous access, to inject unsafe user input into a Confluence page. Using are not affected by this vulnerability. If your Confluence site is accessed via an atlassian.net domain, it is hosted by Atlassian and is not vulnerable to this issue.
CVE-2023-6514	The Bluetooth module of some Huawei Smart Screen products has an identity authentication bypass vulnerability. Successful exploitation of this vulnerability may allow
CVE-2023-22523	This vulnerability, if exploited, allows an attacker to perform privileged RCE (Remote Code Execution) on machines with the Assets Discovery agent installed. The vuln
CVE-2023-35639	Microsoft ODBC Driver Remote Code Execution Vulnerability
CVE-2023-49803	@koa/cors npm provides Cross-Origin Resource Sharing (CORS) for koa, a web framework for Node.js. Prior to version 5.0.0, the middleware operates in a way that if threat to the users of this middleware. If such behavior is expected, for instance, when middleware is used exclusively for prototypes and not for production applications

CVE Number	
CVE-2023-3517	Hitachi Vantara Pentaho Data Integration & Analytics versions before 9.5.0.1 and 9.3.0.5, including 8.3.x does not restrict JNDI identifiers during the creation of XActior
CVE-2023-28523	IBM Informix Dynamic Server 12.10 and 14.10 onsmsync is vulnerable to a heap buffer overflow, caused by improper bounds checking which could allow an attacker to
CVE-2023-6186	Insufficient macro permission validation of The Document Foundation LibreOffice allows an attacker to execute built-in macros without warning. In affected versions Lib
CVE-2023-6185	Improper Input Validation vulnerability in GStreamer integration of The Document Foundation LibreOffice allows an attacker to execute arbitrary GStreamer plugins. In a
CVE-2023-46496	Directory Traversal vulnerability in EverShop NPM versions before v.1.0.0-rc.8 allows a remote attacker to obtain sensitive information via a crafted request to the DELI
CVE-2023-50252	php-svg-lib is an SVG file parsing / rendering library. Prior to version 0.5.1, when handling `<use>` tag that references an `<image>` tag, it merges the attributes from th this issue.
CVE-2023-43301	An issue in DARTS SHOP MAXIM mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.
CVE-2023-43300	An issue in urban_project mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.
CVE-2023-36648	Missing authentication in the internal data streaming system in ProLion CryptoSpike 3.0.15P2 allows remote unauthenticated users to read potentially sensitive informa
CVE-2023-43302	An issue in sanTas mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.
CVE-2023-43303	An issue in craftbeer bar canvas mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.
CVE-2023-43304	An issue in PARK DANDAN mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.
CVE-2023-26158	All versions of the package mockjs are vulnerable to Prototype Pollution via the Util.extend function due to missing check if the attribute resolves to the object prototype attributes of object prototype (such as hasOwnProperty, toString or valueOf). User controlled inputs inside the extend() method of the Mock.Handler, Mock.Random, M continue js // src/mock/handler.js Util.extend = function extend() { var target = arguments[0] || {}, i = 1, length = arguments.length, options, name, src, copy, clone if (leng continue if (Util.isArray(copy) || Util.isObject(copy)) { if (Util.isArray(copy)) clone = src && Util.isArray(src) ? src : [] if (Util.isObject(copy)) clone = src && Util.isObject(src
CVE-2023-43305	An issue in studio kent mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.
CVE-2023-48427	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 2). Affected products do not properly validate the certificate of the configured UMC se
CVE-2023-42481	In SAP Commerce Cloud - versions HY_COM 1905, HY_COM 2005, HY_COM2105, HY_COM 2011, HY_COM 2205, COM_CLOUD 2211, a locked B2B user can mis
CVE-2023-28868	Support Assistant in NCP Secure Enterprise Client before 12.22 allows attackers to delete arbitrary files on the operating system by creating a symbolic link.
CVE-2023-35628	Windows MSHTML Platform Remote Code Execution Vulnerability
CVE-2023-35634	Windows Bluetooth Driver Remote Code Execution Vulnerability

CVE Number	
CVE-2023-48311	dockerspawner is a tool to spawn JupyterHub single user servers in Docker containers. Users of JupyterHub deployments running DockerSpawner starting with 0.11.0 dockerspawner release version 13. Users are advised to upgrade. Users unable to upgrade should explicitly set `DockerSpawner.allowed_images` to a non-empty list
CVE-2023-47565	An OS command injection vulnerability has been found to affect legacy QNAP VioStor NVR models running QVR Firmware 4.x. If exploited, the vulnerability could allov
CVE-2020-12615	An issue was discovered in BeyondTrust Privilege Management for Windows through 5.6. When adding the Add Admin token to a process, and specifying that it runs a
CVE-2023-42912	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2. Processing a maliciously crafted file may
CVE-2023-42911	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2. Processing a maliciously crafted file may
CVE-2023-42926	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2. Processing a maliciously crafted file may
CVE-2023-48861	DLL hijacking vulnerability in TTplayer version 7.0.2, allows local attackers to escalate privileges and execute arbitrary code via urlmon.dll.
CVE-2023-6288	Code injection in Remote Desktop Manager 2023.3.9.3 and earlier on macOS allows an attacker to execute code via the DYLIB_INSERT_LIBRARIES environment var
CVE-2023-36011	Win32k Elevation of Privilege Vulnerability
CVE-2023-36696	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2023-48421	In gpu_pixel_handle_buffer_liveness_update_ioctl of private/google-modules/gpu/mali_kbase/platform/pixel/pixel_gpu_slc.c, there is a possible out of bounds write due
CVE-2020-28369	In BeyondTrust Privilege Management for Windows (aka PMfW) through 5.7, a SYSTEM installation causes Cryptbase.dll to be loaded from the user-writable location '
CVE-2023-48409	In gpu_pixel_handle_buffer_liveness_update_ioctl of private/google-modules/gpu/mali_kbase/mali_kbase_core_linux.c, there is a possible out of bounds write due to a
CVE-2023-48407	there is a possible DCK won't be deleted after factory reset due to a logic error in the code. This could lead to local escalation of privilege with no additional execution p
CVE-2023-48402	In ppcfw_enable of ppcfw.c, there is a possible EoP due to a missing permission check. This could lead to local escalation of privilege with no additional execution privi
CVE-2023-48677	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40901.
CVE-2023-36391	Local Security Authority Subsystem Service Elevation of Privilege Vulnerability
CVE-2023-5058	Improper Input Validation in the processing of user-supplied splash screen during system boot in Phoenix SecureCore™ Technology™ 4 potentially allows denial-of-se
CVE-2020-12612	An issue was discovered in BeyondTrust Privilege Management for Windows through 5.6. When specifying a program to elevate, it can typically be found within the Pro can repoint this variable to any folder the user has full control of. Then, the folder structure can be created in such a way that a rule matches and arbitrary code runs ele

CVE Number	
CVE-2020-12614	An issue was discovered in BeyondTrust Privilege Management for Windows through 5.6. If the publisher criteria is selected, it defines the name of a publisher that mu
CVE-2023-42909	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2. Processing a maliciously crafted file may
CVE-2021-46899	SyncTrayzor 1.1.29 enables CEF (Chromium Embedded Framework) remote debugging, allowing a local attacker to control the application.
CVE-2023-40446	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. P
CVE-2023-50446	An issue was discovered in Mullvad VPN Windows app before 2023.6-beta1. Insufficient permissions on a directory allow any local unprivileged user to escalate privile
CVE-2023-42886	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sonoma 14.2, macOS Ventura 13.6.3, macOS Monterey 12.7.2. A
CVE-2023-35644	Windows Sysmain Service Elevation of Privilege Vulnerability
CVE-2023-42899	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.2, iOS 17.2 and iPadOS 17.2, watchOS 10.2, macOS Ventura 13.(
CVE-2023-35633	Windows Kernel Elevation of Privilege Vulnerability
CVE-2023-42901	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2. Processing a maliciously crafted file may
CVE-2023-42902	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2. Processing a maliciously crafted file may
CVE-2023-42882	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.2. Processing an image may lead to arbitrary code execution.
CVE-2023-42903	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2. Processing a maliciously crafted file may
CVE-2023-42904	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2. Processing a maliciously crafted file may
CVE-2023-42905	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2. Processing a maliciously crafted file may
CVE-2023-42906	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2. Processing a maliciously crafted file may
CVE-2023-42907	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2. Processing a maliciously crafted file may
CVE-2023-42908	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Sonoma 14.2. Processing a maliciously crafted file may
CVE-2023-35631	Win32k Elevation of Privilege Vulnerability

