SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 09 August 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-2023-3572	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote, unauthenticated attacker may use an attribute of a specific HTTP POST request releated to date/time operations to gain full access to the device.	10.0	More Details
CVE-2023-39344	social-media-skeleton is an uncompleted social media project. A SQL injection vulnerability in the project allows UNION based injections, which indirectly leads to remote code execution. Commit 3cabdd35c3d874608883c9eaf9bf69b2014d25c1 contains a fix for this issue.	10.0	More Details
CVE-2023-37470	Metabase is an open-source business intelligence and analytics platform. Prior to versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4, a vulnerability could potentially allow remote code execution on one's Metabase server. The core issue is that one of the supported data warehouses (an embedded in-memory database H2), exposes a number of ways for a connection string to include code that is then executed by the process running the embedded database. Because Metabase allows users to connect to databases, this means that a user supplied string can be used to inject executable code. Metabase allows users to validate their connection string before adding a database (including on setup), and this validation API was the primary vector used as it can be called without validation. Versions 0.43.7.3, 0.44.7.3, 0.45.4.3, 0.46.6.4, 1.43.7.3, 1.44.7.3, 1.45.4.3, and 1.46.6.4 fix this issue by removing the ability of users to add H2 databases entirely. As a workaround, it is possible to block these vulnerabilities at the network level by blocking the endpoints `POST /api/database`, `PUT /api/database/:id`, and `POST /api/setup/validateuntil`. Those who use H2 as a file-based database should migrate to SQLite.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38702	Knowage is an open source analytics and business intelligence suite. Starting in the 6.x.x branch and prior to version 8.1.8, the endpoint `/knowage/restful-services/dossier/importTemplateFile` allows authenticated users to upload `template file` on the server, but does not need any authorization to be reached. When the JSP file is uploaded, the attacker just needs to connect to `/knowageqbeengine/foo.jsp` to gain code execution on the server. By exploiting this vulnerability, an attacker with low privileges can upload a JSP file to the `knowageqbeengine` directory and gain code execution capability on the server. This issue has been patched in Knowage version 8.1.8.	9.9	More Details
CVE-2023-1437	All versions prior to 9.1.4 of Advantech WebAccess/SCADA are vulnerable to use of untrusted pointers. The RPC arguments the client sent could contain raw memory pointers for the server to use as-is. This could allow an attacker to gain access to the remote file system and the ability to execute commands and overwrite files.	9.8	More Details
CVE-2023-38933	Tenda AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6 and AC9 V3.0 V15.03.06.42_multi, and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function.	9.8	More Details
CVE-2023-38939	Tenda F1202 V1.2.0.9 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the mit_ssid parameter in the formWrlsafeset function.	9.8	More Details
CVE-2023-38938	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter at /L7lm.	9.8	More Details
CVE-2023-38937	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, AC9 V3.0 V15.03.06.42_multi and AC10 v4.0 V16.03.10.13 were discovered to contain a stack overflow via the list parameter in the formSetVirtualSer function.	9.8	More Details
CVE-2023-38936	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, AC5 V1.0 V15.03.06.28, FH1203 V2.0.1.6, AC9 V3.0 V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function.	9.8	More Details
CVE-2023-38935	Tenda AC1206 V15.03.06.23, AC8 V4 V16.03.34.06, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and AC9 V3.0 V15.03.06.42_multi were discovered to contain a tack overflow via the list parameter in the formSetQosBand function.	9.8	More Details
CVE-2023-38934	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) was discovered to contain a stack overflow via the deviceId parameter in the formSetDeviceName function.	9.8	More Details
CVE-2023-38932	Tenda F1202 V1.2.0.9, PA202 V1.1.2.5, PW201A V1.1.2.5 and FH1202 V1.2.0.9 were discovered to contain a stack overflow via the page parameter in the SafeEmailFilter function.	9.8	More Details
CVE-2023-37483	SAP PowerDesigner - version 16.7, has improper access control which might allow an unauthenticated attacker to run arbitrary queries against the back-end database via Proxy.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38931	Tenda AC10 V1.0 V15.03.06.23, AC1206 V15.03.06.23, AC8 v4 V16.03.34.06, AC6 V2.0 V15.03.06.23, AC7 V1.0 V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0 V15.03.06.28, AC10 v4.0 V16.03.10.13 and FH1203 V2.0.1.6 were discovered to contain a stack overflow via the list parameter in the setaccount function.	9.8	More Details
CVE-2023-38930	Tenda AC7 V1.0,V15.03.06.44, F1203 V2.0.1.6, AC5 V1.0,V15.03.06.28, AC9 V3.0,V15.03.06.42_multi and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the deviceId parameter in the addWifiMacFilter function.	9.8	More Details
CVE-2023-38929	Tenda 4G300 v1.01.42 was discovered to contain a stack overflow via the page parameter at /VirtualSer.	9.8	More Details
CVE-2023-38928	Netgear R7100LG 1.0.0.78 was discovered to contain a command injection vulnerability via the password parameter at usb_remote_invite.cgi.	9.8	More Details
CVE-2023-38044	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability allows SQL Injection.	9.8	More Details
CVE-2023-34477	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability allows SQL Injection.	9.8	More Details
CVE-2023-23758	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability allows SQL Injection.	9.8	More Details
CVE-2023-38940	Tenda F1203 V2.0.1.6, FH1203 V2.0.1.6 and FH1205 V2.0.0.7(775) were discovered to contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function.	9.8	More Details
CVE-2023-39976	log_blackbox.c in libqb before 2.0.8 allows a buffer overflow via long log messages because the header size is not considered.	9.8	More Details
CVE-2023-32090	Pega platform clients who are using versions 6.1 through 7.3.1 may be utilizing default credentials	9.8	More Details
CVE-2023-3898	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in mAyaNet E-Commerce Software allows SQL Injection.This issue affects E-Commerce Software: before 1.1.	9.8	More Details
CVE-2023-40042	TOTOLINK T10_v2 5.9c.5061_B20200511 has a stack-based buffer overflow in setStaticDhcpConfig in /lib/cste_modules/lan.so. Attackers can send crafted data in an MQTT packet, via the comment parameter, to control the return address and execute code.	9.8	More Details
CVE-2023-40041	TOTOLINK T10_v2 5.9c.5061_B20200511 has a stack-based buffer overflow in setWiFiWpsConfig in /lib/cste_modules/wps.so. Attackers can send crafted data in an MQTT packet, via the pin parameter, to control the return address and execute code.	9.8	More Details
CVE-2023-36911	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36910	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-35385	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-21709	Microsoft Exchange Server Elevation of Privilege Vulnerability	9.8	More Details
CVE-2023-20586	A potential vulnerability was reported in Radeon™ Software Crimson ReLive Edition which may allow escalation of privilege. Radeon™ Software Crimson ReLive Edition falls outside of the security support lifecycle and AMD does not plan to release any mitigations	9.8	More Details
CVE-2023-39532	SES is a JavaScript environment that allows safe execution of arbitrary programs in Compartments. In version 0.18.0 prior to 0.18.7, 0.17.0 prior to 0.17.1, 0.16.0 prior to 0.16.1, 0.15.0 prior to 0.15.24, 0.14.0 prior to 0.14.5, an 0.13.0 prior to 0.13.5, there is a hole in the confinement of guest applications under SES that may manifest as either the ability to exfiltrate information or execute arbitrary code depending on the configuration and implementation of the surrounding host. Guest program running inside a Compartment with as few as no endowments can gain access to the surrounding host's dynamic import by using dynamic import after the spread operator, like `{...import(arbitraryModuleSpecifier)}`. On the web or in web extensions, a Content-Security-Policy following ordinary best practices likely mitigates both the risk of exfiltration and execution of arbitrary code, at least limiting the modules that the attacker can import to those that are already part of the application. However, without a Content-Security-Policy, dynamic import can be used to issue HTTP requests for either communication through the URL or for the execution of code reachable from that origin. Within an XS worker, an attacker can use the host's module system to the extent that the host has been configured. This typically only allows access to module code on the host's file system and is of limited use to an attacker. Within Node.js, the attacker gains access to Node.js's module system. Importing the powerful builtins is not useful except insofar as there are side-effects and tempered because dynamic import returns a promise. Spreading a promise into an object renders the promises useless. However, Node.js allows importing data URLs, so this is a clear path to arbitrary execution. Versions 0.18.7, 0.17.1, 0.16.1, 0.15.24, 0.14.5, and 0.13.5 contain a patch for this issue. Some workarounds are available. On the web, providing a suitably constrained Content-Security-Policy mitigates most of the threat. With XS, building a binary that lacks the ability to load modules at runtime mitigates the entirety of the threat. That will look like an implementation of `fxFindModule` in a file like `xsPlatform.c` that calls `fxRejectModuleFile`.	9.8	More Details
CVE-2023-3522	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in a2 License Portal System allows SQL Injection.This issue affects License Portal System: before 1.48.	9.8	More Details
CVE-2023-3386	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in a2 Camera Trap Tracking System allows SQL Injection.This issue affects Camera Trap Tracking System: before 3.1905.	9.8	More Details
CVE-2023-3651	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Digital Ant E-Commerce Software allows SQL Injection.This issue affects E-Commerce Software: before 11.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3716	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Oduyo Online Collection Software allows SQL Injection.This issue affects Online Collection Software: before 1.0.1.	9.8	More Details
CVE-2023-37682	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /php-jms/deductScores.php.	9.8	More Details
CVE-2023-3717	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Farmakom Remote Administration Console allows SQL Injection.This issue affects Remote Administration Console: before 1.02.	9.8	More Details
CVE-2023-37372	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.4). The affected applications is vulnerable to SQL injection. This could allow an unauthenticated remote attackers to execute arbitrary SQL queries on the server database.	9.8	More Details
CVE-2023-28561	Memory corruption in QESL while processing payload from external ESL device to firmware.	9.8	More Details
CVE-2022-40510	Memory corruption due to buffer copy without checking size of input in Audio while voice call with EVS vocoder.	9.8	More Details
CVE-2023-23757	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability allows SQL Injection.	9.8	More Details
CVE-2023-34476	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability allows SQL Injection.	9.8	More Details
CVE-2023-36133	PHPJabbers Availability Booking Calendar 5.0 is vulnerable to User Account Takeover through username/password change.	9.8	More Details
CVE-2023-38951	A path traversal vulnerability in ZKTeco BioTime v8.5.5 allows attackers to write arbitrary files via using a malicious SFTP configuration.	9.8	More Details
CVE-2023-36131	PHPJabbers Availability Booking Calendar 5.0 is vulnerable to Incorrect Access Control due to improper input validation of password parameter.	9.8	More Details
CVE-2023-36132	PHP Jabbers Availability Booking Calendar 5.0 is vulnerable to Incorrect Access Control.	9.8	More Details
CVE-2023-33666	ai-dev aioptimizedcombinations before v0.1.3 was discovered to contain a SQL injection vulnerability via the component /includes/ajax.php.	9.8	More Details
CVE-2023-38942	Dango-Translator v4.5.5 was discovered to contain a remote command execution (RCE) vulnerability via the component app/config/cloud_config.json.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36213	SQL injection vulnerability in MotoCMS v.3.4.3 allows a remote attacker to gain privileges via the keyword parameter of the search function.	9.8	More Details
CVE-2023-36095	An issue in Harrison Chase langchain v.0.0.194 allows an attacker to execute arbitrary code via the python exec calls in the PALChain, affected functions include from_math_prompt and from_colored_object_prompt.	9.8	More Details
CVE-2023-36134	In PHP Jabbers Class Scheduling System 1.0, lack of verification when changing an email address and/or password (on the Profile Page) allows remote attackers to take over accounts.	9.8	More Details
CVE-2023-36139	In PHPJabbers Cleaning Business Software 1.0, lack of verification when changing an email address and/or password (on the Profile Page) allows remote attackers to take over accounts.	9.8	More Details
CVE-2023-3346	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in MITSUBSHI CNC Series allows a remote unauthenticated attacker to cause Denial of Service (DoS) condition and execute arbitrary code on the product by sending specially crafted packets. In addition, system reset is required for recovery.	9.8	More Details
CVE-2023-38941	django-sspanel v2022.2.2 was discovered to contain a remote command execution (RCE) vulnerability via the component sspanel/admin_view.py -> GoodsCreateView._post.	9.8	More Details
CVE-2023-29689	PyroCMS 3.9 contains a remote code execution (RCE) vulnerability that can be exploited through a server-side template injection (SSTI) flaw. This vulnerability allows a malicious attacker to send customized commands to the server and execute arbitrary code on the affected system.	9.8	More Details
CVE-2023-37679	A remote command execution (RCE) vulnerability in NextGen Mirth Connect v4.3.0 allows attackers to execute arbitrary commands on the hosting server.	9.8	More Details
CVE-2023-36480	The Aerospike Java client is a Java application that implements a network protocol to communicate with an Aerospike server. Prior to versions 7.0.0, 6.2.0, 5.2.0, and 4.5.0 some of the messages received from the server contain Java objects that the client deserializes when it encounters them without further validation. Attackers that manage to trick clients into communicating with a malicious server can include especially crafted objects in its responses that, once deserialized by the client, force it to execute arbitrary code. This can be abused to take control of the machine the client is running on. Versions 7.0.0, 6.2.0, 5.2.0, and 4.5.0 contain a patch for this issue.	9.8	More Details
CVE-2023-38954	ZKTeco BioAccess IVS v3.3.1 was discovered to contain a SQL injection vulnerability.	9.8	More Details
CVE-2023-39143	PaperCut NG and PaperCut MF before 22.1.3 on Windows allow path traversal, enabling attackers to upload, read, or delete arbitrary files. This leads to remote code execution when external device integration is enabled (a very common configuration).	9.8	More Details
CVE-2023-33372	Connected IO v2.1.0 and prior uses a hard-coded username/password pair embedded in their device's firmware used for device communication using MQTT. An attacker who gained access to these credentials is able to connect to the MQTT broker and send messages on behalf of devices, impersonating them. in order to sign and verify JWT session tokens, allowing attackers to sign arbitrary session tokens and bypass authentication.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33373	Connected IO v2.1.0 and prior keeps passwords and credentials in clear-text format, allowing attackers to exfiltrate the credentials and use them to impersonate the devices.	9.8	More Details
CVE-2023-33374	Connected IO v2.1.0 and prior has a command as part of its communication protocol allowing the management platform to specify arbitrary OS commands for devices to execute. Attackers abusing this dangerous functionality may issue all devices OS commands to execute, resulting in arbitrary remote command execution.	9.8	More Details
CVE-2023-33375	Connected IO v2.1.0 and prior has a stack-based buffer overflow vulnerability in its communication protocol, enabling attackers to take control over devices.	9.8	More Details
CVE-2023-33376	Connected IO v2.1.0 and prior has an argument injection vulnerability in its iptables command message in its communication protocol, enabling attackers to execute arbitrary OS commands on devices.	9.8	More Details
CVE-2023-33377	Connected IO v2.1.0 and prior has an OS command injection vulnerability in the set firewall command in part of its communication protocol, enabling attackers to execute arbitrary OS commands on devices.	9.8	More Details
CVE-2023-33378	Connected IO v2.1.0 and prior has an argument injection vulnerability in its AT command message in its communication protocol, enabling attackers to execute arbitrary OS commands on devices.	9.8	More Details