CVE Number	
CVE-2023-35632	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2023-21740	Windows Media Remote Code Execution Vulnerability
CVE-2023-49089	Umbraco is an ASP.NET content management system (CMS). Starting in version 8.0.0 and prior to versions 8.18.10, 10.8.1, and 12.3.0, Backoffice users with permissi
CVE-2023-49096	Jellyfin is a Free Software Media System for managing and streaming media. In affected versions there is an argument injection in the VideosController, specifically the unauthenticated user. In order to exploit this vulnerability an unauthenticated attacker has to guess an itemId, which is a completely random GUID. It's a very unlikely ca videoCodec and audioCodec are vulnerable to the argument injection. The values can be traced through a lot of code and might be changed in the process. However, t possible to add additional arguments to FFmpeg, which is powerful enough as it stands. There is probably a way of overwriting an arbitrary file with malicious content. T
CVE-2022-42784	A vulnerability has been identified in LOGO! 12/24RCE (6ED1052-1MD08-0BA1) (All versions >= V8.3), LOGO! 12/24RCEo (6ED1052-2MD08-0BA1) (All versions >= ' (6ED1052-1HB08-0BA1) (All versions >= V8.3), LOGO! 24RCEo (6ED1052-2HB08-0BA1) (All versions >= V8.3), SIPLUS LOGO! 12/24RCE (6AG1052-1MD08-7BA1) 1CC08-7BA1) (All versions >= V8.3), SIPLUS LOGO! 24CEo (6AG1052-2CC08-7BA1) (All versions >= V8.3), SIPLUS LOGO! 24RCE (6AG1052-1HB08-7BA1) (All ver allow to inject public keys of custom created key pairs which are then signed by the product CA. The generation of a custom certificate allows communication with, and
CVE-2023-6538	SMU versions prior to 14.8.7825.01 are susceptible to unintended information disclosure, through URL manipulation. Authenticated users in Storage, Server or combin
CVE-2023-36020	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability
CVE-2023-4486	Under certain circumstances, invalid authentication credentials could be sent to the login endpoint of Johnson Controls Metasys NAE55, SNE, and SNC engines prior t
CVE-2023-48404	In ProtocolMiscCarrierConfigSimInfoIndAdapter of protocolmiscadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to r
CVE-2023-49713	Denial-of-service (DoS) vulnerability exists in NetBIOS service of HMI GC-A2 series. If a remote unauthenticated attacker sends a specially crafted packets to specific p
CVE-2023-36004	Windows DPAPI (Data Protection Application Programming Interface) Spoofing Vulnerability
CVE-2023-5379	A flaw was found in Undertow. When an AJP request is sent that exceeds the max-header-size attribute in ajp-listener, JBoss EAP is marked in an error state by mod_ receiving an AJP response, and stops forwarding. This issue could allow a malicious user could to repeatedly send requests that exceed the max-header-size, causing
CVE-2023-49143	Denial-of-service (DoS) vulnerability exists in rfe service of HMI GC-A2 series. If a remote unauthenticated attacker sends a specially crafted packets to specific ports, a
CVE-2023-44099	Vulnerability of data verification errors in the kernel module. Successful exploitation of this vulnerability may cause WLAN interruption.
CVE-2023-35643	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-48122	An issue in microweber v.2.0.1 and fixed in v.2.0.4 allows a remote attacker to obtain sensitive information via the HTTP GET method.
CVE-2023-49800	`nuxt-api-party` is an open source module to proxy API requests. The library allows the user to send many options directly to `ofetch`. There is no filter on which options stack overflow as ofetch error handling works recursively resulting in a denial of service. This issue has been addressed in version 0.22.1. Users are advised to upgrad
CVE-2023-36647	A hard-coded cryptographic private key used to sign JWT authentication tokens in ProLion CryptoSpike 3.0.15P2 allows remote attackers to impersonate arbitrary user
CVE-2023-49799	`nuxt-api-party` is an open source module to proxy API requests. nuxt-api-party attempts to check if the user has passed an absolute URL to prevent the aforementione before a fetch is made the URL is normalized. "To normalize a byte sequence potentialValue, remove any leading and trailing HTTP whitespace bytes from potentialVa addressed in version 0.22.1. Users are advised to upgrade. Users unable to upgrade should revert to the previous method of detecting absolute URLs.

CVE Number	
CVE-2023-49140	Denial-of-service (DoS) vulnerability exists in commplex-link service of HMI GC-A2 series. If a remote unauthenticated attacker sends a specially crafted packets to spe
CVE-2023-41963	Denial-of-service (DoS) vulnerability exists in FTP service of HMI GC-A2 series. If a remote unauthenticated attacker sends a specially crafted packets to specific ports
CVE-2023-6337	HashiCorp Vault and Vault Enterprise 1.12.0 and newer are vulnerable to a denial of service through memory exhaustion of the host when handling large unauthenticat
CVE-2023-48416	In multiple locations, there is a possible null dereference due to a missing null check. This could lead to remote denial of service with no additional execution privileges
CVE-2023-39538	AMI AptioV contains a vulnerability in BIOS where a User may cause an unrestricted upload of a BMP Logo file with dangerous type by Local access. A successful exp
CVE-2023-49355	decToString in decNumber/decNumber.c in jq 88f01a7 has a one-byte out-of-bounds write via the " []-1.2e-1111111111" input. NOTE: this is not the same as CVE-202
CVE-2023-6245	The Candid library causes a Denial of Service while parsing a specially crafted payload with 'empty' data type. For example, if the payload is `record { * ; empty }` and tl infinite decoding loop. Canisters using affected versions of candid are exposed to denial of service by causing the decoding to run indefinitely until the canister traps du
CVE-2023-50449	JFinalCMS 5.0.0 could allow a remote attacker to read files via ../ Directory Traversal in the /common/down/file fileKey parameter.
CVE-2023-48641	Archer Platform 6.x before 6.14 P1 HF2 (6.14.0.1.2) contains an insecure direct object reference vulnerability. An authenticated malicious user in a multi-instance instal
CVE-2023-48410	In cd_ParseMsg of cd_codec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no addition
CVE-2023-48398	In ProtocolNetAcBarringInfo::ProtocolNetAcBarringInfo() of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could le
CVE-2023-42478	SAP Business Objects Business Intelligence Platform is vulnerable to stored XSS allowing an attacker to upload agnostic documents in the system which when opened
CVE-2023-48403	In sms_DecodeCodedTpMsg of sms_PduCodec.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosur
CVE-2023-50455	An issue was discovered in Zammad before 6.2.0. Due to lack of rate limiting in the "email address verification" feature, an attacker could send many requests for a knc
CVE-2023-36005	Windows Telephony Server Elevation of Privilege Vulnerability
CVE-2023-49957	An issue was discovered in Dalmann OCPP.Core before 1.3.0 for OCPP (Open Charge Point Protocol) for electric vehicles. It permits multiple transactions with the sar Why should that be rejected?"
CVE-2023-49246	Unauthorized access vulnerability in the card management module. Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2023-49244	Permission management vulnerability in the multi-user module. Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2023-49245	Unauthorized access vulnerability in the Huawei Share module. Successful exploitation of this vulnerability may affect service confidentiality.

CVE Number	
CVE-2023-33411	A web server in the Intelligent Platform Management Interface (IPMI) baseboard management controller (BMC) implementation on Supermicro X11 and M11 based dev
CVE-2023-49967	Typecho v1.2.1 was discovered to be vulnerable to an XML Quadratic Blowup attack via the component /index.php/action/xmlrpc.
CVE-2023-46354	In the module "Orders (CSV, Excel) Export PRO" (ordersexport) < 5.2.0 from MyPrestaModules for PrestaShop, a guest can download personal information without res
CVE-2023-46284	A vulnerability has been identified in Opcenter Execution Foundation (All versions < V2407), Opcenter Quality (All versions < V2312), SIMATIC PCS neo (All versions < Portal (TIA Portal) V17 (All versions < V17 Update 8), Totally Integrated Automation Portal (TIA Portal) V18 (All versions < V18 Update 3). The affected application con
CVE-2023-46285	A vulnerability has been identified in Opcenter Execution Foundation (All versions < V2407), Opcenter Quality (All versions < V2312), SIMATIC PCS neo (All versions < Portal (TIA Portal) V17 (All versions < V17 Update 8), Totally Integrated Automation Portal (TIA Portal) V18 (All versions < V18 Update 3). The affected application con
CVE-2023-39167	In SENEC Storage Box V1,V2 and V3 an unauthenticated remote attacker can obtain the devices' logfiles that contain sensitive data.
CVE-2023-49958	An issue was discovered in Dalmann OCPP.Core through 1.2.0 for OCPP (Open Charge Point Protocol) for electric vehicles. The server processes mishandle StartTra
CVE-2023-49956	An issue was discovered in Dalmann OCPP.Core before 1.3.0 for OCPP (Open Charge Point Protocol) for electric vehicles. A StopTransaction message with any rand
CVE-2023-49955	An issue was discovered in Dalmann OCPP.Core before 1.2.0 for OCPP (Open Charge Point Protocol) for electric vehicles. It does not validate the length of the charge
CVE-2023-35622	Windows DNS Spoofing Vulnerability
CVE-2023-48840	A lack of rate limiting in pjActionAjaxSend in Appointment Scheduler 3.0 allows attackers to cause resource exhaustion.
CVE-2023-46283	A vulnerability has been identified in Opcenter Execution Foundation (All versions < V2407), Opcenter Quality (All versions < V2312), SIMATIC PCS neo (All versions < Portal (TIA Portal) V17 (All versions < V17 Update 8), Totally Integrated Automation Portal (TIA Portal) V18 (All versions < V18 Update 3). The affected application con
CVE-2023-46455	In GL.iNET GL-AR300M routers with firmware v4.3.7 it is possible to write arbitrary files through a path traversal attack in the OpenVPN client file upload functionality.
CVE-2023-49247	Permission verification vulnerability in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2023-48834	A lack of rate limiting in pjActionAjaxSend in Car Rental v3.0 allows attackers to cause resource exhaustion.
CVE-2023-35621	Microsoft Dynamics 365 Finance and Operations Denial of Service Vulnerability
CVE-2023-48833	A lack of rate limiting in pjActionAJaxSend in Time Slots Booking Calendar 4.0 allows attackers to cause resource exhaustion.
CVE-2023-48831	A lack of rate limiting in pjActionAJaxSend in Availability Booking Calendar 5.0 allows attackers to cause resource exhaustion.
CVE-2023-41106	An issue was discovered in Zimbra Collaboration (ZCS) before 10.0.3. An attacker can gain access to a Zimbra account. This is also fixed in 9.0.0 Patch 35 and 8.8.15

CVE Number	
CVE-2009-4123	The jruby-openssl gem before 0.6 for JRuby mishandles SSL certificate validation.
CVE-2015-8314	The Devise gem before 3.5.4 for Ruby mishandles Remember Me cookies for sessions, which may allow an adversary to obtain unauthorized persistent application acc
CVE-2018-16153	An issue was discovered in Apereo Opencast 4.x through 10.x before 10.6. It sends system digest credentials during authentication attempts to arbitrary external servic
CVE-2023-46307	An issue was discovered in server.js in etcd-browser 87ae63d75260. By supplying a /../../../ Directory Traversal input to the URL's GET request while connecting to the
CVE-2023-28465	The package-decompression feature in HL7 (Health Level 7) FHIR Core Libraries before 5.6.106 allows attackers to copy arbitrary files to certain directories via directo
CVE-2023-49243	Vulnerability of unauthorized access to email attachments in the email module. Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2023-36010	Microsoft Defender Denial of Service Vulnerability
CVE-2023-49242	Free broadcast vulnerability in the running management module. Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2023-46156	Affected devices improperly handle specially crafted packets sent to port 102/tcp. This could allow an attacker to create a denial of service condition. A restart is neede
CVE-2023-45285	Using go get to fetch a module with the ".git" suffix may unexpectedly fallback to the insecure "git://" protocol if the module is unavailable via the secure "https://" and "g
CVE-2022-47375	A vulnerability has been identified in SIMATIC PC-Station Plus (All versions), SIMATIC S7-400 CPU 412-2 PN V7 (All versions), SIMATIC S7-400 CPU 414-3 PN/DP V PN/DP V7 (All versions), SIPLUS S7-400 CPU 416-3 PN/DP V7 (All versions). The affected products do not handle long file names correctly. This could allow an attack
CVE-2023-38380	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (incl. SIPLUS variants) (All versions < V3.4.29), SIMATIC CP 1243-1 (incl. SIPLUS variants) (All versions SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0) (All versions < V2.3), SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0) (All versions < V2.3), SIMATIC CP 1543- SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0) (All versions < V2.3), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0) (All a denial-of-service condition in the webserver of the affected product.
CVE-2023-46751	An issue was discovered in the function gdev_prn_open_printer_seekable() in Artifex Ghostscript through 10.02.0 allows remote attackers to crash the application via a
CVE-2023-49239	Unauthorized access vulnerability in the card management module. Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2023-39539	AMI AptioV contains a vulnerability in BIOS where a User may cause an unrestricted upload of a PNG Logo file with dangerous type by Local access. A successful exp
CVE-2023-49240	Unauthorized access vulnerability in the launcher module. Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2023-35638	DHCP Server Service Denial of Service Vulnerability
CVE-2023-49241	API permission control vulnerability in the network management module. Successful exploitation of this vulnerability may affect service confidentiality.
CVE-2023-44113	Vulnerability of missing permission verification for APIs in the Designed for Reliability (DFR) module. Successful exploitation of this vulnerability may affect service conf

CVE Number	
CVE-2022-47374	A vulnerability has been identified in SIMATIC PC-Station Plus (All versions), SIMATIC S7-400 CPU 412-2 PN V7 (All versions), SIMATIC S7-400 CPU 414-3 PN/DP V PN/DP V7 (All versions), SIPLUS S7-400 CPU 416-3 PN/DP V7 (All versions). The affected products do not handle HTTP(S) requests to the web server correctly. This
CVE-2023-6333	The affected ControlByWeb Relay products are vulnerable to a stored cross-site scripting vulnerability, which could allow an attacker to inject arbitrary scripts into the e
CVE-2023-6394	A flaw was found in Quarkus. This issue occurs when receiving a request over websocket with no role-based permission specified on the GraphQL operation, Quarkus
CVE-2023-6655	A vulnerability, which was classified as critical, has been found in Hongjing e-HR 2020. Affected by this issue is some unknown functionality of the file /w_selfservice/oa identifier assigned to this vulnerability.
CVE-2023-49580	SAP GUI for Windows and SAP GUI for Java - versions SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, allow an unauthenticated attacker to a response times of the AS ABAP.
CVE-2023-35624	Azure Connected Machine Agent Elevation of Privilege Vulnerability
CVE-2023-6579	A vulnerability, which was classified as critical, has been found in osCommerce 4. Affected by this issue is some unknown functionality of the file /b2b-supermarket/sho did not respond in any way.
CVE-2023-6647	A vulnerability, which was classified as critical, has been found in AMTT HiBOS 1.0. Affected by this issue is some unknown functionality. The manipulation of the argu
CVE-2023-6652	A vulnerability was found in code-projects Matrimonial Site 1.0. It has been declared as critical. Affected by this vulnerability is the function register of the file /register.pl
CVE-2023-45316	Mattermost fails to validate if a relative path is passed in /plugins/playbooks/api/v0/telemetry/run/<telem_run_id> as a telemetry run ID, allowing an attacker to use a pa
CVE-2023-6648	A vulnerability, which was classified as critical, was found in PHPGurukul Nipah Virus Testing Management System 1.0. This affects an unknown part of the file passwo
CVE-2023-6651	A vulnerability was found in code-projects Matrimonial Site 1.0. It has been classified as critical. Affected is an unknown function of the file /auth/auth.php?user=1. The
CVE-2023-6578	A vulnerability classified as critical has been found in Software AG WebMethods 10.11.x/10.15.x. Affected is an unknown function of the file wm.server/connect/. The m see details like internal IPs, ports, and versions. In some cases if access to /assets/ is refused, you may enter /assets/x as a wrong value, then come back to /assets/ w
CVE-2023-32268	Exposure of Proxy Administrator Credentials An authenticated administrator equivalent Filr user can access the credentials of proxy administrators.
CVE-2023-41623	Emlog version pro2.1.14 was discovered to contain a SQL injection vulnerability via the uid parameter at /admin/media.php.
CVE-2023-43744	An OS command injection vulnerability in Zultys MX-SE, MX-SE II, MX-E, MX-Virtual, MX250, and MX30 with firmware versions prior to 17.0.10 patch 17161 and 16.04 the patch file is passed to a shell script without validation. Including bash command substitution characters in a patch file name results in execution of the provided com
CVE-2022-45362	Server-Side Request Forgery (SSRF) vulnerability in Paytm Paytm Payment Gateway.This issue affects Paytm Payment Gateway: from n/a through 2.7.0.
CVE-2023-48428	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 2). The radius configuration mechanism of affected products does not correctly check
CVE-2023-49788	Collabora Online is a collaborative online office suite based on LibreOffice technology. Unlike a standalone dedicated Collabora Online server, the Built-in CODE Serve accessed are limited to those that the server process has access to. The bug was fixed in Collabora Online - Built-in CODE Server (richdocumentscode) release 23.5.6