CVE-2023-33379	Connected IO v2.1.0 and prior has a misconfiguration in their MQTT broker used for management and device communication, which allows devices to connect to the broker and issue commands to other device, impersonating Connected IO management platform and sending commands to all of Connected IO's devices.	9.8	More Details
CVE-2023-38692	CloudExplorer Lite is an open source, lightweight cloud management platform. Versions prior to 1.3.1 contain a command injection vulnerability in the installation function in module management. The vulnerability has been fixed in v1.3.1. There are no known workarounds aside from upgrading.	9.8	More Details
CVE-2023-36082	An isssue in GatesAIr Flexiva FM Transmitter/Exiter Fax 150W allows a remote attacker to gain privileges via the LDAP and SMTP credentials.	9.8	More Details
CVE-2023-39551	PHPGurukul Online Security Guards Hiring System v.1.0 is vulnerable to SQL Injection via osghs/admin/search.php.	9.8	More Details
CVE-2023-33371	Control ID IDSecure 4.7.26.0 and prior uses a hardcoded cryptographic key in order to sign and verify JWT session tokens, allowing attackers to sign arbitrary session tokens and bypass authentication.	9.8	More Details
CVE-2023-33367	A SQL injection vulnerability exists in Control ID IDSecure 4.7.26.0 and prior, allowing unauthenticated attackers to write PHP files on the server's root directory, resulting in remote code execution.	9.8	More Details
CVE-2023-33665	ai-dev aitable before v0.2.2 was discovered to contain a SQL injection vulnerability via the component /includes/ajax.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39216	Improper input validation in Zoom Desktop Client for Windows before 5.14.7 may allow an unauthenticated user to enable an escalation of privilege via network access.	9.6	More Details
CVE-2023-39213	Improper neutralization of special elements in Zoom Desktop Client for Windows and Zoom VDI Client before 5.15.2 may allow an unauthenticated user to enable an escalation of privilege via network access.	9.6	More Details
CVE-2023-3526	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser.	9.6	More Details
CVE-2023-1935	ROC800-Series RTU devices are vulnerable to an authentication bypass, which could allow an attacker to gain unauthorized access to data or control of the device and cause a denial-of-service condition.	9.4	More Details
CVE-2023-36534	Path traversal in Zoom Desktop Client for Windows before 5.14.7 may allow an unauthenticated user to enable an escalation of privilege via network access.	9.3	More Details
CVE-2023-21651	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	9.3	More Details
CVE-2023-38686	Sydent is an identity server for the Matrix communications protocol. Prior to version 2.5.6, if configured to send emails using TLS, Sydent does not verify SMTP servers' certificates. This makes Sydent's emails vulnerable to interception via a man-in-the-middle (MITM) attack. Attackers with privileged access to the network can intercept room invitations and address confirmation emails. This is patched in Sydent 2.5.6. When patching, make sure that Sydent trusts the certificate of the server it is connecting to. This should happen automatically when using properly issued certificates. Those who use self-signed certificates should make sure to copy their Certification Authority certificate, or their self signed certificate if using only one, to the trust store of your operating system. As a workaround, one can ensure Sydent's emails fail to send by setting the configured SMTP server to a loopback or non-routable address under one's control which does not have a listening SMTP server.	9.3	More Details
CVE-2023-39526	PrestaShop is an open source e-commerce web application. Versions prior to 1.7.8.10, 8.0.5, and 8.1.1 are vulnerable to remote code execution through SQL injection and arbitrary file write in the back office. Versions 1.7.8.10, 8.0.5, and 8.1.1 contain a patch. There are no known workarounds.	9.1	More Details
CVE-2023-33369	A path traversal vulnerability exists in Control ID IDSecure 4.7.26.0 and prior, allowing attackers to delete arbitrary files on IDSecure filesystem, causing a denial of service.	9.1	More Details
CVE-2023-39107	An arbitrary file overwrite vulnerability in NoMachine Free Edition and Enterprise Client for macOS before v8.8.1 allows attackers to overwrite root-owned files by using hardlinks.	9.1	More Details
CVE-2023-38699	MindsDB's AI Virtual Database allows developers to connect any AI/ML model to any datasource. Prior to version 23.7.4.0, a call to requests with `verify=False` disables SSL certificate checks. This rule enforces always verifying SSL certificates for methods in the Requests library. In version 23.7.4.0, certificates are validated by default, which is the desired behavior.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4188	SQL Injection in GitHub repository instantsoft/icms2 prior to 2.16.1-git.	9.1	More Details
CVE-2023-37364	In WS-Inc J WBEM Server 4.7.4 before 4.7.5, the CIM-XML protocol adapter does not disable entity resolution. This allows context-dependent attackers to read arbitrary files or cause a denial of service, a similar issue to CVE-2013-4152.	9.1	More Details
CVE-2023-21643	Memory corruption due to untrusted pointer dereference in automotive during system call.	9.1	More Details
CVE-2023-24845	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC, RUGGEDCOM i802, RUGGEDCOM i802NC, RUGGEDCOM i803, RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM M2100F, RUGGEDCOM M2100NC, RUGGEDCOM M2200, RUGGEDCOM M2200F, RUGGEDCOM M2200NC, RUGGEDCOM M969, RUGGEDCOM M969F, RUGGEDCOM M969NC, RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC, RUGGEDCOM RS400, RUGGEDCOM RS400F, RUGGEDCOM RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC, RUGGEDCOM RS416, RUGGEDCOM RS416F, RUGGEDCOM RS416NC, RUGGEDCOM RS416NCv2 V4.X, RUGGEDCOM RS416NCv2 V5.X, RUGGEDCOM RS416P, RUGGEDCOM RS416PF, RUGGEDCOM RS416PNC, RUGGEDCOM RS416PNCv2 V4.X, RUGGEDCOM RS416PNCv2 V5.X, RUGGEDCOM RS416Pv2 V4.X, RUGGEDCOM RS416Pv2 V5.X, RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC, RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900F, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GF, RUGGEDCOM RS900GNC, RUGGEDCOM RS900GNC(32M) V4.X, RUGGEDCOM RS900GNC(32M) V5.X, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPF, RUGGEDCOM RS900GPNC, RUGGEDCOM RS900L, RUGGEDCOM RS900L, RUGGEDCOM RS900LNC, RUGGEDCOM RS900LNC, RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-GETS-XX, RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM RS900MNC-STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM RS900NC, RUGGEDCOM RS900NC(32M) V4.X, RUGGEDCOM RS900NC(32M) V5.X, RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GF, RUGGEDCOM RS940GNC, RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100F, RUGGEDCOM RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PF, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200F, RUGGEDCOM RSG2200NC, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM	9.1	More Details

CVE Number	Description	Base Score	Reference
	RSG2300 V5.X, RUGGEDCOM RSG2300F, RUGGEDCOM RSG2300NC V4.X, RUGGEDCOM RSG2300NC V5.X, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PF, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488F, RUGGEDCOM RSG2488NC V4.X, RUGGEDCOM RSG2488NC V5.X, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM RSL910, RUGGEDCOM RSL910NC, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. The affected products insufficiently block data from being forwarded over the mirror port into the mirrored network. An attacker could use this behavior to transmit malicious packets to systems in the mirrored network, possibly influencing their configuration and runtime behavior.		
CVE-2023-20214	A vulnerability in the request authentication validation for the REST API of Cisco SD-WAN vManage software could allow an unauthenticated, remote attacker to gain read permissions or limited write permissions to the configuration of an affected Cisco SD-WAN vManage instance. This vulnerability is due to insufficient request validation when using the REST API feature. An attacker could exploit this vulnerability by sending a crafted API request to an affected vManage instance. A successful exploit could allow the attacker to retrieve information from and send information to the configuration of the affected Cisco vManage instance. This vulnerability only affects the REST API and does not affect the web-based management interface or the CLI.	9.1	More Details
CVE-2023-4202	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the device name field of the web-interface.	9.0	More Details
CVE-2023-36217	Cross Site Scripting vulnerability in Xoops CMS v.2.5.10 allows a remote attacker to execute arbitrary code via the category name field of the image manager function.	9.0	More Details
CVE-2023-4203	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stored Cross-Site Scripting vulnerability, which can be triggered by authenticated users in the ping tool of the web-interface.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-33366	A SQL injection vulnerability exists in Suprema BioStar 2 before 2.9.1, which allows authenticated users to inject arbitrary SQL directives into an SQL statement and execute arbitrary SQL commands.	8.8	More Details
CVE-2023-36255	An issue in Eramba Limited Eramba Enterprise and Community edition v.3.19.1 allows a remote attacker to execute arbitrary code via the path parameter in the URL.	8.8	More Details
CVE-2023-38759	Cross Site Request Forgery (CSRF) vulnerability in wger Project wger Workout Manager 2.2.0a3 allows a remote attacker to gain privileges via the user-management feature in the gym/views/gym.py, templates/gym/reset_user_password.html, templates/user/overview.html, core/views/user.py, and templates/user/preferences.html, core/forms.py components.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3663	In CODESYS Development System versions from 3.5.11.20 and before 3.5.19.20 a missing integrity check might allow an unauthenticated remote attacker to manipulate the content of notifications received via HTTP by the CODESYS notification server.	8.8	More Details
CVE-2023-29328	Microsoft Teams Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-29330	Microsoft Teams Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-35368	Microsoft Exchange Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-21407	A broken access control was found allowing for privileged escalation of the operator account to gain administrator privileges.	8.8	More Details
CVE-2023-4126	Insufficient Session Expiration in GitHub repository answerdev/answer prior to v1.1.0.	8.8	More Details
CVE-2023-4125	Weak Password Requirements in GitHub repository answerdev/answer prior to v1.1.0.	8.8	More Details
CVE-2023-35381	Windows Fax Service Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-36212	File Upload vulnerability in Total CMS v.1.7.4 allows a remote attacker to execute arbitrary code via a crafted PHP file to the edit page function.	8.8	More Details
CVE-2023-36882	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-35387	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability	8.8	More Details
CVE-2023-4078	Inappropriate implementation in Extensions in Google Chrome prior to 115.0.5790.170 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-4077	Insufficient data validation in Extensions in Google Chrome prior to 115.0.5790.170 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-4076	Use after free in WebRTC in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted WebRTC session. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4075	Use after free in Cast in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-4074	Use after free in Blink Task Scheduling in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-4073	Out of bounds memory access in ANGLE in Google Chrome on Mac prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-4072	Out of bounds read and write in WebGL in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-4071	Heap buffer overflow in Visuals in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-4046	In CODESYS Control in multiple versions a improper restriction of operations within the bounds of a memory buffer allow an remote attacker with user privileges to gain full access of the device.	8.8	More Details
CVE-2023-38922	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the update_auth function.	8.8	More Details
CVE-2023-36298	DedeCMS v5.7.109 has a File Upload vulnerability, leading to remote code execution (RCE).	8.8	More Details
CVE-2023-36299	A File Upload vulnerability in typecho v.1.2.1 allows a remote attacker to execute arbitrary code via the upload and options-general parameters in index.php.	8.8	More Details
CVE-2023-38925	Netgear DC112A 1.0.0.64, EX6200 1.0.3.94 and R6300v2 1.0.4.8 were discovered to contain a buffer overflow via the http_passwd parameter in password.cgi.	8.8	More Details
CVE-2023-38926	Netgear EX6200 v1.0.3.94 was discovered to contain a buffer overflow via the wla_temp_ssid parameter at acosNvramConfig_set.	8.8	More Details
CVE-2023-39550	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the check_auth function.	8.8	More Details
CVE-2023-38921	Netgear WG302v2 v5.2.9 and WAG302v2 v5.1.19 were discovered to contain multiple command injection vulnerabilities in the upgrade_handler function via the firmwareRestore and firmwareServerip parameters.	8.8	More Details
CVE-2023-38591	Netgear DG834Gv5 1.6.01.34 was discovered to contain multiple buffer overflows via the wla_ssid and wla_temp_ssid parameters at bsw_ssid.cgi.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38412	Netgear R6900P v1.3.3.154 was discovered to contain multiple buffer overflows via the wla_ssid and wlg_ssid parameters at ia_ap_setting.cgi.	8.8	More Details
CVE-2023-36499	Netgear XR300 v1.0.3.78 was discovered to contain multiple buffer overflows via the wla_ssid and wlg_ssid parameters at genie_ap_wifi_change.cgi.	8.8	More Details
CVE-2023-39439	SAP Commerce Cloud may accept an empty passphrase for user ID and passphrase authentication, allowing users to log into the system without a passphrase.	8.8	More Details
CVE-2023-3570	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP DELETE request to gain full access to the device.	8.8	More Details
CVE-2023-3571	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST releated to certificate operations to gain full access to the device.	8.8	More Details
CVE-2023-3573	In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a command injection in a HTTP POST request releated to font configuration operations to gain full access to the device.	8.8	More Details
CVE-2023-37569	This vulnerability exists in ESDS Emagic Data Center Management Suit due to lack of input sanitization in its Ping component. A remote authenticated attacker could exploit this by injecting OS commands on the targeted system. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code on targeted system.	8.8	More Details
CVE-2023-39508	Execution with Unnecessary Privileges, : Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Software Foundation Apache Airflow.The "Run Task" feature enables authenticated user to bypass some of the restrictions put in place. It allows to execute code in the webserver context as well as allows to bypas limitation of access the user has to certain DAGs. The "Run Task" feature is considered dangerous and it has been removed entirely in Airflow 2.6.0 This issue affects Apache Airflow: before 2.6.0.	8.8	More Details
CVE-2023-38943	ShuiZe_0x727 v1.0 was discovered to contain a remote command execution (RCE) vulnerability via the component /iniFile/config.ini.	8.8	More Details
CVE-2023-39346	LinuxASMCallGraph is software for drawing the call graph of the programming code. Linux ASMCallGraph before commit 20dba06bd1a3cf260612d4f21547c25002121cd5 allows attackers to cause a remote code execution on the server side via uploading a crafted ZIP file due to incorrect filtering rules of uploaded file. The problem has been patched in commit 20dba06bd1a3cf260612d4f21547c25002121cd5. There are no known workarounds.	8.8	More Details
CVE-2023-2843	The MultiParcels Shipping For WooCommerce WordPress plugin before 1.14.15 does not properly sanitize and escape a parameter before using it in an SQL statement, which could allow any authenticated users, such as subscribers, to perform SQL Injection attacks.	8.8	More Details
CVE-2023-4159	Unrestricted Upload of File with Dangerous Type in GitHub repository omeka/omeka-s prior to 4.0.3.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27411	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.4). The affected applications is vulnerable to SQL injection. This could allow an authenticated remote attackers to execute arbitrary SQL queries on the server database and escalate privileges.	8.8	More Details
CVE-2023-33364	An OS Command injection vulnerability exists in Suprema BioStar 2 before V2.9.1, which allows authenticated users to execute arbitrary OS commands on the BioStar 2 server.	8.8	More Details
CVE-2023-4069	Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-4195	PHP Remote File Inclusion in GitHub repository cockpit-hq/cockpit prior to 2.6.3.	8.8	More Details
CVE-2023-38169	Microsoft SQL OLE DB Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-38181	Microsoft Exchange Server Spoofing Vulnerability	8.8	More Details
CVE-2023-38186	Windows Mobile Device Management Elevation of Privilege Vulnerability	8.8	More Details
CVE-2023-38185	Microsoft Exchange Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-39211	Improper privilege management in Zoom Desktop Client for Windows and Zoom Rooms for Windows before 5.15.5 may allow an authenticated user to enable an information disclosure via local access.	8.8	More Details
CVE-2023-36899	ASP.NET Elevation of Privilege Vulnerability	8.8	More Details