CVE Number	
CVE-2023-36651	Hidden and hard-coded credentials in ProLion CryptoSpike 3.0.15P2 allow remote attackers to login to web management as super-admin and consume the most privile
CVE-2023-36650	A missing integrity check in the update system in ProLion CryptoSpike 3.0.15P2 allows attackers to execute OS commands as the root Linux user on the host system v
CVE-2023-49692	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V7.2.2), RUGGEDCOM RM1224 LTE(4G) NAM (6(SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V7.2.2), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V7.2.2) < V7.2.2), SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V7.2.2), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V7.2.2), SCALAN versions < V7.2.2), SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V7.2.2), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All v administrators to issue commands on system level after a new connection is established.
CVE-2023-49691	A vulnerability has been identified in RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2) (All versions < V8.0), RUGGEDCOM RM1224 LTE(4G) NAM (6GK SCALANCE M816-1 ADSL-Router (6GK5816-1AA00-2AA2) (All versions < V8.0), SCALANCE M816-1 ADSL-Router (6GK5816-1BA00-2AA2) (All versions < V8.0), SC SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2) (All versions < V8.0), SCALANCE M876-4 (6GK5876-4AA10-2BA2) (All versions < V8.0), SCALANCE M876-4 (E SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1) (All versions < V8.0), SCALANCE S615 EEC LAN-Router (6GK5615-0AA01-2AA2) (All versions < V8.0), SCA commands on system level after a successful IP address update.
CVE-2023-39171	SENEC Storage Box V1,V2 and V3 accidentially expose a management UI accessible with publicly known admin credentials.
CVE-2023-41804	Server-Side Request Forgery (SSRF) vulnerability in Brainstorm Force Starter Templates — Elementor, WordPress & Beaver Builder Templates.This issue affects Star
CVE-2023-6458	Mattermost webapp fails to validate route parameters in/<TEAM_NAME>/channels/<CHANNEL_NAME> allowing an attacker to perform a client-side path traversal.
CVE-2023-46282	A vulnerability has been identified in Opcenter Execution Foundation (All versions < V2407), Opcenter Quality (All versions < V2312), SIMATIC PCS neo (All versions < Portal (TIA Portal) V17 (All versions < V17 Update 8), Totally Integrated Automation Portal (TIA Portal) V18 (All versions < V18 Update 3). A reflected cross-site scriptir
CVE-2023-49782	Collabora Online is a collaborative online office suite based on LibreOffice technology. Users of Nextcloud with `Collabora Online - Built-in CODE Server` app can be vu
CVE-2023-6542	Due to lack of proper authorization checks in Emarsys SDK for Android, an attacker can call a particular activity and can forward himself web pages and/or deep links w
CVE-2023-46281	A vulnerability has been identified in Opcenter Execution Foundation (All versions < V2407), Opcenter Quality (All versions < V2312), SIMATIC PCS neo (All versions < Portal (TIA Portal) V17 (All versions < V17 Update 8), Totally Integrated Automation Portal (TIA Portal) V18 (All versions < V18 Update 3). When accessing the UMC W
CVE-2023-6610	An out-of-bounds read vulnerability was found in smb2_dump_detail in fs/smb/client/smb2ops.c in the Linux Kernel. This issue could allow a local attacker to crash the
CVE-2023-6606	An out-of-bounds read vulnerability was found in smbCalcSize in fs/smb/client/netmisc.c in the Linux Kernel. This issue could allow a local attacker to crash the system
CVE-2023-5764	A template injection flaw was found in Ansible where a user's controller internal templating operations may remove the unsafe designation from template data. This issu
CVE-2023-49695	OS command injection vulnerability in WRC-X3000GSN v1.0.2, WRC-X3000GS v1.0.24 and earlier, and WRC-X3000GSA v1.0.24 and earlier allows a network-adjacer
CVE-2023-6687	An issue was discovered by Elastic whereby Elastic Agent would log a raw event in its own logs at the WARN or ERROR level if ingesting that event to Elasticsearch fa by limiting these types of logs to DEBUG level logging, which is disabled by default.
CVE-2023-42476	SAP Business Objects Web Intelligence - version 420, allows an authenticated attacker to inject JavaScript code into Web Intelligence documents which is then execut
CVE-2023-48431	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 2). Affected software does not correctly validate the response received by an UMC se

CVE Number	
CVE-2023-49923	An issue was discovered by Elastic whereby the Documents API of App Search logged the raw contents of indexed documents at INFO log level. Depending on the co
CVE-2023-49922	An issue was discovered by Elastic whereby Beats and Elastic Agent would log a raw event in its own logs at the WARN or ERROR level if ingesting that event to Elast 7.17.16 that prevents this issue by limiting these types of logs to DEBUG level logging, which is disabled by default.
CVE-2023-35629	Microsoft USBHUB 3.0 Device Driver Remote Code Execution Vulnerability
CVE-2023-48406	there is a possible permanent DoS or way for the modem to boot unverified firmware due to a logic error in the code. This could lead to local escalation of privilege with
CVE-2023-49802	The LinkedCustomFields plugin for MantisBT allows users to link values between two custom fields, creating linked drop-downs. Prior to version 2.0.1, cross-site scripti Content Security Policy, which blocks script execution.
CVE-2023-48405	there is a possible way for the secure world to write to NS memory due to a logic error in the code. This could lead to local escalation of privilege with System executior
CVE-2023-49804	Uptime Kuma is an easy-to-use self-hosted monitoring tool. Prior to version 1.23.9, when a user changes their login password in Uptime Kuma, a previously logged-in u CVE-2023-44400, but logging existing users out of their accounts was forgotten. To mitigate the risks associated with this vulnerability, the maintainers made the serve
CVE-2023-48414	In the Pixel Camera Driver, there is a possible use after free due to a logic error in the code. This could lead to local escalation of privilege with System execution privile
CVE-2023-36003	XAML Diagnostics Elevation of Privilege Vulnerability
CVE-2023-23372	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to inject n h5.0.1.2515 build 20230907 and later QuTS hero h4.5.4.2476 build 20230728 and later
CVE-2023-50495	NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _nc_wrap_entry().
CVE-2023-46218	This flaw allows a malicious HTTP server to set "super cookies" in curl that are then passed back to more origins than what is otherwise allowed or possible. This allow when the URL used a lower case hostname `curl.co.uk`, even though `co.uk` is listed as a PSL domain.
CVE-2023-41120	An issue was discovered in EnterpriseDB Postgres Advanced Server (EPAS) before 11.21.32, 12.x before 12.16.20, 13.x before 13.12.16, 14.x before 14.9.0, and 15.x
CVE-2023-6588	Offline mode is always enabled, even if permission disallows it, in Devolutions Server data source in Devolutions Workspace 2023.3.2.0 and earlier. This allows an atta
CVE-2023-46701	Mattermost fails to perform authorization checks in the /plugins/playbooks/api/v0/runs/add-to-timeline-dialog endpoint of the Playbooks plugin allowing an attacker to ge
CVE-2023-49795	MindsDB connects artificial intelligence models to real time data. Versions prior to 23.11.4.1 contain a server-side request forgery vulnerability in `file.py`. This can lead
CVE-2023-4421	The NSS code used for checking PKCS#1 v1.5 was leaking information useful in mounting Bleichenbacher-like attacks. Both the overall correctness of the padding as key exchange), or forge a signature using the victim's key. The issue was fixed by implementing the implicit rejection algorithm, in which the NSS returns a determinisi
CVE-2023-26920	fast-xml-parser before 4.1.2 allows __proto__ for Prototype Pollution.
CVE-2023-35636	Microsoft Outlook Information Disclosure Vulnerability

CVE Number	
CVE-2023-5907	The File Manager WordPress plugin before 6.3 does not restrict the file managers root directory, allowing an administrator to set a root outside of the WordPress root d
CVE-2023-47440	Gladys Assistant v4.27.0 and prior is vulnerable to Directory Traversal. The patch of CVE-2023-43256 was found to be incomplete, allowing authenticated attackers to
CVE-2023-28869	Support Assistant in NCP Secure Enterprise Client before 12.22 allows attackers read the contents of arbitrary files on the operating system by creating a symbolic link
CVE-2023-50463	The caddy-geo-ip (aka GeoIP) middleware through 0.6.0 for Caddy 2, when trust_header X-Forwarded-For is used, allows attackers to spoof their source IP address vi
CVE-2023-35642	Internet Connection Sharing (ICS) Denial of Service Vulnerability
CVE-2023-41114	An issue was discovered in EnterpriseDB Postgres Advanced Server (EPAS) before 11.21.32, 12.x before 12.16.20, 13.x before 13.12.16, 14.x before 14.9.0, and 15.x
CVE-2023-6566	Business Logic Errors in GitHub repository microweber/microweber prior to 2.0.
CVE-2023-41115	An issue was discovered in EnterpriseDB Postgres Advanced Server (EPAS) before 11.21.32, 12.x before 12.16.20, 13.x before 13.12.16, 14.x before 14.9.0, and 15.x
CVE-2023-36654	Directory traversal in the log-download REST API endpoint in ProLion CryptoSpike 3.0.15P2 allows remote authenticated attackers to download host server SSH privat
CVE-2023-28870	Insecure File Permissions in Support Assistant in NCP Secure Enterprise Client before 12.22 allow attackers to write to configuration files from low-privileged user acco
CVE-2023-6512	Inappropriate implementation in Web Browser UI in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to potentially spoof the contents of an iframe dialo
CVE-2023-48420	there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not
CVE-2022-48616	A Huawei data communication product has a command injection vulnerability. Successful exploitation of this vulnerability may allow attackers to gain higher privileges.
CVE-2023-50430	The Goodix Fingerprint Device, as shipped in Dell Inspiron 15 computers, does not follow the Secure Device Connection Protocol (SDCP) when enrolling via Linux, and
CVE-2021-27795	Brocade Fabric OS (FOS) hardware platforms running any version of Brocade Fabric OS software, which supports the license string format; contain cryptographic issue
CVE-2023-49587	SAP Solution Manager - version 720, allows an authorized attacker to execute certain deprecated function modules which can read or modify data of same or other cor
CVE-2023-6659	A vulnerability, which was classified as critical, has been found in Campcodes Web-Based Student Clearance System 1.0. This issue affects some unknown processing
CVE-2023-6671	A vulnerability has been discovered on OJS, that consists in a CSRF (Cross-Site Request Forgery) attack that forces an end user to execute unwanted actions on a we
CVE-2023-6574	A vulnerability was found in Byzoro Smart S20 up to 20231120 and classified as critical. Affected by this issue is some unknown functionality of the file /sysmanage/upd vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