CVE-2023-0426	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible. Stack-based Buffer Overflow vulnerability in ABB Freelance controllers AC 700F (conroller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects: Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019 , through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0425	ABB is aware of vulnerabilities in the product versions listed below. An update is available that resolves the reported vulnerabilities in the product versions under maintenance. An attacker who successfully exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible. Numeric Range Comparison Without Minimum Check vulnerability in ABB Freelance controllers AC 700F (Controller modules), ABB Freelance controllers AC 900F (controller modules).This issue affects: Freelance controllers AC 700F: from 9.0;0 through V9.2 SP2, through Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1; Freelance controllers AC 900F: Freelance 2013, through Freelance 2013SP1, through Freelance 2016, through Freelance 2016SP1, through Freelance 2019, through Freelance 2019 SP1, through Freelance 2019 SP1 FP1.	8.6	More Details
CVE-2023-2423	A vulnerability was discovered in the Rockwell Automation Armor PowerFlex device when the product sends communications to the local event log. Threat actors could exploit this vulnerability by sending an influx of network commands, causing the product to generate an influx of event log traffic at a high rate. If exploited, the product would stop normal operations and self-reset creating a denial-of-service condition. The error code would need to be cleared prior to resuming normal operations.	8.6	More Details
CVE-2023-28537	Memory corruption while allocating memory in COmxApeDec module in Audio.	8.4	More Details
CVE-2023-21408	Due to insufficient file permissions, unprivileged users could gain access to unencrypted user credentials that are used in the integration interface towards 3rd party systems.	8.4	More Details
CVE-2023-21409	Due to insufficient file permissions, unprivileged users could gain access to unencrypted administrator credentials allowing the configuration of the application.	8.4	More Details
CVE-2023-22666	Memory Corruption in Audio while playing amrwbplus clips with modified content.	8.4	More Details
CVE-2023-39527	PrestaShop is an open source e-commerce web application. Versions prior to 1.7.8.10, 8.0.5, and 8.1.1 are vulnerable to cross-site scripting through the `isCleanHTML` method. Versions 1.7.8.10, 8.0.5, and 8.1.1 contain a patch. There are no known workarounds.	8.3	More Details
CVE-2023-3932	An issue has been discovered in GitLab EE affecting all versions starting from 13.12 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible for an attacker to run pipeline jobs as an arbitrary user via scheduled security scan policies.	8.2	More Details
CVE-2023-21625	Information disclosure in Network Services due to buffer over-read while the device receives DNS response.	8.2	More Details
CVE-2023-34196	In the Keyfactor EJBCA before 8.0.0, the RA web certificate distribution servlet /ejbca/ra/cert allows partial denial of service due to an authentication issue. In configurations using OAuth, disclosure of CA certificates (attributes and public keys) to unauthenticated or less privileged users may occur.	8.2	More Details
CVE-2023-36897	Visual Studio Tools for Office Runtime Spoofing Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37498	A user is capable of assigning him/herself to arbitrary groups by reusing a POST request issued by an administrator. It is possible that an attacker could potentially escalate their privileges.	8.1	More Details
CVE-2023-3365	The MultiParcels Shipping For WooCommerce WordPress plugin before 1.14.14 does not have authorisation when deleting shipment, allowing any authenticated users, such as subscriber to delete arbitrary shipment	8.1	More Details
CVE-2023-38689	Logistics Pipes is a modification (a.k.a. mod) for the computer game Minecraft Java Edition. The mod used Java's `ObjectInputStream#readObject` on untrusted data coming from clients or servers over the network resulting in possible remote code execution when sending specifically crafted network packets after connecting. The affected versions were released between 2013 and 2016 and the issue (back then unknown) was fixed in 2016 by a refactoring of the network IO code. The issue is present in all Logistics Pipes versions ranged from 0.7.0.91 prior to 0.10.0.71, which were downloaded from different platforms summing up to multi-million downloads. For Minecraft version 1.7.10 the issue was fixed in build 0.10.0.71. Everybody on Minecraft 1.7.10 should check their version number of Logistics Pipes in their modlist and update, if the version number is smaller than 0.10.0.71. Any newer supported Minecraft version (like 1.12.2) never had a Logistics Pipes version with vulnerable code. The best available workaround for vulnerable versions is to play in singleplayer only or update to newer Minecraft versions and modpacks.	8.1	More Details
CVE-2023-37501	A Persistent XSS vulnerability can be carried out in a certain field of Unica Campaign. An attacker could hijack a user's session and perform other attacks.	8.1	More Details
CVE-2020-26064	A vulnerability in the web UI of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to gain read and write access to information that is stored on an affected system. The vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by persuading a user to import a crafted XML file with malicious entries. A successful exploit could allow the attacker to read and write files within the affected application.	8.1	More Details
CVE-2023-37500	A Persistent Cross-site Scripting (XSS) vulnerability can be carried out on certain pages of Unica Platform. An attacker could hijack a user's session and perform other attacks.	8.1	More Details
CVE-2023-37499	A Persistent Cross-site Scripting (XSS) vulnerability can be carried out in a certain field of the Unica Platform. An attacker could hijack a user's session and perform other attacks.	8.1	More Details
CVE-2023-37497	The Unica application exposes an API which accepts arbitrary XML input. By manipulating the given XML, an authenticated attacker with certain rights can successfully perform XML External Entity attacks (XXE) against the backend service.	8.1	More Details
CVE-2023-39349	Sentry is an error tracking and performance monitoring platform. Starting in version 22.1.0 and prior to version 23.7.2, an attacker with access to a token with few or no scopes can query `/api/0/api-tokens/` for a list of all tokens created by a user, including tokens with greater scopes, and use those tokens in other requests. There is no evidence that the issue was exploited on `sentry.io`. For self-hosted users, it is advised to rotate user auth tokens. A fix is available in version 23.7.2 of `sentry` and `self-hosted`. There are no known workarounds.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38704	import-in-the-middle is a module loading interceptor specifically for ESM modules. The import-in-the-middle loader works by generating a wrapper module on the fly. The wrapper uses the module specifier to load the original module and add some wrapping code. Prior to version 1.4.2, it allows for remote code execution in cases where an application passes user-supplied input directly to the `import()` function. This vulnerability has been patched in import-in-the-middle version 1.4.2. Some workarounds are available. Do not pass any user-supplied input to `import()`. Instead, verify it against a set of allowed values. If using import-in-the-middle, directly or indirectly, and support for EcmaScript Modules is not needed, ensure that no options are set, either via command-line or the `NODE_OPTIONS` environment variable, that would enable loader hooks.	8.1	More Details
CVE-2023-4070	Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2022-40609	IBM SDK, Java Technology Edition 7.1.5.18 and 8.0.8.0 could allow a remote attacker to execute arbitrary code on the system, caused by an unsafe deserialization flaw. By sending specially-crafted data, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 236069.	8.1	More Details
CVE-2023-4068	Type Confusion in V8 in Google Chrome prior to 115.0.5790.170 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	8.1	More Details
CVE-2023-4141	The WP Ultimate CSV Importer plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 7.9.8 via the '->cus2' parameter. This allows authenticated attackers with author-level permissions or above, if the administrator previously grants access in the plugin settings, to create a PHP file and execute code on the server. The author resolved this vulnerability by removing the ability for authors and editors to import files, please note that this means php file creation is still allowed for site administrators, use the plugin with caution.	8.0	More Details
CVE-2023-38182	Microsoft Exchange Server Remote Code Execution Vulnerability	8.0	More Details
CVE-2023-35388	Microsoft Exchange Server Remote Code Execution Vulnerability	8.0	More Details
CVE-2023-36892	Microsoft SharePoint Server Spoofing Vulnerability	8.0	More Details
CVE-2023-36891	Microsoft SharePoint Server Spoofing Vulnerability	8.0	More Details
CVE-2023-36541	Insufficient verification of data authenticity in Zoom Desktop Client for Windows before 5.14.5 may allow an authenticated user to enable an escalation of privilege via network access.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4142	The WP Ultimate CSV Importer plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 7.9.8 via the '->cus1' parameter. This allows authenticated attackers with author-level permissions or above, if the administrator previously grants access in the plugin settings, to execute code on the server. The author resolved this vulnerability by removing the ability for authors and editors to import files, please note that this means remote code execution is still possible for site administrators, use the plugin with caution.	8.0	More Details
CVE-2023-39212	Untrusted search path in Zoom Rooms for Windows before version 5.15.5 may allow an authenticated user to enable a denial of service via local access.	7.9	More Details
CVE-2023-38497	Cargo downloads the Rust project's dependencies and compiles the project. Cargo prior to version 0.72.2, bundled with Rust prior to version 1.71.1, did not respect the umask when extracting crate archives on UNIX-like systems. If the user downloaded a crate containing files writeable by any local user, another local user could exploit this to change the source code compiled and executed by the current user. To prevent existing cached extractions from being exploitable, the Cargo binary version 0.72.2 included in Rust 1.71.1 or later will purge caches generated by older Cargo versions automatically. As a workaround, configure one's system to prevent other local users from accessing the Cargo directory, usually located in `~/.cargo`.	7.9	More Details
CVE-2023-38530	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions < V14.3.0.3). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-38525	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions < V14.3.0.3). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-38641	A vulnerability has been identified in SICAM TOOLBOX II (All versions < V07.10). The affected application's database service is executed as `NT AUTHORITY\SYSTEM`. This could allow a local attacker to execute operating system commands with elevated privileges.	7.8	More Details
CVE-2023-38531	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.12), Teamcenter Visualization V14.3 (All versions < V14.3.0.9), Teamcenter Visualization V2312 (All versions < V2312.0004). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-38175	Microsoft Windows Defender Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38529	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.12), Teamcenter Visualization V14.3 (All versions < V14.3.0.9), Teamcenter Visualization V2312 (All versions < V2312.0004). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-38528	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.197), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions < V14.3.0.3). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted X_T file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-22317	Use after free vulnerability exists in CX-Programmer Ver.9.79 and earlier. By having a user open a specially crafted CXP file, information disclosure and/or arbitrary code execution may occur. This vulnerability is different from CVE-2023-22277 and CVE-2023-22314.	7.8	More Details
CVE-2023-22314	Use after free vulnerability exists in CX-Programmer Ver.9.79 and earlier. By having a user open a specially crafted CXP file, information disclosure and/or arbitrary code execution may occur. This vulnerability is different from CVE-2023-22277 and CVE-2023-22317.	7.8	More Details
CVE-2023-38527	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.12), Teamcenter Visualization V14.3 (All versions < V14.3.0.9), Teamcenter Visualization V2312 (All versions < V2312.0004). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-38526	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions < V14.3.0.3). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-30796	A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-38679	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21106)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38681	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted IGS file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21270)	7.8	More Details
CVE-2023-38418	The BIG-IP Edge Client Installer on macOS does not follow best practices for elevating privileges during the installation process. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.8	More Details
CVE-2023-39185	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-39187	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-39188	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-39419	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds write past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-39549	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 2). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted DWG file. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19562)	7.8	More Details
CVE-2023-4147	A use-after-free flaw was found in the Linux kernel's Netfilter functionality when adding a rule with NFTA_RULE_CHAIN_ID. This flaw allows a local user to crash or escalate their privileges on the system.	7.8	More Details
CVE-2023-39186	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-32764	Fabasoft Cloud Enterprise Client 23.3.0.130 allows a user to escalate their privileges to local administrator.	7.8	More Details
CVE-2023-39184	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PSM files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38680	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21132)	7.8	More Details
CVE-2023-39183	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PSM files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-39182	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-39181	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-3896	Divide By Zero in vim/vim from 9.0.1367-1 to 9.0.1367-3	7.8	More Details
CVE-2023-38683	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Teamcenter Visualization V13.2 (All versions < V13.2.0.14), Teamcenter Visualization V14.1 (All versions < V14.1.0.10), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted TIFF file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-38682	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Teamcenter Visualization V13.2 (All versions < V13.2.0.14), Teamcenter Visualization V14.1 (All versions < V14.1.0.10), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted TIFF files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-28830	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2023-30795	A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4), Parasolid V34.0 (All versions < V34.0.253), Parasolid V34.1 (All versions < V34.1.243), Parasolid V35.0 (All versions < V35.0.177), Parasolid V35.1 (All versions < V35.1.073). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-22277	Use after free vulnerability exists in CX-Programmer Ver.9.79 and earlier. By having a user open a specially crafted CXP file, information disclosure and/or arbitrary code execution may occur. This vulnerability is different from CVE-2023-22317 and CVE-2023-22314.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35390	.NET and Visual Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-46782	An issue was discovered in Stormshield SSL VPN Client before 3.2.0. A logged-in user, able to only launch the VPNSSL Client, can use the OpenVPN instance to execute malicious code as administrator on the local machine.	7.8	More Details
CVE-2023-36923	SAP SQLA for PowerDesigner 17 bundled with SAP PowerDesigner 16.7 SP06 PL03, allows an attacker with local access to the system, to place a malicious library, that can be executed by the application. An attacker could thereby control the behavior of the application.	7.8	More Details
CVE-2023-36344	An issue in Diebold Nixdorf Vynamic View Console v.5.3.1 and before allows a local attacker to execute arbitrary code via not restricting the search path for required DLLs and not verifying the signature.	7.8	More Details
CVE-2023-38748	Use after free vulnerability exists in CX-Programmer Included in CX-One CXONE-AL[][]D-V4 V9.80 and earlier. By having a user open a specially crafted CXP file, information disclosure and/or arbitrary code execution may occur.	7.8	More Details
CVE-2023-38747	Heap-based buffer overflow vulnerability exists in CX-Programmer Included in CX-One CXONE-AL[][]D-V4 V9.80 and earlier. By having a user open a specially crafted CXP file, information disclosure and/or arbitrary code execution may occur.	7.8	More Details
CVE-2023-35379	Reliability Analysis Metrics Calculation Engine (RACEng) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-38746	Out-of-bounds read vulnerability/issue exists in CX-Programmer Included in CX-One CXONE-AL[][]D-V4 V9.80 and earlier. By having a user open a specially crafted CXP file, information disclosure and/or arbitrary code execution may occur.	7.8	More Details
CVE-2023-35380	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-36904	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-38154	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-36895	Microsoft Outlook Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-35382	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-39062	A vulnerability has been identified in SICAM TOOLBOX II (All versions < V07.10). Affected applications do not properly set permissions for product folders. This could allow an authenticated attacker with low privileges to replace DLLs and conduct a privilege escalation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41544	A vulnerability has been identified in Siemens Software Center (All versions < V3.0). A DLL Hijacking vulnerability could allow a local attacker to execute code with elevated privileges by placing a malicious DLL in one of the directories on the DLL search path.	7.8	More Details
CVE-2023-36896	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-31432	Through manipulation of passwords or other variables, using commands such as portcfgupload, configupload, license, myid, a non-privileged user could obtain root privileges in Brocade Fabric OS versions before Brocade Fabric OS v9.1.1c and v9.2.0.	7.8	More Details
CVE-2023-35386	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-36903	Windows System Assessment Tool Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-35372	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-36866	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-35371	Microsoft Office Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-37646	An issue in the CAB file extraction function of Bitberry File Opener v23.0 allows attackers to execute a directory traversal.	7.8	More Details
CVE-2023-20555	Insufficient input validation in CpmDisplayFeatureSmm may allow an attacker to corrupt SMM memory by overwriting an arbitrary bit in an attacker-controlled pointer potentially leading to arbitrary code execution in SMM.	7.8	More Details
CVE-2023-36898	Tablet Windows User Interface Application Core Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-38170	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-36900	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-20562	Insufficient validation in the IOCTL (Input Output Control) input buffer in AMD uProf may allow an authenticated user to load an unsigned driver potentially leading to arbitrary kernel execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36865	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-35359	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21652	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	7.7	More Details
CVE-2023-39214	Exposure of sensitive information in Zoom Client SDK's before 5.15.5 may allow an authenticated user to enable a denial of service via network access.	7.6	More Details
CVE-2023-37490	SAP Business Objects Installer - versions 420, 430, allows an authenticated attacker within the network to overwrite an executable file created in a temporary directory during the installation process. On replacing this executable with a malicious file, an attacker can completely compromise the confidentiality, integrity, and availability of the system	7.6	More Details
CVE-2023-39437	SAP business One allows - version 10.0, allows an attacker to insert malicious code into the content of a web page or application and gets it delivered to the client, resulting to Cross-site scripting. This could lead to harmful action affecting the Confidentiality, Integrity and Availability of the application.	7.6	More Details
CVE-2022-34453	Dell XtremIO X2 XMS versions prior to 6-4-1.11 contain an improper access control vulnerability. A remote read only user could potentially exploit this vulnerability to perform add/delete QoS policies which are disabled by default.	7.6	More Details
CVE-2023-26439	The cacheservice API could be abused to inject parameters with SQL syntax which was insufficiently sanitized before getting executed as SQL statement. Attackers with access to a local or restricted network were able to perform arbitrary SQL queries, discovering other users cached data. We have improved the input check for API calls and filter for potentially malicious content. No publicly available exploits are known.	7.6	More Details
CVE-2023-36135	User enumeration is found in in PHPJabbers Class Scheduling System v1.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	7.5	More Details
CVE-2023-38952	Insecure access control in ZKTeco BioTime v8.5.5 allows unauthenticated attackers to read sensitive backup files and access sensitive information such as user credentials via sending a crafted HTTP request to the static files resources of the system.	7.5	More Details
CVE-2023-38950	A path traversal vulnerability in the iclock API of ZKTeco BioTime v8.5.5 allows unauthenticated attackers to read arbitrary files via supplying a crafted payload.	7.5	More Details
CVE-2023-38949	An issue in a hidden API in ZKTeco BioTime v8.5.5 allows unauthenticated attackers to arbitrarily reset the Administrator password via a crafted web request.	7.5	More Details
CVE-2023-3364	An issue has been discovered in GitLab CE/EE affecting all versions starting from 8.14 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A Regular Expression Denial of Service was possible via sending crafted payloads which use AutolinkFilter to the preview_markdown endpoint.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38180	.NET and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2023-0525	Weak Encoding for Password vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT27 model versions 01.49.000 and prior, GT25 model versions 01.49.000 and prior, GT23 model versions 01.49.000 and prior, GT21 model versions 01.49.000 and prior, GOT SIMPLE Series GS25 model versions 01.49.000 and prior, GS21 model versions 01.49.000 and prior, GT Designer3 Version1 (GOT2000) versions 1.295H and prior and GT SoftGOT2000 versions 1.295H and prior allows a remote unauthenticated attacker to obtain plaintext passwords by sniffing packets containing encrypted passwords and decrypting the encrypted passwords, in the case of transferring data with GT Designer3 Version1(GOT2000) and GOT2000 Series or GOT SIMPLE Series with the Data Transfer Security function enabled, or in the case of transferring data by the SoftGOT-GOT link function with GT SoftGOT2000 and GOT2000 series with the Data Transfer Security function enabled.	7.5	More Details
CVE-2023-28555	Transient DOS in Audio while remapping channel buffer in media codec decoding.	7.5	More Details
CVE-2023-30146	Assmann Digitus Plug&View IP Camera HT-IP211HDP, version 2.000.022 allows unauthenticated attackers to download a copy of the camera's settings and the administrator credentials.	7.5	More Details
CVE-2023-39533	go-libp2p is the Go implementation of the libp2p Networking Stack. Prior to versions 0.27.8, 0.28.2, and 0.29.1 malicious peer can use large RSA keys to run a resource exhaustion attack & force a node to spend time doing signature verification of the large key. This vulnerability is present in the core/crypto module of go-libp2p and can occur during the Noise handshake and the libp2p x509 extension verification step. To prevent this attack, go-libp2p versions 0.27.8, 0.28.2, and 0.29.1 restrict RSA keys to <= 8192 bits. To protect one's application, it is necessary to update to these patch releases and to use the updated Go compiler in 1.20.7 or 1.19.12. There are no known workarounds for this issue.	7.5	More Details
CVE-2022-48579	UnRAR before 6.2.3 allows extraction of files outside of the destination folder via symlink chains.	7.5	More Details
CVE-2021-24916	The Qubely WordPress plugin before 1.8.6 allows unauthenticated user to send arbitrary e-mails to arbitrary addresses via the qubely_send_form_data AJAX action.	7.5	More Details
CVE-2023-4012	ntpd will crash if the server is not NTS-enabled (no certificate) and it receives an NTS-enabled client request (mode 3).	7.5	More Details
CVE-2023-39379	Fujitsu Software Infrastructure Manager (ISM) stores sensitive information at the product's maintenance data (ismsnap) in cleartext form. As a result, the password for the proxy server that is configured in ISM may be retrieved. Affected products and versions are as follows: Fujitsu Software Infrastructure Manager Advanced Edition V2.8.0.060, Fujitsu Software Infrastructure Manager Advanced Edition for PRIMEFLEX V2.8.0.060, and Fujitsu Software Infrastructure Manager Essential Edition V2.8.0.060.	7.5	More Details
CVE-2023-32783	The event analysis component in Zoho ManageEngine ADAudit Plus 7.1.1 allows an attacker to bypass audit detection by creating or renaming user accounts with a "$" symbol suffix. NOTE: the vendor states "We do not consider this as a security bug and it's an expected behaviour."	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39086	ASUS RT-AC66U B1 3.0.0.4.286_51665 was discovered to transmit sensitive information in cleartext.	7.5	More Details
CVE-2023-37896	Nuclei is a vulnerability scanner. Prior to version 2.9.9, a security issue in the Nuclei project affected users utilizing Nuclei as Go code (SDK) running custom templates. This issue did not affect CLI users. The problem was related to sanitization issues with payload loading in sandbox mode. There was a potential risk with payloads loading in sandbox mode. The issue occurred due to relative paths not being converted to absolute paths before doing the check for `sandbox` flag allowing arbitrary files to be read on the filesystem in certain cases when using Nuclei from `Go` SDK implementation. This issue has been fixed in version 2.9.9. The maintainers have also enabled sandbox by default for filesystem loading. This can be optionally disabled if required. The `-sandbox` option has been deprecated and is now divided into two new options: `-lfa` (allow local file access) which is enabled by default and `-lna` (restrict local network access) which can be enabled by users optionally. The `-lfa` allows file (payload) access anywhere on the system (disabling sandbox effectively), and `-lna` blocks connections to the local/private network.	7.5	More Details
CVE-2023-3994	An issue has been discovered in GitLab CE/EE affecting all versions starting from 9.3 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A Regular Expression Denial of Service was possible via sending crafted payloads which use ProjectReferenceFilter to the preview_markdown endpoint.	7.5	More Details
CVE-2023-38184	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	7.5	More Details
CVE-2023-38688	twitch-tui provides Twitch chat in a terminal. Prior to version 2.4.1, the connection is not using TLS for communication. In the configuration of the irc connection, the software disables TLS, which makes all communication to Twitch IRC servers unencrypted. As a result, communication, including auth tokens, can be sniffed. Version 2.4.1 has a patch for this issue.	7.5	More Details
CVE-2023-37491	The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EXT, can be bypassed in certain conditions, which may enable an authenticated malicious user to enter the network of the SAP systems served by the attacked SAP Message server. This may lead to unauthorized read and write of data as well as rendering the system unavailable.	7.5	More Details
CVE-2023-4139	The WP Ultimate CSV Importer plugin for WordPress is vulnerable to Sensitive Information Exposure via Directory Listing due to missing restriction in export folder indexing in versions up to, and including, 7.9.8. This makes it possible for unauthenticated attackers to list and view exported files.	7.5	More Details
CVE-2022-46484	Information disclosure in password protected surveys in Data Illusion Survey Software Solutions NGSurvey v2.4.28 and below allows attackers to view the password to access and arbitrarily submit surveys.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39269	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC, RUGGEDCOM i802, RUGGEDCOM i802NC, RUGGEDCOM i803, RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM M2100F, RUGGEDCOM M2100NC, RUGGEDCOM M2200, RUGGEDCOM M2200F, RUGGEDCOM M2200NC, RUGGEDCOM M969, RUGGEDCOM M969F, RUGGEDCOM M969NC, RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC, RUGGEDCOM RS400, RUGGEDCOM RS400F, RUGGEDCOM RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC, RUGGEDCOM RS416, RUGGEDCOM RS416F, RUGGEDCOM RS416NC, RUGGEDCOM RS416NCv2 V4.X, RUGGEDCOM RS416NCv2 V5.X, RUGGEDCOM RS416P, RUGGEDCOM RS416PF, RUGGEDCOM RS416PNC, RUGGEDCOM RS416PNCv2 V4.X, RUGGEDCOM RS416PNCv2 V5.X, RUGGEDCOM RS416Pv2 V4.X, RUGGEDCOM RS416Pv2 V5.X, RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC, RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900F, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GF, RUGGEDCOM RS900GNC, RUGGEDCOM RS900GNC(32M) V4.X, RUGGEDCOM RS900GNC(32M) V5.X, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPF, RUGGEDCOM RS900GPNC, RUGGEDCOM RS900L, RUGGEDCOM RS900LNC, RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-GETS-XX, RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM RS900MNC-STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM RS900NC(32M) V4.X, RUGGEDCOM RS900NC(32M) V5.X, RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GF, RUGGEDCOM RS940GNC, RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100F, RUGGEDCOM RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PF, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200F, RUGGEDCOM RSG2200NC, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300F, RUGGEDCOM RSG2300NC V4.X, RUGGEDCOM RSG2300NC V5.X, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PF, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488F, RUGGEDCOM RSG2488NC V4.X, RUGGEDCOM RSG2488NC V5.X, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM RSL910, RUGGEDCOM RSL910NC, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. The web server of the affected devices contains a vulnerability that may lead to a denial of service condition. An attacker may cause total loss of availability of the web server, which might recover after the attack is over.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39144	Element55 KnowMore appliances version 21 and older was discovered to store passwords in plaintext.	7.5	More Details
CVE-2023-36912	Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability	7.5	More Details
CVE-2023-38773	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the volopp1 and volopp2 parameters within the /QueryView.php.	7.5	More Details
CVE-2023-24698	Insufficient parameter validation in the Foswiki::Sandbox component of Foswiki v2.1.7 and below allows attackers to perform a directory traversal via supplying a crafted web request.	7.5	More Details
CVE-2023-38178	.NET Core and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2023-38556	Improper input validation vulnerability in SEIKO EPSON printer Web Config allows a remote attacker to turned off the printer. [Note] Web Config is the software that allows users to check the status and change the settings of SEIKO EPSON printers via a web browser. Web Config is pre-installed in some printers provided by SEIKO EPSON CORPORATION. For the details of the affected product names/model numbers, refer to the information provided by the vendor.	7.5	More Details
CVE-2023-33756	An issue in the SpreadSheetPlugin component of Foswiki v2.1.7 and below allows attackers to execute a directory traversal.	7.5	More Details
CVE-2023-38172	Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability	7.5	More Details
CVE-2023-38760	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the role and gender parameters within the /QueryView.php component.	7.5	More Details
CVE-2023-38762	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the friendmonths parameter within the /QueryView.php.	7.5	More Details
CVE-2023-38764	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the birthmonth and percls parameters within the /QueryView.php.	7.5	More Details
CVE-2023-38765	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the membermonth parameter within the /QueryView.php.	7.5	More Details
CVE-2023-38767	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the 'value' and 'custom' parameters within the /QueryView.php.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38768	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the PropertyID parameter within the /QueryView.php.	7.5	More Details
CVE-2023-38769	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the searchstring and searchwhat parameters within the /QueryView.php.	7.5	More Details
CVE-2023-38770	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the group parameter within the /QueryView.php.	7.5	More Details
CVE-2023-35383	Microsoft Message Queuing Information Disclosure Vulnerability	7.5	More Details