CVE Number	
CVE-2023-6654	A vulnerability classified as critical was found in PHPEMS 6.x/7.x/8.x/9.0. Affected by this vulnerability is an unknown functionality in the library lib/session.cls.php of the
CVE-2023-42914	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.2, iOS 17.2 and iPadOS 17.2, watchOS 10.2, macOS Ventura 13.(
CVE-2023-6576	A vulnerability was found in Byzoro S210 up to 20231123. It has been declared as critical. This vulnerability affects unknown code of the file /Tool/uploadfile.php of the was contacted early about this disclosure but did not respond in any way.
CVE-2023-45866	Bluetooth HID Hosts in BlueZ may permit an unauthenticated Peripheral role HID Device to initiate and establish an encrypted connection, and accept HID keyboard re addressed this Bluetooth HID Hosts issue.
CVE-2023-6575	A vulnerability was found in Byzoro S210 up to 20231121. It has been classified as critical. This affects an unknown part of the file /Tool/repair.php of the component H contacted early about this disclosure but did not respond in any way.
CVE-2023-4932	SAS application is vulnerable to Reflected Cross-Site Scripting (XSS). Improper input validation in the `_program` parameter of the the `/SASStoredProcess/do` endpoi mentioned versions hot fixes were published.
CVE-2023-47722	IBM API Connect V10.0.5.3 and V10.0.6.0 stores user credentials in browser cache which can be read by a local user. IBM X-Force ID: 271912.
CVE-2023-28526	IBM Informix Dynamic Server 12.10 and 14.10 archecker is vulnerable to a heap buffer overflow, caused by improper bounds checking which could allow a local user to
CVE-2023-28527	IBM Informix Dynamic Server 12.10 and 14.10 cdr is vulnerable to a heap buffer overflow, caused by improper bounds checking which could allow a local user to cause
CVE-2023-46688	Open redirect vulnerability in Pleasanter 1.3.47.0 and earlier allows a remote unauthenticated attacker to redirect users to arbitrary web sites via a specially crafted URI
CVE-2023-46693	Cross Site Scripting (XSS) vulnerability in FormaLMS before 4.0.5 allows attackers to run arbitrary code via title parameters.
CVE-2023-6527	The Email Subscription Popup plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the HTTP_REFERER header in all versions up to, and including
CVE-2023-49488	A cross-site scripting (XSS) vulnerability in Openfiler ESA v2.99.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the nic p
CVE-2023-48928	Franklin Fueling Systems System Sentinel AnyWare (SSA) version 1.6.24.492 is vulnerable to Open Redirect. The 'path' parameter of the prefs.asp resource allows an
CVE-2023-49490	XunRuiCMS v4.5.5 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the component /admin.php.
CVE-2023-5750	The EmbedPress WordPress plugin before 3.9.2 does not sanitise and escape a parameter before outputting it back in the page containing a specific content, leading t
CVE-2023-5749	The EmbedPress WordPress plugin before 3.9.2 does not sanitise and escape user input before outputting it back in the page, leading to a Reflected Cross-Site Scripti
CVE-2023-49494	DedeCMS v5.7.111 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the component select_media_post_wangEditor.php.
CVE-2023-4958	In Red Hat Advanced Cluster Security (RHACS), it was found that some security related HTTP headers were missing, allowing an attacker to exploit this with a clickjac

CVE Number	
CVE-2023-41170	NetScout nGeniusONE 6.3.4 build 2298 allows a Reflected Cross-Site scripting vulnerability.
CVE-2023-49493	DedeCMS v5.7.111 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the v parameter at selectimages.php.
CVE-2023-49492	DedeCMS v5.7.111 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the imgstick parameter at selectimages.php.
CVE-2023-49577	The SAP HCM (SMART PAYE solution) - versions S4HCMCIE 100, SAP_HRCIE 600, SAP_HRCIE 604, SAP_HRCIE 608, does not sufficiently encode user-controllec
CVE-2023-41337	h2o is an HTTP server with support for HTTP/1.x, HTTP/2 and HTTP/3. In version 2.3.0-beta2 and prior, when h2o is configured to listen to multiple addresses or ports of that HTTPS request being sent. The attack involves a victim client trying to resume a TLS connection and an attacker redirecting the packets to a different address o server address, port, or the X.509 certificate, and therefore it is possible for an attacker to force the victim connection to wrongfully resume against a different server ad forwarded to the attacker's server. An H2O instance is vulnerable to this attack only if the instance is configured to listen to different addresses or ports using the listen level ones.
CVE-2023-28604	The fluid_components (aka Fluid Components) extension before 3.5.0 for TYPO3 allows XSS via a component argument parameter, for certain {content} use cases tha
CVE-2023-48206	A Cross Site Scripting (XSS) vulnerability in GaatiTrack Courier Management System 1.0 allows a remote attacker to inject JavaScript via the page parameter to login.p
CVE-2023-43103	An XSS issue was discovered in a web endpoint in Zimbra Collaboration (ZCS) before 10.0.4 via an unsanitized parameter. This is also fixed in 8.8.15 Patch 43 and 9.(
CVE-2023-48208	A Cross Site Scripting vulnerability in Availability Booking Calendar 5.0 allows an attacker to inject JavaScript via the name, plugin_sms_api_key, plugin_sms_country_
CVE-2022-48614	Special:Ask in Semantic MediaWiki before 4.0.2 allows Reflected XSS.
CVE-2023-43102	An issue was discovered in Zimbra Collaboration (ZCS) before 10.0.4. An XSS issue can be exploited to access the mailbox of an authenticated user. This is also fixed
CVE-2023-42479	An unauthenticated attacker can embed a hidden access to a Biller Direct URL in a frame which, when loaded by the user, will submit a cross-site scripting request to tl
CVE-2023-6568	A reflected Cross-Site Scripting (XSS) vulnerability exists in the mlflow/mlflow repository, specifically within the handling of the Content-Type header in POST requests. mlflow/server/auth/__init__.py file, where the user-supplied Content-Type header is directly injected into a Python formatted string and returned to the user, facilitating t
CVE-2023-49563	Cross Site Scripting (XSS) in Voltronic Power SNMP Web Pro v.1.1 allows an attacker to execute arbitrary code via a crafted script within a request to the webserver.
CVE-2023-28874	The next parameter in the /accounts/login endpoint of Seafile 9.0.6 allows attackers to redirect users to arbitrary sites.
CVE-2023-49225	A cross-site-scripting vulnerability exists in Ruckus Access Point products (ZoneDirector, SmartZone, and AP Solo). If this vulnerability is exploited, an arbitrary script m
CVE-2023-46499	Cross Site Scripting vulnerability in EverShop NPM versions before v.1.0.0-rc.5 allows a remote attacker to obtain sensitive information via a crafted scripts to the Admi
CVE-2023-46495	Cross Site Scripting vulnerability in EverShop NPM versions before v.1.0.0-rc.8 allows a remote attacker to obtain sensitive information via a crafted request to the sortl
CVE-2023-46494	Cross Site Scripting vulnerability in EverShop NPM versions before v.1.0.0-rc.5 allows a remote attacker to obtain sensitive information via a crafted request to the Proc

CVE Number	
CVE-2023-6507	An issue was found in CPython 3.12.0 `subprocess` module on POSIX platforms. The issue was fixed in CPython 3.12.1 and does not affect other stable releases. Wh isn't used or when any value is used besides an empty list. This issue only impacts CPython processes run with sufficient privilege to make the `setgroups` system call
CVE-2023-2861	A flaw was found in the 9p passthrough filesystem (9pfs) implementation in QEMU. The 9pfs server did not prohibit opening special files on the host side, potentially all
CVE-2023-49805	Uptime Kuma is an easy-to-use self-hosted monitoring tool. Prior to version 1.23.9, the application uses WebSocket (with Socket.io), but it does not verify that the sour communicate with it. Other websites still need to authenticate to access most features, however this can be used to circumvent firewall protections made in place by pe the application. However, such a connection may allow attacker to further exploit unseen vulnerabilities of the application. Users with "No-auth" mode configured who a handler. By default, if the `Origin` header is present, it would be checked against the Host header. Connection would be denied if the hostnames do not match, which w
CVE-2023-24547	On affected platforms running Arista MOS, the configuration of a BGP password will cause the password to be logged in clear text that can be revealed in local logs or
CVE-2020-25835	A potential vulnerability has been identified in Micro Focus ArcSight Management Center. The vulnerability could be remotely exploited resulting in stored Cross-Site Sc
CVE-2023-26154	Versions of the package pubnub before 7.4.0; all versions of the package com.pubnub:pubnub; versions of the package pubnub before 6.19.0; all versions of the packa versions of the package pubnub/c-core before 4.5.0; versions of the package com.pubnub:pubnub-kotlin before 7.7.0; versions of the package pubnub/swift before 6.2. hex encoding and trimming are applied, leaving half of the bits in the key always the same for every encoded message or file. **Note:** In order to exploit this vulnerabi
CVE-2023-49798	OpenZeppelin Contracts is a library for smart contract development. A merge issue when porting the 5.0.1 patch to the 4.9 branch caused a line duplication. In the vers version 4.9.5. The 4.9.4 version is marked as deprecated. Users are advised to upgrade. There are no known workarounds for this issue.
CVE-2023-50454	An issue was discovered in Zammad before 6.2.0. In several subsystems, SSL/TLS was used to establish connections to external services without proper validation of
CVE-2023-6146	A Qualys web application was found to have a stored XSS vulnerability resulting from the absence of HTML encoding in the presentation of logging information to users
CVE-2023-48399	In ProtocolMiscATCommandAdapter::Init() of protocolmiscadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local in
CVE-2023-6608	A vulnerability was found in Tongda OA 2017 up to 11.9 and classified as critical. Affected by this issue is some unknown functionality of the file general/notify/manage/ vulnerability is VDB-247244. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-34320	Cortex-A77 cores (r0p0 and r1p0) are affected by erratum 1508412 where software, under certain circumstances, could deadlock a core due to the execution of either a
CVE-2023-42919	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.2, iOS 17.2 and iPadOS 17.2, watchOS 1(
CVE-2023-42922	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma 14.2, iOS 17.2 and iPadOS 17.2, macOS Ventura 13.
CVE-2023-42924	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.2, macOS Ventura 13.6.3. An app may be able to access sensitive user d
CVE-2023-6622	A null pointer dereference vulnerability was found in nft_dynset_init() in net/netfilter/nft_dynset.c in nf_tables in the Linux kernel. This issue may allow a local attacker w
CVE-2023-6619	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality
CVE-2023-42932	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.2, macOS Ventura 13.6.3, macOS Monterey 12.7.2. An app may be able t
CVE-2023-6618	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown t