CVE-2023-38744	Denial-of-service (DoS) vulnerability due to improper validation of specified type of input issue exists in the built-in EtherNet/IP port of the CJ Series CJ2 CPU unit and the communication function of the CS/CJ Series EtherNet/IP unit. If an affected product receives a packet which is specially crafted by a remote unauthenticated attacker, the unit of the affected product may fall into a denial-of-service (DoS) condition. Affected products/versions are as follows: CJ2M CPU Unit CJ2M-CPU3[] Unit version of the built-in EtherNet/IP section Ver. 2.18 and earlier, CJ2H CPU Unit CJ2H-CPU6[]-EIP Unit version of the built-in EtherNet/IP section Ver. 3.04 and earlier, CS/CJ Series EtherNet/IP Unit CS1W-EIP21 V3.04 and earlier, and CS/CJ Series EtherNet/IP Unit CJ1W-EIP21 V3.04 and earlier.	7.5	More Details
CVE-2023-38955	ZKTeco BioAccess IVS v3.3.1 allows unauthenticated attackers to obtain sensitive information about all managed devices, including their IP addresses and device names.	7.5	More Details
CVE-2023-38956	A path traversal vulnerability in ZKTeco BioAccess IVS v3.3.1 allows unauthenticated attackers to read arbitrary files via supplying a crafted payload.	7.5	More Details
CVE-2023-38138	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2023-0956	External input could be used on TEL-STER TelWin SCADA WebInterface to construct paths to files and directories without properly neutralizing special elements within the pathname, which could allow an unauthenticated attacker to read files on the system.	7.5	More Details
CVE-2023-33370	An uncaught exception vulnerability exists in Control ID IDSecure 4.7.26.0 and prior, allowing attackers to cause the main web server of IDSecure to fault and crash, causing a denial of service.	7.5	More Details
CVE-2022-46485	Data Illusion Survey Software Solutions ngSurvey version 2.4.28 and below is vulnerable to Denial of Service if a survey contains a "Text Field", "Comment Field" or "Contact Details".	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26451	Functions with insufficient randomness were used to generate authorization tokens of the integrated oAuth Authorization Service. Authorization codes were predictable for third parties and could be used to intercept and take over the client authorization process. As a result, other users accounts could be compromised. The oAuth Authorization Service is not enabled by default. We have updated the implementation to use sources with sufficient randomness to generate authorization tokens. No publicly available exploits are known.	7.5	More Details
CVE-2023-38771	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the volopp parameter within the /QueryView.php.	7.5	More Details
CVE-2023-33363	An authentication bypass vulnerability exists in Suprema BioStar 2 before 2.9.1, which allows unauthenticated users to access some functionality on BioStar 2 servers.	7.5	More Details
CVE-2023-33365	A path traversal vulnerability exists in Suprema BioStar 2 before 2.9.1, which allows unauthenticated attackers to fetch arbitrary files from the server's web server.	7.5	More Details
CVE-2023-36873	.NET Framework Spoofing Vulnerability	7.4	More Details
CVE-2023-2754	The Cloudflare WARP client for Windows assigns loopback IPv4 addresses for the DNS Servers, since WARP acts as local DNS server that performs DNS queries in a secure manner, however, if a user is connected to WARP over an IPv6-capable network, te WARP client did not assign loopback IPv6 addresses but Unique Local Addresses, which under certain conditions could point towards unknown devices in the same local network which enables an Attacker to view DNS queries made by the device.	7.4	More Details
CVE-2023-4136	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CrafterCMS Engine on Windows, MacOS, Linux, x86, ARM, 64 bit allows Reflected XSS.This issue affects CrafterCMS: from 4.0.0 through 4.0.2, from 3.1.0 through 3.1.27.	7.4	More Details
CVE-2023-4219	A vulnerability was found in SourceCodester Doctors Appointment System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation of the argument useremail leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-236365 was assigned to this vulnerability.	7.3	More Details
CVE-2023-36540	Untrusted search path in the installer for Zoom Desktop Client for Windows before 5.14.5 may allow an authenticated user to enable an escalation of privilege via local access.	7.3	More Details
CVE-2023-4180	A vulnerability classified as critical was found in SourceCodester Free Hospital Management System for Small Practices 1.0. Affected by this vulnerability is an unknown functionality of the file /vm/login.php. The manipulation of the argument useremail/userpassword leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-236215.	7.3	More Details
CVE-2023-4182	A vulnerability, which was classified as critical, was found in SourceCodester Inventory Management System 1.0. This affects an unknown part of the file edit_sell.php. The manipulation of the argument up_pid leads to sql injection. It is possible to initiate the attack remotely. The identifier VDB-236217 was assigned to this vulnerability.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4184	A vulnerability was found in SourceCodester Inventory Management System 1.0 and classified as critical. This issue affects some unknown processing of the file sell_return.php. The manipulation of the argument pid leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-236219.	7.3	More Details
CVE-2023-3662	In CODESYS Development System versions from 3.5.17.0 and prior to 3.5.19.20 a vulnerability allows for execution of binaries from the current working directory in the users context .	7.3	More Details
CVE-2023-37570	This vulnerability exists in ESDS Emagic Data Center Management Suit due to non-expiry of session cookie. By reusing the stolen cookie, a remote attacker could gain unauthorized access to the targeted system.	7.2	More Details
CVE-2020-23564	File Upload vulnerability in SEMCMS 3.9 allows remote attackers to run arbitrary code via SEMCMS_Upfile.php.	7.2	More Details
CVE-2023-4009	In MongoDB Ops Manager v5.0 prior to 5.0.22 and v6.0 prior to 6.0.17 it is possible for an authenticated user with project owner or project user admin access to generate an API key with the privileges of org owner resulting in privilege escalation.	7.2	More Details
CVE-2023-21411	User provided input is not sanitized in the “Settings > Access Control” configuration interface allowing for arbitrary code execution.	7.2	More Details
CVE-2023-21410	User provided input is not sanitized on the AXIS License Plate Verifier specific “api.cgi” allowing for arbitrary code execution.	7.2	More Details
CVE-2023-38167	Microsoft Dynamics 365 Business Central Elevation of Privilege Vulnerability	7.2	More Details
CVE-2023-21412	User provided input is not sanitized on the AXIS License Plate Verifier specific “search.cgi” allowing for SQL injections.	7.2	More Details
CVE-2023-33913	In DRM/oemcrypto, there is a possible out of bounds write due to an incorrect calculation of buffer size.This could lead to remote escalation of privilege with System execution privileges needed	7.2	More Details
CVE-2023-39121	emlog v2.1.9 was discovered to contain a SQL injection vulnerability via the component /admin/user.php.	7.2	More Details
CVE-2023-37687	Online Nurse Hiring System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the View Request of Nurse Page in the Admin portal.	7.2	More Details
CVE-2023-35081	A path traversal vulnerability in Ivanti EPMM versions (11.10.x < 11.10.0.3, 11.9.x < 11.9.1.2 and 11.8.x < 11.8.1.2) allows an authenticated administrator to write arbitrary files onto the appliance.	7.2	More Details
CVE-2023-36220	Directory Traversal vulnerability in Textpattern CMS v4.8.8 allows a remote authenticated attacker to execute arbitrary code and gain access to sensitive information via the plugin Upload function.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38947	An arbitrary file upload vulnerability in the /languages/install.php component of WBCE CMS v1.6.1 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2023-38948	An arbitrary file download vulnerability in the /c/PluginsController.php component of jizhi CMS 1.9.5 allows attackers to execute arbitrary code via downloading a crafted plugin.	7.2	More Details
CVE-2023-36876	Reliability Analysis Metrics Calculation (RacTask) Elevation of Privilege Vulnerability	7.1	More Details
CVE-2023-36535	Client-side enforcement of server-side security in Zoom clients before 5.14.10 may allow an authenticated user to enable information disclosure via network access.	7.1	More Details
CVE-2023-3749	A local user could edit the VideoEdge configuration file and interfere with VideoEdge operation.	7.1	More Details
CVE-2023-32503	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in GTmetrix GTmetrix for WordPress plugin <= 0.4.6 versions.	7.1	More Details
CVE-2023-33993	B1i module of SAP Business One - version 10.0, application allows an authenticated user with deep knowledge to send crafted queries over the network to read or modify the SQL data. On successful exploitation, the attacker can cause high impact on confidentiality, integrity and availability of the application.	7.1	More Details
CVE-2023-27421	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Everest themes Everest News theme <= 1.1.0 versions.	7.1	More Details
CVE-2023-37873	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WooCommerce Shipping Multiple Addresses plugin <= 3.8.5 versions.	7.1	More Details
CVE-2023-36689	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WPFactory WPFactory Helper plugin <= 1.5.2 versions.	7.1	More Details
CVE-2023-36686	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in CartFlows Pro plugin <= 1.11.11 versions.	7.1	More Details
CVE-2023-36858	An insufficient verification of data vulnerability exists in BIG-IP Edge Client for Windows and macOS that may allow an attacker to modify its configured server list. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.1	More Details
CVE-2023-31926	System files could be overwritten using the less command in Brocade Fabric OS before Brocade Fabric OS v9.1.1c and v9.2.0.	7.1	More Details
CVE-2023-36533	Uncontrolled resource consumption in Zoom SDKs before 5.14.7 may allow an unauthenticated user to enable a denial of service via network access.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30491	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in CodeBard CodeBard's Patron Button and Widgets for Patreon plugin <= 2.1.8 versions.	7.1	More Details
CVE-2023-24409	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution WP Responsive Tabs horizontal vertical and accordion Tabs plugin <= 1.1.15 versions.	7.1	More Details
CVE-2023-38392	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Hiroaki Miyashita Custom Field Template plugin <= 2.5.9 versions.	7.1	More Details
CVE-2023-27412	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Everest themes Mocho Blog theme <= 1.0.4 versions.	7.1	More Details
CVE-2023-25600	An issue was discovered in InsydeH2O. A malicious operating system can tamper with a runtime-writable EFI variable, leading to out-of-bounds memory reads and a denial of service. This is fixed in version 01.01.04.0016.	7.1	More Details
CVE-2023-26440	The cacheservice API could be abused to indirectly inject parameters with SQL syntax which was insufficiently sanitized and would later be executed when creating new cache groups. Attackers with access to a local or restricted network could perform arbitrary SQL queries. We have improved the input check for API calls and filter for potentially malicious content. No publicly available exploits are known.	7.1	More Details
CVE-2023-24413	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution WordPress vertical image slider plugin <= 1.2.16 versions.	7.1	More Details
CVE-2023-38384	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Syntactics, Inc. EaSYNC plugin <= 1.3.7 versions.	7.1	More Details
CVE-2023-21626	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	7.1	More Details
CVE-2023-27627	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in eggemplo Woocommerce Email Report plugin <= 2.4 versions.	7.1	More Details
CVE-2023-26317	Xiaomi routers have an external interface that can lead to command injection. The vulnerability is caused by lax filtering of responses from external interfaces. Attackers can exploit this vulnerability to gain access to the router by hijacking the ISP or upper-layer routing.	7.0	More Details
CVE-2023-35378	Windows Projected File System Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-38176	Azure Arc-Enabled Servers Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30297	An issue found in N-able Technologies N-central Server before 2023.4 allows a local attacker to execute arbitrary code via the monitoring function of the server.	7.0	More Details
CVE-2023-3492	The WP Shopping Pages WordPress plugin through 1.14 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	6.8	More Details
CVE-2023-20589	An attacker with specialized hardware and physical access to an impacted device may be able to perform a voltage fault injection attack resulting in compromise of the ASP secure boot potentially leading to arbitrary code execution.	6.8	More Details
CVE-2023-39528	PrestaShop is an open source e-commerce web application. Prior to version 8.1.1, the `displayAjaxEmailHTML` method can be used to read any file on the server, potentially even outside of the project if the server is not correctly configured. Version 8.1.1 contains a patch for this issue. There are no known workarounds.	6.8	More Details
CVE-2023-39523	ScanCode.io is a server to script and automate software composition analysis with ScanPipe pipelines. Prior to version 32.5.1, the software has a possible command injection vulnerability in the docker fetch process as it allows to append malicious commands in the `docker_reference` parameter. In the function `scanpipe/pipes/fetch.py:fetch_docker_image` the parameter `docker_reference` is user controllable. The `docker_reference` variable is then passed to the vulnerable function `get_docker_image_platform`. However, the `get_docker_image_plaform` function constructs a shell command with the passed `docker_reference`. The `pipes.run_command` then executes the shell command without any prior sanitization, making the function vulnerable to command injections. A malicious user who is able to create or add inputs to a project can inject commands. Although the command injections are blind and the user will not receive direct feedback without logs, it is still possible to cause damage to the server/container. The vulnerability appears for example if a malicious user adds a semicolon after the input of `docker://;`, it would allow appending malicious commands. Version 32.5.1 contains a patch for this issue. The `docker_reference` input should be sanitized to avoid command injections and, as a workaround, one may avoid creating commands with user controlled input directly.	6.8	More Details
CVE-2023-20783	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905.	6.7	More Details
CVE-2023-20814	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560.	6.7	More Details
CVE-2023-20817	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600.	6.7	More Details
CVE-2023-20786	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811.	6.7	More Details
CVE-2023-20815	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20795	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900.	6.7	More Details
CVE-2023-20811	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061.	6.7	More Details
CVE-2023-20805	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326411.	6.7	More Details
CVE-2023-20816	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589.	6.7	More Details
CVE-2023-20797	In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629582; Issue ID: ALPS07629582.	6.7	More Details
CVE-2023-20808	In OPTEE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: DTV03645895.	6.7	More Details
CVE-2023-20809	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198.	6.7	More Details
CVE-2023-20804	In imgsys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07199773; Issue ID: ALPS07326384.	6.7	More Details
CVE-2023-20784	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989.	6.7	More Details
CVE-2023-20806	In hcp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07537437.	6.7	More Details
CVE-2023-21650	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length.	6.7	More Details
CVE-2023-20807	In dpe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608433; Issue ID: ALPS07608433.	6.7	More Details
CVE-2023-39529	PrestaShop is an open source e-commerce web application. Prior to version 8.1.1, it is possible to delete a file from the server by using the Attachments controller and the Attachments API. Version 8.1.1 contains a patch for this issue. There are no known workarounds.	6.7	More Details
CVE-2023-21627	Memory corruption in Trusted Execution Environment while calling service API with invalid address.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39524	PrestaShop is an open source e-commerce web application. Prior to version 8.1.1, SQL injection possible in the product search field, in BO's product page. Version 8.1.1 contains a patch for this issue. There are no known workarounds.	6.7	More Details
CVE-2023-21648	Memory corruption in RIL while trying to send apdu packet.	6.7	More Details
CVE-2023-21649	Memory corruption in WLAN while running doDriverCmd for an unspecific command.	6.7	More Details
CVE-2023-28575	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it.	6.7	More Details
CVE-2023-28577	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address.	6.7	More Details
CVE-2023-4140	The WP Ultimate CSV Importer plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 7.9.8 due to insufficient restriction on the 'get_header_values' function. This makes it possible for authenticated attackers, with minimal permissions such as an author, if the administrator previously grants access in the plugin settings, to modify their user role by supplying the 'wp_capabilities->cus1' parameter.	6.6	More Details
CVE-2023-36893	Microsoft Outlook Spoofing Vulnerability	6.5	More Details
CVE-2023-35376	Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability	6.5	More Details
CVE-2023-35377	Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability	6.5	More Details
CVE-2023-35389	Microsoft Dynamics 365 On-Premises Remote Code Execution Vulnerability	6.5	More Details
CVE-2023-36890	Microsoft SharePoint Server Information Disclosure Vulnerability	6.5	More Details
CVE-2023-38924	Netgear DGN3500 1.1.00.37 was discovered to contain a buffer overflow via the http_password parameter at setup.cgi.	6.5	More Details
CVE-2023-36136	PHPJabbers Class Scheduling System 1.0 lacks encryption on the password when editing a user account (update user page) allowing an attacker to capture all user names and passwords in clear text.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36894	Microsoft SharePoint Server Information Disclosure Vulnerability	6.5	More Details
CVE-2023-36908	Windows Hyper-V Information Disclosure Vulnerability	6.5	More Details
CVE-2023-36909	Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability	6.5	More Details
CVE-2023-36913	Microsoft Message Queuing Information Disclosure Vulnerability	6.5	More Details
CVE-2023-38254	Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability	6.5	More Details
CVE-2023-38763	SQL injection vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to obtain sensitive information via the FundRaiserID parameter within the /FundRaiserEditor.php endpoint.	6.5	More Details
CVE-2023-23877	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in bkmacdaddy designs Pinterest RSS Widget plugin <= 2.3.1 versions.	6.5	More Details
CVE-2023-30482	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in VillaTheme WPBulky plugin <= 1.0.10 versions.	6.5	More Details
CVE-2023-28773	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Kolja Nolte Secondary Title plugin <= 2.0.9.1 versions.	6.5	More Details
CVE-2023-23880	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in ExactMetrics plugin <= 7.14.1 versions.	6.5	More Details
CVE-2022-38795	In Gitea through 1.17.1, repo cloning can occur in the migration function.	6.5	More Details
CVE-2023-23829	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Pierre JEHAN Owl Carousel plugin <= 0.5.3 versions.	6.5	More Details
CVE-2022-45821	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in NooTheme Noo Timetable plugin <= 2.1.3 versions.	6.5	More Details
CVE-2023-29099	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Elegant themes Divi theme <= 4.20.2 versions.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21647	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation.	6.5	More Details
CVE-2023-38157	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	6.5	More Details
CVE-2023-36054	lib/kadm5/kadm_rpc_xdr.c in MIT Kerberos 5 (aka krb5) before 1.20.2 and 1.21.x before 1.21.1 frees an uninitialized pointer. A remote authenticated user can trigger a kadmind crash. This occurs because _xdr_kadm5_principal_ent_rec does not validate the relationship between n_key_data and the key_data array count.	6.5	More Details
CVE-2023-39530	PrestaShop is an open source e-commerce web application. Prior to version 8.1.1, it is possible to delete files from the server via the CustomerMessage API. Version 8.1.1 contains a patch for this issue. There are no known workarounds.	6.5	More Details
CVE-2023-39525	PrestaShop is an open source e-commerce web application. Prior to version 8.1.1, in the back office, files can be compromised using path traversal by replaying the import file deletion query with a specified file path that uses the traversal path. Version 8.1.1 contains a patch for this issue. There are no known workarounds.	6.5	More Details
CVE-2023-0632	An issue has been discovered in GitLab affecting all versions starting from 15.2 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A Regular Expression Denial of Service was possible by using crafted payloads to search Harbor Registry.	6.5	More Details
CVE-2023-39951	OpenTelemetry Java Instrumentation provides OpenTelemetry auto-instrumentation and instrumentation libraries for Java. OpenTelemetry Java Instrumentation prior to version 1.28.0 contains an issue related to the instrumentation of Java applications using the AWS SDK v2 with Amazon Simple Email Service (SES) v1 API. When SES POST requests are instrumented, the query parameters of the request are inserted into the trace `url.path` field. This behavior leads to the http body, containing the email subject and message, to be present in the trace request url metadata. Any user using a version before 1.28.0 of OpenTelemetry Java Instrumentation to instrument AWS SDK v2 call to SES's v1 SendEmail API is affected. The e-mail content sent to SES may end up in telemetry backend. This exposes the e-mail content to unintended audiences. The issue can be mitigated by updating OpenTelemetry Java Instrumentation to version 1.28.0 or later.	6.5	More Details
CVE-2023-20803	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07326455; Issue ID: ALPS07326374.	6.5	More Details
CVE-2023-37546	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550	6.5	More Details
CVE-2023-37548	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37549 and CVE-2023-37550	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37549	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37550	6.5	More Details
CVE-2023-37550	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548 and CVE-2023-37549.	6.5	More Details
CVE-2023-37551	In multiple Codesys products in multiple versions, after successful authentication as a user, specially crafted network communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller.	6.5	More Details
CVE-2023-37552	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37553, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556.	6.5	More Details
CVE-2023-37553	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37554, CVE-2023-37555 and CVE-2023-37556.	6.5	More Details
CVE-2023-37554	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37555 and CVE-2023-37556.	6.5	More Details
CVE-2023-37555	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37556.	6.5	More Details
CVE-2023-37556	In multiple versions of multiple Codesys products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37552, CVE-2023-37553, CVE-2023-37554 and CVE-2023-37555.	6.5	More Details
CVE-2023-37557	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37558	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37559	6.5	More Details
CVE-2023-37559	After successful authentication as a user in multiple Codesys products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37558	6.5	More Details
CVE-2023-4190	Insufficient Session Expiration in GitHub repository admidio/admidio prior to 4.2.11.	6.5	More Details
CVE-2023-32600	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Rank Math SEO plugin <= 1.0.119 versions.	6.5	More Details
CVE-2022-26838	Path traversal vulnerability in Importing Mobile Device Data of Cybozu Remote Service 3.1.2 allows a remote authenticated attacker to cause a denial-of-service (DoS) condition.	6.5	More Details
CVE-2023-28468	An issue was discovered in FvbServicesRuntimeDxe in Insyde InsydeH2O with kernel 5.0 through 5.5. The FvbServicesRuntimeDxe SMM module exposes an SMI handler that allows an attacker to interact with the SPI flash at run-time from the OS.	6.5	More Details
CVE-2023-20802	In imgsys, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420976.	6.5	More Details
CVE-2023-4138	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.8.0.	6.5	More Details
CVE-2023-30950	The foundry campaigns service was found to be vulnerable to an unauthenticated information disclosure in a rest endpoint	6.5	More Details
CVE-2020-26065	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system.	6.5	More Details
CVE-2022-4955	Inappropriate implementation in DevTools in Google Chrome prior to 108.0.5359.71 allowed an attacker who convinced a user to install a malicious extension to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38487	HedgeDoc is software for creating real-time collaborative markdown notes. Prior to version 1.9.9, the API of HedgeDoc 1 can be used to create notes with an alias matching the ID of existing notes. The affected existing note can then not be accessed anymore and is effectively hidden by the new one. When the freeURL feature is enabled (by setting the `allowFreeURL` config option or the `CMD_ALLOW_FREEURL` environment variable to `true`), any user with the appropriate permissions can create a note by making a POST request to the `/new/<ALIAS>` API endpoint. The `<ALIAS>` parameter can be set to the ID of an existing note. HedgeDoc did not verify whether the provided `<ALIAS>` value corresponds to a valid ID of an existing note and always allowed creation of the new note. When a visitor tried to access the existing note, HedgeDoc will first search for a note with a matching alias before it searches using the ID, therefore only the new note can be accessed. Depending on the permission settings of the HedgeDoc instance, the issue can be exploited only by logged-in users or by all (including non-logged-in) users. The exploit requires knowledge of the ID of the target note. Attackers could use this issue to present a manipulated copy of the original note to the user, e.g. by replacing the links with malicious ones. Attackers can also use this issue to prevent access to the original note, causing a denial of service. No data is lost, as the original content of the affected notes is still present in the database. This issue was fixed in version 1.9.9. As a workaround, disabling freeURL mode prevents the exploitation of this issue. The impact can be limited by restricting freeURL note creation to trusted, logged-in users by enabling `requireFreeURLAuthentication`/`CMD_REQUIRE_FREEURL_AUTHENTICATION`.	6.5	More Details
CVE-2022-41401	OpenRefine <= v3.5.2 contains a Server-Side Request Forgery (SSRF) vulnerability, which permits unauthorized users to exploit the system, potentially leading to unauthorized access to internal resources and sensitive file disclosure.	6.5	More Details
CVE-2023-39112	ECShop v4.1.16 contains an arbitrary file deletion vulnerability in the Admin Panel.	6.5	More Details
CVE-2023-38332	Zoho ManageEngine ADManager Plus through 7201 allow authenticated users to take over another user's account via sensitive information disclosure.	6.5	More Details
CVE-2023-37547	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37545, CVE-2023-37546, CVE-2023-37548, CVE-2023-37549 and CVE-2023-37550	6.5	More Details
CVE-2023-38695	cypress-image-snapshot shows visual regressions in Cypress with jest-image-snapshot. Prior to version 8.0.2, it's possible for a user to pass a relative file path for the snapshot name and reach outside of the project directory into the machine running the test. This issue has been patched in version 8.0.2.	6.5	More Details
CVE-2023-37545	In multiple Codesys products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition. This vulnerability is different to CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550	6.5	More Details
CVE-2023-4124	Missing Authorization in GitHub repository answerdev/answer prior to v1.1.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3329	SpiderControl SCADA Webserver versions 2.08 and prior are vulnerable to path traversal. An attacker with administrative privileges could overwrite files on the webserver using the HMI's upload file feature. This could create size zero files anywhere on the webserver, potentially overwriting system files and creating a denial-of-service condition.	6.5	More Details
CVE-2023-33368	Some API routes exists in Control ID IDSecure 4.7.26.0 and prior, exfiltrating sensitive information and passwords to users accessing these API routes.	6.5	More Details
CVE-2023-29408	The TIFF decoder does not place a limit on the size of compressed tile data. A maliciously-crafted image can exploit this to cause a small image (both in terms of pixel width/height, and encoded size) to make the decoder decode large amounts of compressed data, consuming excessive memory and CPU.	6.5	More Details
CVE-2023-29407	A maliciously-crafted image can cause excessive CPU consumption in decoding. A tiled image with a height of 0 and a very large width can cause excessive CPU consumption, despite the image size (width * height) appearing to be zero.	6.5	More Details
CVE-2023-20800	In imgsys, there is a possible system crash due to a mssing ptr check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420955.	6.5	More Details
CVE-2023-20788	In thermal, 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 needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735.	6.4	More Details
CVE-2023-20787	In thermal, 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 needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734.	6.4	More Details
CVE-2023-20801	In imgsys, 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 needed for exploitation. Patch ID: ALPS07420968; Issue ID: ALPS07420968.	6.4	More Details
CVE-2023-20785	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524.	6.4	More Details
CVE-2023-28576	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues.	6.4	More Details
CVE-2023-38708	Pimcore is an Open Source Data & Experience Management Platform: PIM, MDM, CDP, DAM, DXP/CMS & Digital Commerce. A path traversal vulnerability exists in the `AssetController::importServerFilesAction`, which allows an attacker to overwrite or modify sensitive files by manipulating the pimcore_log parameter.This can lead to potential denial of service---key file overwrite. The impact of this vulnerability allows attackers to: overwrite or modify sensitive files, potentially leading to unauthorized access, privilege escalation, or disclosure of confidential information. This could also cause a denial of service (DoS) if critical system files are overwritten or deleted.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4169	A vulnerability was found in Ruijie RG-EW1200G 1.0(1)B1P5. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /api/sys/set_passwd of the component Administrator Password Handler. The manipulation leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-236185 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-30951	The Foundry Magritte plugin rest-source was found to be vulnerable to an an XML external Entity attack (XXE).	6.3	More Details
CVE-2023-3385	An issue has been discovered in GitLab affecting all versions starting from 8.10 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. Under specific circumstances, a user importing a project 'from export' could access and read unrelated files via uploading a specially crafted file. This was due to a bug in `tar`, fixed in [`tar-1.35`] (https://lists.gnu.org/archive/html/info-gnu/2023-07/msg00005.html).	6.3	More Details
CVE-2023-36869	Azure DevOps Server Spoofing Vulnerability	6.3	More Details
CVE-2023-31928	A reflected cross-site scripting (XSS) vulnerability exists in Brocade Webtools PortSetting.html of Brocade Fabric OS version before Brocade Fabric OS v9.2.0 that could allow a remote unauthenticated attacker to execute arbitrary JavaScript code in a target user's session with the Brocade Webtools application.	6.3	More Details
CVE-2023-4176	A vulnerability was found in SourceCodester Hospital Management System 1.0. It has been classified as critical. This affects an unknown part of the file appointmentapproval.php. The manipulation of the argument time leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-236211.	6.3	More Details
CVE-2023-4201	A vulnerability was found in SourceCodester Inventory Management System 1.0 and classified as critical. This issue affects some unknown processing of the file ex_catagory_data.php. The manipulation of the argument columns[1][data] leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-236291.	6.3	More Details
CVE-2023-4200	A vulnerability has been found in SourceCodester Inventory Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file product_data.php.. The manipulation of the argument columns[1][data] leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-236290 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-4179	A vulnerability classified as critical has been found in SourceCodester Free Hospital Management System for Small Practices 1.0. Affected is an unknown function of the file /vm/doctor/doctors.php?action=view. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-236214 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-4191	A vulnerability, which was classified as critical, has been found in SourceCodester Resort Reservation System 1.0. Affected by this issue is some unknown functionality of the file index.php. The manipulation of the argument page leads to file inclusion. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-236234 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4199	A vulnerability, which was classified as critical, was found in SourceCodester Inventory Management System 1.0. This affects an unknown part of the file catagory_data.php. The manipulation of the argument columns[1][data] leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-236289 was assigned to this vulnerability.	6.3	More Details
CVE-2023-4120	A vulnerability was found in Byzoro Smart S85F Management Platform up to 20230722 and classified as critical. This issue affects some unknown processing of the file importhtml.php. The manipulation of the argument sql leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235967. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-4192	A vulnerability, which was classified as critical, was found in SourceCodester Resort Reservation System 1.0. This affects an unknown part of the file manage_user.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-236235.	6.3	More Details