CVE Number	
CVE-2023-6617	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0. It has been classified as critical. Affected is an unknown function of the file attend
CVE-2023-48958	gpac 2.3-DEV-rev617-g671976fcc-master contains memory leaks in gf_mpd_resolve_url media_tools/mpd.c:4589.
CVE-2023-6581	A vulnerability has been found in D-Link DAR-7000 up to 20231126 and classified as critical. This vulnerability affects unknown code of the file /user/inc/workidajax.php
CVE-2023-49994	Espeak-ng 1.52-dev was discovered to contain a Floating Point Exception via the function PeaksToHarmspect at wavegen.c.
CVE-2023-6607	A vulnerability has been found in Tongda OA 2017 up to 11.10 and classified as critical. Affected by this vulnerability is an unknown functionality of the file general/wiki/ did not respond in any way.
CVE-2023-6612	A vulnerability was found in Totolink X5000R 9.1.0cu.2300_B20230112. It has been rated as critical. This issue affects the function setDdnsCfg/setDynamicRoute/setFirewallType/setIPSecCfg/setIpPortFilterRules/setLancfg/setLoginPasswordCfg/setMacFilterRules/setMtknatCfg/setNetworkConfig/s of the file /cgi-bin/cstecgi.cgi. The manipulation leads to os command injection. The exploit has been disclosed to the public and may be used. The associated identifier
CVE-2023-48422	In Init of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additiona
CVE-2023-48415	In Init of protocolembmsadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no addit
CVE-2023-48412	In private_handle_t of mali_gralloc_buffer.h, there is a possible information leak due to a logic error in the code. This could lead to local information disclosure with no a
CVE-2023-48411	In SignalStrengthAdapter::FillGsmSignalStrength() of protocolmiscadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead t
CVE-2023-48408	In ProtocolNetSimFileInfoAdapter() of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local informatio
CVE-2023-48401	In GetSizeOfEenlRecords of protocoladapter.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosu
CVE-2023-6560	An out-of-bounds memory access flaw was found in the io_uring SQ/CQ rings functionality in the Linux kernel. This issue could allow a local user to crash the system.
CVE-2023-47465	An issue in GPAC v.2.2.1 and before allows a local attacker to cause a denial of service (DoS) via the ctts_box_read function of file src/isomedia/box_code_base.c.
CVE-2023-6611	A vulnerability was found in Tongda OA 2017 up to 11.9. It has been declared as critical. This vulnerability affects unknown code of the file pda/pad/email/delete.php. T vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-42898	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.2, watchOS 10.2, iOS 17.2 and iPadOS 17.2, tvOS 17.2. Processi
CVE-2023-6657	A vulnerability classified as critical has been found in SourceCodester Simple Student Attendance System 1.0. This affects an unknown part of the file /modals/student_
CVE-2023-42883	The issue was addressed with improved memory handling. This issue is fixed in Safari 17.2, macOS Sonoma 14.2, iOS 17.2 and iPadOS 17.2, watchOS 10.2, tvOS 17
CVE-2023-42884	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma 14.2, iOS 17.2 and iPadOS 17.2, macOS Ventura 13.

CVE Number	
CVE-2015-2179	The xaviershay-dm-rails gem 0.10.3.8 for Ruby allows local users to discover MySQL credentials by listing a process and its arguments.
CVE-2023-42891	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.2, macOS Ventura 13.6.3, macOS Monterey 12.7.2
CVE-2023-42894	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma 14.2, macOS Ventura 13.6.3, macOS Monterey 12.7.
CVE-2023-6658	A vulnerability classified as critical was found in SourceCodester Simple Student Attendance System 1.0. This vulnerability affects unknown code of the file ajax-api.php
CVE-2023-40238	A LogoFAIL issue was discovered in BmpDecoderDxe in Insyde InsydeH2O with kernel 5.2 before 05.28.47, 5.3 before 05.37.47, 5.4 before 05.45.47, 5.5 before 05.53 compression.
CVE-2023-35635	Windows Kernel Denial of Service Vulnerability
CVE-2023-42900	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.2. An app may be able to access user-sensitive data.
CVE-2023-49248	Vulnerability of unauthorized file access in the Settings app. Successful exploitation of this vulnerability may cause unauthorized file access.
CVE-2023-6679	A null pointer dereference vulnerability was found in dpll_pin_parent_pin_set() in drivers/dpll/dpll_netlink.c in the Digital Phase Locked Loop (DPLL) subsystem in the Li
CVE-2023-50431	sec_attest_info in drivers/accel/habanalabs/common/habanalabs_ioctl.c in the Linux kernel through 6.6.5 allows an information leak to user space because info->pad0
CVE-2023-36009	Microsoft Word Information Disclosure Vulnerability
CVE-2023-49487	JFinalCMS v5.0.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the navigation management department.
CVE-2023-46857	Squidex before 7.9.0 allows XSS via an SVG document to the Upload Assets feature. This occurs because there is an incomplete blacklist in the SVG inspection, allow
CVE-2023-49485	JFinalCMS v5.0.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the column management department.
CVE-2023-49484	Dreamer CMS v4.1.3 was discovered to contain a cross-site scripting (XSS) vulnerability in the article management department.
CVE-2023-34439	Pleasanter 1.3.47.0 and earlier contains a stored cross-site scripting vulnerability. If this vulnerability is exploited, an arbitrary script may be executed on the user's web
CVE-2023-48940	A stored cross-site scripting (XSS) vulnerability in /admin.php of DaiCuo v2.5.15 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.
CVE-2023-28017	HCL Connections is vulnerable to a cross-site scripting attack where an attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspec
CVE-2023-49444	An arbitrary file upload vulnerability in DoraCMS v2.1.8 allow attackers to execute arbitrary code via uploading a crafted HTML or image file to the user avatar.

CVE Number	
CVE-2023-48837	Car Rental Script 3.0 is vulnerable to Multiple HTML Injection issues via SMS API Key or Default Country Code.
CVE-2023-48172	A Cross Site Scripting (XSS) vulnerability in Shuttle Booking Software 2.0 allows a remote attacker to inject JavaScript via the name, description, title, or address paran
CVE-2023-48824	BoidCMS 2.0.1 is vulnerable to Multiple Stored Cross-Site Scripting (XSS) issues via the title, subtitle, footer, or keywords parameter in a page=create action.
CVE-2023-41905	NETSCOUT nGeniusONE 6.3.4 build 2298 allows a Reflected Cross-Site scripting (XSS) vulnerability by an authenticated user.
CVE-2023-48825	Availability Booking Calendar 5.0 is vulnerable to Multiple HTML Injection issues via SMS API Key or Default Country Code.
CVE-2023-48838	Appointment Scheduler 3.0 is vulnerable to Multiple HTML Injection issues via the SMS API Key or Default Country Code.
CVE-2023-48827	Time Slots Booking Calendar 4.0 is vulnerable to Multiple HTML Injection issues via the name, plugin_sms_api_key, plugin_sms_country_code, calendar_id, title, coun
CVE-2023-41171	NetScout nGeniusONE 6.3.4 build 2298 allows a Stored Cross-Site scripting vulnerability (issue 3 of 4).
CVE-2023-48828	Time Slots Booking Calendar 4.0 is vulnerable to Multiple Stored Cross-Site Scripting (XSS) issues via the name, plugin_sms_api_key, plugin_sms_country_code, cale
CVE-2023-41169	NetScout nGeniusONE 6.3.4 build 2298 allows a Stored Cross-Site scripting vulnerability (issue 2 of 4).
CVE-2023-41168	NetScout nGeniusONE 6.3.4 build 2298 allows a Stored Cross-Site scripting vulnerability (issue 1 of 4).
CVE-2023-48836	Car Rental Script 3.0 is vulnerable to Multiple Stored Cross-Site Scripting (XSS) issues via the name, plugin_sms_api_key, plugin_sms_country_code, calendar_id, title
CVE-2023-48642	Archer Platform 6.x before 6.13 P2 (6.13.0.2) contains an authenticated HTML content injection vulnerability. A remote authenticated malicious Archer user could poten
CVE-2023-6710	A flaw was found in the mod_proxy_cluster in the Apache server. This issue may allow a malicious user to add a script in the 'alias' parameter in the URL to trigger the
CVE-2023-46974	Cross Site Scripting vulnerability in Best Courier Management System v.1.000 allows a remote attacker to execute arbitrary code via a crafted payload to the page para
CVE-2023-48839	Appointment Scheduler 3.0 is vulnerable to Multiple Stored Cross-Site Scripting (XSS) issues via the name, plugin_sms_api_key, plugin_sms_country_code, calendar_
CVE-2023-41172	NetScout nGeniusONE 6.3.4 build 2298 allows a Stored Cross-Site scripting vulnerability (issue 4 of 4).
CVE-2023-49486	JFinalCMS v5.0.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the model management department.
CVE-2023-46497	Directory Traversal vulnerability in EverShop NPM versions before v.1.0.0-rc.8 allows a remote attacker to obtain sensitive information via a crafted request to the mkdi