CVE-2023-4121	A vulnerability was found in Byzoro Smart S85F Management Platform up to 20230722. It has been classified as critical. Affected is an unknown function. The manipulation of the argument file_upload leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235968. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-4193	A vulnerability has been found in SourceCodester Resort Reservation System 1.0 and classified as critical. This vulnerability affects unknown code of the file view_fee.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-236236.	6.3	More Details
CVE-2023-4186	A vulnerability was found in SourceCodester Pharmacy Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file manage_website.php. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-236221 was assigned to this vulnerability.	6.3	More Details
CVE-2023-4185	A vulnerability was found in SourceCodester Online Hospital Management System 1.0. It has been classified as critical. Affected is an unknown function of the file patientlogin.php. The manipulation of the argument loginid/password leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-236220.	6.3	More Details
CVE-2023-35391	ASP.NET Core SignalR and Visual Studio Information Disclosure Vulnerability	6.2	More Details
CVE-2023-38964	Creative Item Academy LMS 6.0 was discovered to contain a cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2023-38761	Cross Site Scripting (XSS) vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to execute arbitrary code via a crafted payload to the systemSettings.php component.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38045	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in advcomsys.com oneVote component for Joomla. It allows XSS Targeting Non-Script Elements.	6.1	More Details
CVE-2023-3524	The WPCode WordPress plugin before 2.0.13.1 does not escape generated URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting	6.1	More Details
CVE-2023-36159	Cross Site Scripting (XSS) vulnerability in sourcecodester Lost and Found Information System 1.0 allows remote attackers to run arbitrary code via the First Name, Middle Name and Last Name fields on the Create User page.	6.1	More Details
CVE-2023-36158	Cross Site Scripting (XSS) vulnerability in sourcecodester Toll Tax Management System 1.0 allows remote attackers to run arbitrary code via the First Name and Last Name fields on the My Account page.	6.1	More Details
CVE-2023-36138	PHPJabbers Cleaning Business Software 1.0 is vulnerable to Cross Site Scripting (XSS) via the theme parameter of preview.php.	6.1	More Details
CVE-2023-36137	There is a Cross Site Scripting (XSS) vulnerability in the "theme" parameter of preview.php in PHPJabbers Class Scheduling System 1.0.	6.1	More Details
CVE-2020-20808	Cross Site Scripting vulnerability in Qibosoft qibosoft v.7 and before allows a remote attacker to execute arbitrary code via the eindtijd and starttijd parameters of do/search.php.	6.1	More Details
CVE-2023-39218	Client-side enforcement of server-side security in Zoom clients before 5.14.10 may allow a privileged user to enable information disclosure via network access.	6.1	More Details
CVE-2023-20181	A vulnerability in the web-based management interface of Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to conduct XSS attacks. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2023-4067	The Bus Ticket Booking with Seat Reservation plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab_date' and 'tab_date_r' parameters in versions up to, and including, 5.2.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-3671	The MultiParcels Shipping For WooCommerce WordPress plugin before 1.15.4 does not sanitise and escape various parameters before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-3978	Text nodes not in the HTML namespace are incorrectly literally rendered, causing text which should be escaped to not be. This could lead to an XSS attack.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3652	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Digital Ant E-Commerce Software allows Reflected XSS.This issue affects E-Commerce Software: before 11.	6.1	More Details
CVE-2023-36306	A Cross Site Scripting (XSS) vulnerability in Adiscon Aiscon LogAnalyzer through 4.1.13 allows a remote attacker to execute arbitrary code via the asktheoracle.php, details.php, index.php, search.php, export.php, reports.php, and statistics.php components.	6.1	More Details
CVE-2023-37488	In SAP NetWeaver Process Integration - versions SAP_XIESR 7.50, SAP_XITOOL 7.50, SAP_XIAF 7.50, user-controlled inputs, if not sufficiently encoded, could result in Cross-Site Scripting (XSS) attack. On successful exploitation the attacker can cause limited impact on confidentiality and integrity of the system.	6.1	More Details
CVE-2023-26316	A XSS vulnerability exists in the Xiaomi cloud service Application product. The vulnerability is caused by Webview's whitelist checking function allowing javascript protocol to be loaded and can be exploited by attackers to steal Xiaomi cloud service account's cookies.	6.1	More Details
CVE-2023-3180	A flaw was found in the QEMU virtual crypto device while handling data encryption/decryption requests in virtio_crypto_handle_sym_req. There is no check for the value of `src_len` and `dst_len` in virtio_crypto_sym_op_helper, potentially leading to a heap buffer overflow when the two values differ.	6.0	More Details
CVE-2023-4135	A heap out-of-bounds memory read flaw was found in the virtual nvme device in QEMU. The QEMU process does not validate an offset provided by the guest before computing a host heap pointer, which is used for copying data back to the guest. Arbitrary heap memory relative to an allocated buffer can be disclosed.	6.0	More Details
CVE-2023-3470	Specific F5 BIG-IP platforms with Cavium Nitrox FIPS HSM cards generate a deterministic password for the Crypto User account. The predictable nature of the password allows an authenticated user with TMSH access to the BIG-IP system, or anyone with physical access to the FIPS HSM, the information required to generate the correct password. On vCMP systems, all Guests share the same deterministic password, allowing those with TMSH access on one Guest to access keys of a different Guest. The following BIG-IP hardware platforms are affected: 10350v-F, i5820-DF, i7820-DF, i15820-DF, 5250v-F, 7200v-F, 10200v-F, 6900-F, 8900-F, 11000-F, and 11050-F. The BIG-IP rSeries r5920-DF and r10920-DF are not affected, nor does the issue affect software FIPS implementations or network HSM configurations. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.0	More Details
CVE-2023-39209	Improper input validation in Zoom Desktop Client for Windows before 5.15.5 may allow an authenticated user to enable an information disclosure via network access.	5.9	More Details
CVE-2023-36532	Buffer overflow in Zoom Clients before 5.14.5 may allow an unauthenticated user to enable a denial of service via network access.	5.9	More Details
CVE-2023-38494	MeterSphere is an open-source continuous testing platform. Prior to version 2.10.4 LTS, some interfaces of the Cloud version of MeterSphere do not have configuration permissions, and are sensitively leaked by attackers. Version 2.10.4 LTS contains a patch for this issue.	5.9	More Details
CVE-2023-32292	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in GetButton Chat Button by GetButton.Io plugin <= 1.8.9.4 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25063	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Anadnet Quick Page/Post Redirect Plugin plugin <= 5.2.3 versions.	5.9	More Details
CVE-2023-3373	Predictable Exact Value from Previous Values vulnerability in Mitsubishi Electric Corporation GOT2000 Series GT21 model versions 01.49.000 and prior and GOT SIMPLE Series GS21 model versions 01.49.000 and prior allows a remote unauthenticated attacker to hijack data connections (session hijacking) or prevent legitimate users from establishing data connections (to cause DoS condition) by guessing the listening port of the data connection on FTP server and connecting to it.	5.9	More Details
CVE-2023-28934	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Mammothology WP Full Stripe Free plugin <= 1.6.1 versions.	5.9	More Details
CVE-2023-28931	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Never5 Post Connector plugin <= 1.0.9 versions.	5.9	More Details
CVE-2023-4127	Race Condition within a Thread in GitHub repository answerdev/answer prior to v1.1.1.	5.9	More Details
CVE-2023-25984	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Rigorous & Factory Pattern Dovetail plugin <= 1.2.13 versions.	5.9	More Details
CVE-2023-3766	A vulnerability was discovered in the odoh-rs rust crate that stems from faulty logic during the parsing of encrypted queries. This issue specifically occurs when processing encrypted query data received from remote clients and enables an attacker with knowledge of this vulnerability to craft and send specially designed encrypted queries to targeted ODOH servers running with odoh-rs. Upon successful exploitation, the server will crash abruptly, disrupting its normal operation and rendering the service temporarily unavailable.	5.9	More Details
CVE-2023-27416	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Decon Digital Decon WP SMS plugin <= 1.1 versions.	5.9	More Details
CVE-2023-27422	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in NsThemes NS Coupon To Become Customer plugin <= 1.2.2 versions.	5.9	More Details
CVE-2023-27415	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Themeqx LetterPress plugin <= 1.1.2 versions.	5.9	More Details
CVE-2023-36692	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Christian Kramer & Hendrik Thole WP-Cirrus plugin <= 0.6.11 versions.	5.9	More Details
CVE-2023-31221	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Ransom Christofferson PDQ CSV plugin <= 1.0.0 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25459	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Postsnippets Post Snippets plugin <= 4.0.2 versions.	5.9	More Details
CVE-2023-34377	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Joseph C Dolson My Content Management plugin <= 1.7.6 versions.	5.9	More Details
CVE-2023-39903	An issue was discovered in Fujitsu Software Infrastructure Manager (ISM) before 2.8.0.061. The ismsnap component (in this specific case at /var/log/fujitsu/ServerViewSuite/ism/FirmwareManagement/FirmwareManagement.log) allows insecure collection and storage of authorization credentials in cleartext. That occurs when users perform any ISM Firmware Repository Address setup test (Test the Connection), or regularly authorize against an already configured remote firmware repository site, as set up in ISM Firmware Repository Address. A privileged attacker is therefore able to potentially gather the associated ismsnap maintenance data, in the same manner as a trusted party allowed to export ismsnap data from ISM. The preconditions for an ISM installation to be generally vulnerable are that the Download Firmware (Firmware Repository Server) function is enabled and configured, and that the character \ (backslash) is used in a user credential (i.e., user/ID or password) of the remote proxy host / firmware repository server. NOTE: this may overlap CVE-2023-39379.	5.9	More Details
CVE-2023-36678	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WP-buy WP Content Copy Protection & No Right Click plugin <= 3.5.5 versions.	5.9	More Details
CVE-2023-37874	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Dimitar Ivanov HTTP Headers plugin <= 1.18.11 versions.	5.9	More Details
CVE-2023-37486	Under certain conditions SAP Commerce (OCC API) - versions HY_COM 2105, HY_COM 2205, COM_CLOUD 2211, endpoints allow an attacker to access information which would otherwise be restricted. On successful exploitation there could be a high impact on confidentiality with no impact on integrity and availability of the application.	5.9	More Details
CVE-2023-39363	Vyper is a Pythonic Smart Contract Language for the Ethereum Virtual Machine (EVM). In versions 0.2.15, 0.2.16 and 0.3.0, named re-entrancy locks are allocated incorrectly. Each function using a named re-entrancy lock gets a unique lock regardless of the key, allowing cross-function re-entrancy in contracts compiled with the susceptible versions. A specific set of conditions is required to result in misbehavior of affected contracts, specifically: a `.vy` contract compiled with `vyper` versions `0.2.15`, `0.2.16`, or `0.3.0`; a primary function that utilizes the `@nonreentrant` decorator with a specific `key` and does not strictly follow the check-effects-interaction pattern (i.e. contains an external call to an untrusted party before storage updates); and a secondary function that utilizes the same `key` and would be affected by the improper state caused by the primary function. Version 0.3.1 contains a fix for this issue.	5.9	More Details
CVE-2023-39436	SAP Supplier Relationship Management -versions 600, 602, 603, 604, 605, 606, 616, 617, allows an unauthorized attacker to discover information relating to SRM within Vendor Master Data for Business Partners replication functionality.This information could be used to allow the attacker to specialize their attacks against SRM.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20215	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked. This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device.	5.8	More Details
CVE-2023-20218	A vulnerability in web-based management interface of Cisco SPA500 Series Analog Telephone Adapters (ATAs) could allow an authenticated, remote attacker to to modify a web page in the context of a user's browser. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious websites, or the attacker could use this vulnerability to conduct further client-side attacks. Cisco will not release software updates that address this vulnerability. {{value}} ["%7b%7bvalue%7d%7d"])}]]	5.8	More Details
CVE-2023-34010	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in submodule of David Lingren Media Library Assistant plugin <= 3.0.7 versions.	5.8	More Details
CVE-2020-26082	A vulnerability in the zip decompression engine of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass content filters that are configured on an affected device. The vulnerability is due to improper handling of password-protected zip files. An attacker could exploit this vulnerability by sending a malicious file inside a crafted zip-compressed file to an affected device. A successful exploit could allow the attacker to bypass configured content filters that would normally drop the email.	5.8	More Details
CVE-2023-38697	protocol-http1 provides a low-level implementation of the HTTP/1 protocol. RFC 9112 Section 7.1 defined the format of chunk size, chunk data and chunk extension. The value of Content-Length header should be a string of 0-9 digits, the chunk size should be a string of hex digits and should split from chunk data using CRLF, and the chunk extension shouldn't contain any invisible character. However, Falcon has following behaviors while disobey the corresponding RFCs: accepting Content-Length header values that have `+` prefix, accepting Content-Length header values that written in hexadecimal with `0x` prefix, accepting `0x` and `+` prefixed chunk size, and accepting LF in chunk extension. This behavior can lead to desync when forwarding through multiple HTTP parsers, potentially results in HTTP request smuggling and firewall bypassing. This issue is fixed in `protocol-http1` v0.15.1. There are no known workarounds.	5.8	More Details
CVE-2023-38690	matrix-appservice-irc is a Node.js IRC bridge for Matrix. Prior to version 1.0.1, it is possible to craft a command with newlines which would not be properly parsed. This would mean you could pass a string of commands as a channel name, which would then be run by the IRC bridge bot. Versions 1.0.1 and above are patched. There are no robust workarounds to the bug. One may disable dynamic channels in the config to disable the most common execution method but others may exist.	5.8	More Details
CVE-2023-3894	Those using jackson-dataformats-text to parse TOML data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3348	The Wrangler command line tool (<=wrangler@3.1.0 or <=wrangler@2.20.1) was affected by a directory traversal vulnerability when running a local development server for Pages (wrangler pages dev command). This vulnerability enabled an attacker in the same network as the victim to connect to the local development server and access the victim's files present outside of the directory for the development server.	5.7	More Details
CVE-2023-26441	Cacheservice did not correctly check if relative cache object were pointing to the defined absolute location when accessing resources. An attacker with access to the database and a local or restricted network would be able to read arbitrary local file system resources that are accessible by the services system user account. We have improved path validation and make sure that any access is contained to the defined root directory. No publicly available exploits are known.	5.7	More Details
CVE-2023-26443	Full-text autocomplete search allows user-provided SQL syntax to be injected to SQL statements. With existing sanitization in place, this can be abused to trigger benign SQL Exceptions but could potentially be escalated to a malicious SQL injection vulnerability. We now properly encode single quotes for SQL FULLTEXT queries. No publicly available exploits are known.	5.5	More Details