CVE Number	
CVE-2023-48715	Tuleap is an open source suite to improve management of software developments and collaboration. Prior to version 15.2.99.103 of Tuleap Community Edition and pric code. Tuleap Community Edition 15.2.99.103, Tuleap Enterprise Edition 15.2-4, and Tuleap Enterprise Edition 15.1-8 contain a fix for this issue.
CVE-2023-50465	A stored cross-site scripting (XSS) vulnerability exists in Monica (aka MonicaHQ) 4.0.0 via an SVG document uploaded by an authenticated user.
CVE-2023-5756	The Digital Publications by Supsystic plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.6. This is due to missing or
CVE-2023-28875	A Stored XSS issue in shared files download terms in Filerun Update 20220202 allows attackers to inject JavaScript code that is executed when a user follows the craf
CVE-2023-49273	Umbraco is an ASP.NET content management system (CMS). Starting in version 8.0.0 and prior to versions 8.18.10, 10.8.1, and 12.3.4, users with low privileges (Edit
CVE-2023-28873	An XSS issue in wiki and discussion pages in Seafile 9.0.6 allows attackers to inject JavaScript into the Markdown editor.
CVE-2023-6193	quiche v. 0.15.0 through 0.19.0 was discovered to be vulnerable to unbounded queuing of path validation messages, which could lead to excessive resource consumpt connection (e.g. by restricting the peer's congestion window size) so that PATH_RESPONSE frames can only be sent at the slower rate than they are received; leading
CVE-2023-48205	Jorani Leave Management System 1.0.2 allows a remote attacker to spoof a Host header associated with password reset emails.
CVE-2023-35909	Uncontrolled Resource Consumption vulnerability in Saturday Drive Ninja Forms Contact Form – The Drag and Drop Form Builder for WordPress leading to DoS.This is
CVE-2023-49990	Espeak-ng 1.52-dev was discovered to contain a buffer-overflow via the function SetUpPhonemeTable at synthdata.c.
CVE-2023-49991	Espeak-ng 1.52-dev was discovered to contain a Stack Buffer Underflow via the function CountVowelPosition at synthdata.c.
CVE-2023-49992	Espeak-ng 1.52-dev was discovered to contain a Stack Buffer Overflow via the function RemoveEnding at dictionary.c.
CVE-2023-49993	Espeak-ng 1.52-dev was discovered to contain a Buffer Overflow via the function ReadClause at readclause.c.
CVE-2023-50428	In Bitcoin Core through 26.0 and Bitcoin Knots before 25.1.knots20231115, datacarrier size limits can be bypassed by obfuscating data as code (e.g., with OP_FALSE
CVE-2023-43299	An issue in DA BUTCHERS mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.
CVE-2022-44543	The femanager extension before 5.5.2, 6.x before 6.3.3, and 7.x before 7.0.1 for TYPO3 allows creation of frontend users in restricted groups (if there is a usergroup fie
CVE-2023-43298	An issue in SCOL Members Card mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.
CVE-2023-50453	An issue was discovered in Zammad before 6.2.0. It uses the public endpoint /api/v1/signshow for its login screen. This endpoint returns internal configuration data of u
CVE-2023-31048	The OPC UA .NET Standard Reference Server before 1.4.371.86. places sensitive information into an error message that may be seen remotely.

CVE Number	
CVE-2023-50456	An issue was discovered in Zammad before 6.2.0. An attacker can trigger phishing links in generated notification emails via a crafted first or last name.
CVE-2023-35619	Microsoft Outlook for Mac Spoofing Vulnerability
CVE-2023-6393	A flaw was found in the Quarkus Cache Runtime. When request processing utilizes a Uni cached using @CacheResult and the cached Uni reuses the initial "completio access to sensitive data.
CVE-2023-39326	A malicious HTTP sender can use chunk extensions to cause a receiver reading from a request or response body to read many more bytes from the network than are i metadata in a request or response body sent using the chunked encoding. The net/http chunked encoding reader discards this metadata. A sender can exploit this by i
CVE-2023-6459	Mattermost is grouping calls in the /metrics endpoint by id and reports that id in the response. Since this id is the channelID, the public /metrics endpoint is revealing ch
CVE-2023-6273	Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally
CVE-2023-41268	Improper input validation vulnerability in Samsung Open Source Escargot allows stack overflow and segmentation fault. This issue affects Escargot: from 3.0.0 through
CVE-2023-36012	DHCP Server Service Information Disclosure Vulnerability
CVE-2023-45292	When using the default implementation of Verify to check a Captcha, verification can be bypassed. For example, if the first parameter is a non-existent id, the second p
CVE-2023-50251	php-svg-lib is an SVG file parsing / rendering library. Prior to version 0.5.1, when parsing the attributes passed to a `use` tag inside an svg document, an attacker can c potentially cause resource exhaustion to the point that the system is unable to handle incoming request. Version 0.5.1 contains a patch for this issue.
CVE-2023-46493	Directory Traversal vulnerability in EverShop NPM versions before v.1.0.0-rc.8 allows a remote attacker to obtain sensitive information via a crafted request to the readl
CVE-2023-42923	This issue was addressed through improved state management. This issue is fixed in iOS 17.2 and iPadOS 17.2. Private Browsing tabs may be accessed without auth
CVE-2023-46219	When saving HSTS data to an excessively long file name, curl could end up removing all contents, making subsequent requests using that file unaware of the HSTS st
CVE-2023-49796	MindsDB connects artificial intelligence models to real time data. Versions prior to 23.11.4.1 contain a limited file write vulnerability in `file.py` Users should use MindsD
CVE-2023-46871	GPAC version 2.3-DEV-rev602-ged8424300-master in MP4Box contains a memory leak in NewSFDouble scenegraph/vrml_tools.c:300. This vulnerability may lead to a
CVE-2023-49278	Umbraco is an ASP.NET content management system (CMS). Starting in version 8.0.0 and prior to versions 8.18.10, 10.8.1, and 12.3.4, a brute force exploit can be us
CVE-2023-40053	A vulnerability has been identified within Serv-U 15.4 that allows an authenticated actor to insert content on the file share function feature of Serv-U, which could be use
CVE-2023-6656	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in DeepFaceLab pretrained DF.wf.288res.384.92.72.22. It has been rated as critical. Affected by th NOTE: This vulnerability only affects products that are no longer supported by the maintainer.
CVE-2023-5536	A feature in LXD (LP#1829071), affects the default configuration of Ubuntu Server which allows privileged users in the lxd group to escalate their privilege to root withou

CVE Number	
CVE-2023-48397	In Init of protocolcalladapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with System e
CVE-2023-48413	In Init of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with System e
CVE-2023-49746	Server-Side Request Forgery (SSRF) vulnerability in Softaculous Team SpeedyCache – Cache, Optimization, Performance.This issue affects SpeedyCache – Cache,
CVE-2023-46641	Server-Side Request Forgery (SSRF) vulnerability in Code for Recovery 12 Step Meeting List.This issue affects 12 Step Meeting List: from n/a through 3.14.24.
CVE-2023-32975	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow build 20230927 and later
CVE-2023-5757	The WP Crowdfunding WordPress plugin before 2.1.8 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perfor
CVE-2023-5940	The WP Not Login Hide (WPNLH) WordPress plugin through 1.0 does not sanitise and escape some of its settings, which could allow high privilege users such as adm
CVE-2023-36880	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
CVE-2023-5955	The Contact Form Email WordPress plugin before 1.3.44 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to pe
CVE-2022-48615	An improper access control vulnerability exists in a Huawei datacom product. Attackers can exploit this vulnerability to obtain partial device information.
CVE-2023-35625	Azure Machine Learning Compute Instance for SDK Users Information Disclosure Vulnerability
CVE-2023-47548	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in SoftLab Integrate Google Drive – Browse, Upload, Download, Embed, Play, Share, Gallery, and Ma
CVE-2023-47779	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks. Integration for Constant Contact and Contact Form 7, WPForms, Elementor, Ninja Forr
CVE-2023-48325	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in PluginOps Landing Page Builder – Lead Page – Optin Page – Squeeze Page – WordPress Landing
CVE-2023-45762	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Michael Uno (miunosoft) Responsive Column Widgets.This issue affects Responsive Column Widge
CVE-2023-42897	The issue was addressed with improved checks. This issue is fixed in iOS 17.2 and iPadOS 17.2. An attacker with physical access may be able to use Siri to access se
CVE-2023-34064	Workspace ONE Launcher contains a Privilege Escalation Vulnerability. A malicious actor with physical access to Workspace ONE Launcher could utilize the Edge Par
CVE-2023-32968	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow build 20230927 and later
CVE-2023-49584	SAP Fiori launchpad - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, UI_700 200, SAP_BASIS 793, allows an attacker to u

CVE Number	
CVE-2023-46916	Maxima Max Pro Power 1.0 486A devices allow BLE traffic replay. An attacker can use GATT characteristic handle 0x0012 to perform potentially disruptive actions suc
CVE-2023-28876	A Broken Access Control issue in comments to uploaded files in Filerun through Update 20220202 allows attackers to delete comments on files uploaded by other user
CVE-2023-28871	Support Assistant in NCP Secure Enterprise Client before 12.22 allows attackers to read registry information of the operating system by creating a symbolic link.
CVE-2023-6511	Inappropriate implementation in Autofill in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to bypass Autofill restrictions via a crafted HTML page. (Ch
CVE-2023-48313	Umbraco is an ASP.NET content management system (CMS). Starting in 10.0.0 and prior to versions 10.8.1 and 12.3.4, Umbraco contains a cross-site scripting (XSS)
CVE-2023-45847	Mattermost fails to to check the length when setting the title in a run checklist in Playbooks, allowing an attacker to send a specially crafted request and crash the Playb
CVE-2023-6649	A vulnerability has been found in PHPGurukul Teacher Subject Allocation Management System 1.0 and classified as problematic. This vulnerability affects unknown co vulnerability.
CVE-2023-45210	Pleasanter 1.3.47.0 and earlier contains an improper access control vulnerability, which may allow a remote authenticated attacker to view the temporary files uploaded
CVE-2023-6650	A vulnerability was found in SourceCodester Simple Invoice Generator System 1.0 and classified as problematic. This issue affects some unknown processing of the fil
CVE-2023-6653	A vulnerability was found in PHPGurukul Teacher Subject Allocation Management System 1.0. It has been rated as problematic. Affected by this issue is some unknow identifier assigned to this vulnerability.
CVE-2023-41116	An issue was discovered in EnterpriseDB Postgres Advanced Server (EPAS) before 11.21.32, 12.x before 12.16.20, 13.x before 13.12.16, 14.x before 14.9.0, and 15.x
CVE-2023-49607	Mattermost fails to validate the type of the "reminder" body request parameter allowing an attacker to crash the Playbook Plugin when updating the status dialog.
CVE-2023-5868	A memory disclosure vulnerability was found in PostgreSQL that allows remote users to access sensitive information by exploiting certain aggregate function calls with some portion of system memory.
CVE-2023-49809	Mattermost fails to handle a null request body in the /add endpoint, allowing a simple member to send a request with null request body to that endpoint and make it cras
CVE-2023-5710	The System Dashboard plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the sd_constants() function hooked via
CVE-2023-5711	The System Dashboard plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the sd_php_info() function hooked via a
CVE-2023-5712	The System Dashboard plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the sd_global_value() function hooked v
CVE-2023-38174	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability
CVE-2023-5713	The System Dashboard plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the sd_option_value() function hooked v

CVE Number	
CVE-2023-5714	The System Dashboard plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the sd_db_specs() function hooked via
CVE-2023-36652	A SQL Injection in the users searching REST API endpoint in ProLion CryptoSpike 3.0.15P2 allows remote authenticated attackers to read database data via SQL com
CVE-2023-49874	Mattermost fails to check whether a user is a guest when updating the tasks of a private playbook run allowing a guest to update the tasks of a private playbook run if th
CVE-2023-6577	A vulnerability was found in Byzoro PatrolFlow 2530Pro up to 20231126. It has been rated as problematic. This issue affects some unknown processing of the file /log/r NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-50457	An issue was discovered in Zammad before 6.2.0. When listing tickets linked to a knowledge base answer, or knowledge base answers of a ticket, a user could see ent
CVE-2023-6599	Missing Standardized Error Handling Mechanism in GitHub repository microweber/microweber prior to 2.0.
CVE-2023-48227	Umbraco is an ASP.NET content management system (CMS). Starting in version 8.0.0 and prior to versions 8.18.10, 10.7.0, and 12.3.0, Backoffice users with send for
CVE-2023-41113	An issue was discovered in EnterpriseDB Postgres Advanced Server (EPAS) before 11.21.32, 12.x before 12.16.20, 13.x before 13.12.16, 14.x before 14.9.0, and 15.x configured one or more directories for filesystem access via CREATE DIRECTORY and adopted certain non-default settings for log_line_prefix and log_connections.
CVE-2022-46141	A vulnerability has been identified in SIMATIC STEP 7 (TIA Portal) (All versions < V19). An information disclosure vulnerability could allow a local attacker to gain acces
CVE-2023-6120	The Welcart e-Commerce plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.9.6 via the upload_certificate_file function. Thi
CVE-2023-20275	A vulnerability in the AnyConnect SSL VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could al tunnel. A successful exploit could allow the attacker to send a packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return p
CVE-2023-49581	SAP GUI for Windows and SAP GUI for Java allow an unauthenticated attacker to access information which would otherwise be restricted and confidential. In addition,
CVE-2023-50247	h2o is an HTTP server with support for HTTP/1.x, HTTP/2 and HTTP/3. The QUIC stack (quicly), as used by H2O up to commit 43f86e5 (in version 2.3.0-beta and prior resolved in commit d67e81d03be12a9d53dc8271af6530f40164cd35. HTTP/1 and HTTP/2 are not affected by this vulnerability as they do not use QUIC. Administrators
CVE-2023-49279	Umbraco is an ASP.NET content management system (CMS). Starting in version 7.0.0 and prior to versions 7.15.11, 8.18.9, 10.7.0, 11.5.0, and 12.2.0, a user with acc Implement the server side file validation or serve all media from an different host (e.g cdn) than where Umbraco is hosted.
CVE-2023-49274	Umbraco is an ASP.NET content management system (CMS). Starting in version 8.0.0 and prior to versions 8.18.10, 10.8.1, and 12.3.4, a user enumeration attack is p
CVE-2023-50263	Nautobot is a Network Source of Truth and Network Automation Platform built as a web application atop the Django Python framework with a PostgreSQL or MySQL da ephemeral and are deleted once the Job in question runs. In the default implementation used in Nautobot, as provided by `django-db-file-storage`, these URLs do not b unauthenticated user would have to guess names to discover arbitrary files for download, but if a user knows the file name/path value, they can access it without auther
CVE-2023-6547	Mattermost fails to validate team membership when a user attempts to access a playbook, allowing a user with permissions to a playbook but no permissions to the tea
CVE-2023-38694	Umbraco is an ASP.NET content management system (CMS). Starting in version 8.0.0 and prior to versions 8.18.10, 10.7.0, and 12.1.0, a user with access to a specifi
CVE-2023-6609	A vulnerability was found in osCommerce 4. It has been classified as problematic. This affects an unknown part of the file /b2b-supermarket/catalog/all-products. The m VDB-247245 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

CVE Number	
CVE-2023-49578	SAP Cloud Connector - version 2.0, allows an authenticated user with low privilege to perform Denial of service attack from adjacent UI by sending a malicious request
CVE-2023-6616	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0 and classified as problematic. This issue affects some unknown processing of the
CVE-2023-6615	A vulnerability, which was classified as problematic, has been found in Typecho 1.2.1. Affected by this issue is some unknown functionality of the file /admin/manage-u any way.
CVE-2023-49058	SAP Master Data Governance File Upload application allows an attacker to exploit insufficient validation of path information provided by users, thus characters represe
CVE-2023-6646	A vulnerability classified as problematic has been found in linkding 1.23.0. Affected is an unknown function. The manipulation of the argument q leads to cross site scrip NOTE: The vendor was contacted early, responded in a very professional manner and immediately released a fixed version of the affected product.
CVE-2023-6727	Mattermost fails to perform correct authorization checks when creating a playbook action, allowing users without access to the playbook to create playbook actions. If th
CVE-2023-6194	In Eclipse Memory Analyzer versions 0.7 to 1.14.0, report definition XML files are not filtered to prohibit document type definition (DTD) references to external entities. T
CVE-2023-48429	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 2). The Web UI of affected devices does not check the length of parameters in certair
CVE-2023-48430	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 2). The REST API of affected devices does not check the length of parameters in cert
CVE-2023-6614	A vulnerability classified as problematic was found in Typecho 1.2.1. Affected by this vulnerability is an unknown functionality of the file /admin/manage-pages.php of th disclosure but did not respond in any way.
CVE-2023-42874	This issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.2. Secure text fields may be displayed via the Accessibility Keyb
CVE-2023-6613	A vulnerability classified as problematic has been found in Typecho 1.2.1. Affected is an unknown function of the file /admin/options-theme.php of the component Logo respond in any way.
CVE-2023-5870	A flaw was found in PostgreSQL involving the pg_cancel_backend role that signals background workers, including the logical replication launcher, autovacuum workers
CVE-2023-42927	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2023-6061	Rejected reason: This CVE ID has been rejected/withdrawn by its CVE Numbering Authority (Palo Alto Networks) based on discussions with Mitsubishi Electronics Cor
CVE-2023-49787	Rejected reason: CVE request originates from private repository
CVE-2023-39170	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it's a duplicate of CVE-2023-39169.
CVE-2023-39168	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it's a duplicate of CVE-2023-39167.