CVE-2023-33909	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-4132	A use-after-free vulnerability was found in the siano smsusb module in the Linux kernel. The bug occurs during device initialization when the siano device is plugged in. This flaw allows a local user to crash the system, causing a denial of service condition.	5.5	More Details
CVE-2023-31428	Brocade Fabric OS before Brocade Fabric OS v9.1.1c, v9.2.0 contains a vulnerability in the command line that could allow a local user to dump files under user's home directory using grep.	5.5	More Details
CVE-2023-31430	A buffer overflow vulnerability in “secpolicydelete” command in Brocade Fabric OS before Brocade Fabric OS v9.1.1c and v9.2.0 could allow an authenticated privileged user to crash the Brocade Fabric OS switch leading to a denial of service.	5.5	More Details
CVE-2023-39210	Cleartext storage of sensitive information in Zoom Client SDK for Windows before 5.15.0 may allow an authenticated user to enable an information disclosure via local access.	5.5	More Details
CVE-2023-31431	A buffer overflow vulnerability in “diagstatus” command in Brocade Fabric OS before Brocade Fabric v9.2.0 and v9.1.1c could allow an authenticated user to crash the Brocade Fabric OS switch leading to a denial of service.	5.5	More Details
CVE-2023-39520	Cryptomator encrypts data being stored on cloud infrastructure. The MSI installer provided on the homepage for Cryptomator version 1.9.2 allows local privilege escalation for low privileged users, via the `repair` function. The problem occurs as the repair function of the MSI is spawning an SYSTEM Powershell without the `-NoProfile` parameter. Therefore the profile of the user starting the repair will be loaded. Version 1.9.3 contains a fix for this issue. Adding a `-NoProfile` to the powershell is a possible workaround.	5.5	More Details
CVE-2023-33906	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33907	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2022-2346	In affected versions of Octopus Deploy it is possible for a low privileged guest user to interact with extension endpoints.	5.5	More Details
CVE-2023-33908	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-20556	Insufficient validation of the IOCTL (Input Output Control) input buffer in AMD µProf may allow an authenticated user to send an arbitrary buffer potentially resulting in a Windows crash leading to denial of service.	5.5	More Details
CVE-2023-36907	Windows Cryptographic Services Information Disclosure Vulnerability	5.5	More Details
CVE-2023-20561	Insufficient validation of the IOCTL (Input Output Control) input buffer in AMD µProf may allow an authenticated user to send an arbitrary address potentially resulting in a Windows crash leading to denial of service.	5.5	More Details
CVE-2023-33910	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-33911	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-33912	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-27373	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. Due to insufficient input validation, an attacker can tamper with a runtime-accessible EFI variable to cause a dynamic BAR setting to overlap SMRAM.	5.5	More Details
CVE-2022-2416	In affected versions of Octopus Deploy it is possible for a low privileged guest user to craft a request that allows enumeration/recon of an environment.	5.5	More Details
CVE-2023-39114	ngiflib commit 84a75 was discovered to contain a segmentation violation via the function SDL_LoadAnimatedGif at ngiflibSDL.c. This vulnerability is triggered when running the program SDLaffgif.	5.5	More Details
CVE-2023-39113	ngiflib commit fb271 was discovered to contain a segmentation violation via the function "main" at gif2tag.c. This vulnerability is triggered when running the program gif2tga.	5.5	More Details
CVE-2023-36914	Windows Smart Card Resource Management Server Security Feature Bypass Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36889	Windows Group Policy Security Feature Bypass Vulnerability	5.5	More Details
CVE-2023-36905	Windows Wireless Wide Area Network Service (WwanSvc) Information Disclosure Vulnerability	5.5	More Details
CVE-2023-36906	Windows Cryptographic Services Information Disclosure Vulnerability	5.5	More Details
CVE-2023-4194	A flaw was found in the Linux kernel's TUN/TAP functionality. This issue could allow a local user to bypass network filters and gain unauthorized access to some resources. The original patches fixing CVE-2023-1076 are incorrect or incomplete. The problem is that the following upstream commits - a096ccca6e50 ("tun: tun_chr_open(): correctly initialize socket uid"), - 66b2c338adce ("tap: tap_open(): correctly initialize socket uid"), pass "inode->i_uid" to sock_init_data_uid() as the last parameter and that turns out to not be accurate.	5.5	More Details
CVE-2023-20588	A division-by-zero error on some AMD processors can potentially return speculative data resulting in loss of confidentiality.	5.5	More Details
CVE-2023-4133	A use-after-free vulnerability was found in the cxgb4 driver in the Linux kernel. The bug occurs when the cxgb4 device is detaching due to a possible rearming of the flower_stats_timer from the work queue. This flaw allows a local user to crash the system, causing a denial of service condition.	5.5	More Details
CVE-2023-4166	A vulnerability has been found in Tongda OA and classified as critical. This vulnerability affects unknown code of the file general/system/seal_manage/dianju/delete_log.php. The manipulation of the argument DELETE_STR leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. VDB-236182 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-4165	A vulnerability, which was classified as critical, was found in Tongda OA. This affects an unknown part of the file general/system/seal_manage/iweboffice/delete_seal.php. The manipulation of the argument DELETE_STR leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-236181 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-38991	An issue in the delete function in the ActModelController class of jeesite v1.2.6 allows authenticated attackers to arbitrarily delete models created by the Administrator.	5.4	More Details
CVE-2023-39096	WebBoss.io CMS v3.7.0.1 contains a stored Cross-Site Scripting (XSS) vulnerability due to lack of input validation and output encoding.	5.4	More Details
CVE-2023-36081	Cross Site Scripting vulnerability in GatesAIr Flexiva FM Transmitter/Exciter v.FAX 150W allows a remote attacker to execute arbitrary code via a crafted script to the web application dashboard.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3575	The Quiz And Survey Master WordPress plugin before 8.1.11 does not properly sanitize and escape question titles, which could allow users with the Contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-36121	Cross Site Scripting vulnerability in e107 v.2.3.2 allows a remote attacker to execute arbitrary code via the description function in the SEO project.	5.4	More Details
CVE-2023-39518	social-media-skeleton is an uncompleted social media project implemented using PHP, MySQL, CSS, JavaScript, and HTML. Versions 1.0.0 until 1.0.3 have a stored cross-site scripting vulnerability. The problem is patched in v1.0.3.	5.4	More Details
CVE-2023-4158	Cross-site Scripting (XSS) - Stored in GitHub repository omeka/omeka-s prior to 4.0.3.	5.4	More Details
CVE-2023-3653	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Digital Ant E-Commerce Software allows Stored XSS.This issue affects E-Commerce Software: before 11.	5.4	More Details
CVE-2023-26445	Frontend themes are defined by user-controllable jslob settings and could point to a malicious resource which gets processed during login. Malicious script code can be executed within the victims context. This can lead to session hijacking or triggering unwanted actions via the web interface and API. To exploit this an attacker would require temporary access to the users account or lure a user to a compromised account. We now sanitize the theme value and use a default fallback if no theme matches. No publicly available exploits are known.	5.4	More Details
CVE-2023-38758	Cross Site Scripting vulnerability in wger Project wger Workout Manager v.2.2.0a3 allows a remote attacker to gain privileges via the license_author field in the add-ingredient function in the templates/ingredients/view.html, models/ingredients.py, and views/ingredients.py components.	5.4	More Details
CVE-2023-38423	A cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.4	More Details
CVE-2023-4196	Cross-site Scripting (XSS) - Stored in GitHub repository cockpit-hq/cockpit prior to 2.6.3.	5.4	More Details
CVE-2023-37581	Insufficient input validation and sanitation in Weblog Category name, Website About and File Upload features in all versions of Apache Roller on all platforms allows an authenticated user to perform an XSS attack. Mitigation: if you do not have Roller configured for untrusted users, then you need to do nothing because you trust your users to author raw HTML and other web content. If you are running with untrusted users then you should upgrade to Roller 6.1.2 and you should disable Roller's File Upload feature.	5.4	More Details
CVE-2023-20204	A vulnerability in the web-based management interface of Cisco BroadWorks CommPilot Application Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4181	A vulnerability, which was classified as critical, has been found in SourceCodester Free Hospital Management System for Small Practices 1.0. Affected by this issue is some unknown functionality of the file /vm/admin/delete-doctor.php?id=2 of the component Redirect Handler. The manipulation leads to enforcement of behavioral workflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-236216.	5.4	More Details
CVE-2023-39097	WebBoss.io CMS v3.7.0.1 contains a stored cross-site scripting (XSS) vulnerability.	5.4	More Details
CVE-2023-26446	The users clientID at "application passwords" was not sanitized or escaped before being added to DOM. Malicious script code can be executed within the victims context. This can lead to session hijacking or triggering unwanted actions via the web interface and API. To exploit this an attacker would require temporary access to the users account or lure a user to a compromised account. We now sanitize the user-controllable clientID parameter. No publicly available exploits are known.	5.4	More Details
CVE-2023-38766	Cross Site Scripting (XSS) vulnerability in ChurchCRM v.5.0.0 allows a remote attacker to execute arbitrary code via a crafted payload to the PersonView.php component.	5.4	More Details
CVE-2023-26447	The "upsell" widget for the portal allows to specify a product description. This description taken from a user-controllable jslob did not get escaped before being added to DOM. Malicious script code can be executed within the victims context. This can lead to session hijacking or triggering unwanted actions via the web interface and API. To exploit this an attacker would require temporary access to the users account or lure a user to a compromised account. We now sanitize jslob content. No publicly available exploits are known.	5.4	More Details
CVE-2023-26448	Custom log-in and log-out locations are used-defined as jslob but were not checked to contain malicious protocol handlers. Malicious script code can be executed within the victims context. This can lead to session hijacking or triggering unwanted actions via the web interface and API. To exploit this an attacker would require temporary access to the users account or lure a user to a compromised account. We now sanitize jslob content for those locations to avoid redirects to malicious content. No publicly available exploits are known.	5.4	More Details
CVE-2023-26449	The "OX Chat" web service did not specify a media-type when processing responses by external resources. Malicious script code can be executed within the victims context. This can lead to session hijacking or triggering unwanted actions via the web interface and API. To exploit this an attacker would require temporary access to the users account or lure a user to a compromised account. We are now defining the accepted media-type to avoid code execution. No publicly available exploits are known.	5.4	More Details
CVE-2023-26450	The "OX Count" web service did not specify a media-type when processing responses by external resources. Malicious script code can be executed within the victims context. This can lead to session hijacking or triggering unwanted actions via the web interface and API. To exploit this an attacker would require temporary access to the users account or lure a user to a compromised account. We are now defining the accepted media-type to avoid code execution. No publicly available exploits are known.	5.4	More Details
CVE-2023-4145	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/customer-data-framework prior to 3.4.2.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33257	Verint Engagement Management 15.3 Update 2023R2 is vulnerable to HTML injection via the user data form in the live chat.	5.4	More Details
CVE-2023-35384	Windows HTML Platforms Security Feature Bypass Vulnerability	5.4	More Details
CVE-2023-2164	An issue has been discovered in GitLab affecting all versions starting from 15.9 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible for an attacker to trigger a stored XSS vulnerability via user interaction with a crafted URL in the WebIDE beta.	5.4	More Details
CVE-2023-0604	The WP Food Manager WordPress plugin before 1.0.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	5.4	More Details
CVE-2023-34038	VMware Horizon Server contains an information disclosure vulnerability. A malicious actor with network access may be able to access information relating to the internal network configuration.	5.3	More Details
CVE-2023-34037	VMware Horizon Server contains a HTTP request smuggling vulnerability. A malicious actor with network access may be able to perform HTTP smuggle requests.	5.3	More Details
CVE-2023-4008	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.9 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible to takeover GitLab Pages with unique domain URLs if the random string added was known.	5.3	More Details
CVE-2023-36141	User enumeration is found in in PHPJabbers Cleaning Business Software 1.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	5.3	More Details
CVE-2023-33383	Shelly 4PM Pro four-channel smart switch 0.11.0 allows an attacker to trigger a BLE out of bounds read fault condition that results in a device reload.	5.3	More Details
CVE-2023-38958	An access control issue in ZKTeco BioAccess IVS v3.3.1 allows unauthenticated attackers to arbitrarily close and open the doors managed by the platform remotely via sending a crafted web request.	5.3	More Details
CVE-2023-38330	OXID eShop Enterprise Edition 6.5.0 – 6.5.2 before 6.5.3 allows uploading files with modified headers in the administration area. An attacker can upload a file with a modified header to create a HTTP Response Splitting attack.	5.3	More Details
CVE-2023-39217	Improper input validation in Zoom SDK's before 5.14.10 may allow an unauthenticated user to enable a denial of service via network access.	5.3	More Details
CVE-2023-4002	An issue has been discovered in GitLab EE affecting all versions starting from 14.1 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible for EE-licensed users to link any security policy project by its ID to projects or groups the user has access to, potentially revealing the security projects's configured security policies.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37373	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.4). The affected applications accept unauthenticated file write messages. An unauthenticated remote attacker could write arbitrary files to the affected application's file system.	5.3	More Details
CVE-2023-37487	SAP Business One (Service Layer) - version 10.0, allows an authenticated attacker with deep knowledge perform certain operation to access unintended data over the network which could lead to high impact on confidentiality with no impact on integrity and availability of the application	5.3	More Details
CVE-2023-37484	SAP PowerDesigner - version 16.7, queries all password hashes in the backend database and compares it with the user provided one during login attempt, which might allow an attacker to access password hashes from the client's memory.	5.3	More Details
CVE-2023-29409	Extremely large RSA keys in certificate chains can cause a client/server to expend significant CPU time verifying signatures. With fix, the size of RSA keys transmitted during handshakes is restricted to <= 8192 bits. Based on a survey of publicly trusted RSA keys, there are currently only three certificates in circulation with keys larger than this, and all three appear to be test certificates that are not actively deployed. It is possible there are larger keys in use in private PKIs, but we target the web PKI, so causing breakage here in the interests of increasing the default safety of users of crypto/tls seems reasonable.	5.3	More Details
CVE-2023-31927	An information disclosure in the web interface of Brocade Fabric OS versions before Brocade Fabric OS v9.2.0 and v9.1.1c, could allow a remote unauthenticated attacker to get technical details about the web interface.	5.3	More Details
CVE-2023-4157	CWE-74 Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') in GitHub repository omeka/omeka-s prior to version 4.0.3.	5.2	More Details
CVE-2023-30952	A security defect was discovered in Foundry Issues that enabled users to create convincing phishing links by editing the request sent when creating an Issue. This defect was resolved in Frontend release 6.228.0 .	5.0	More Details
CVE-2023-38691	matrix-appservice-bridge provides an API for setting up bridges. Starting in version 4.0.0 and prior to versions 8.1.2 and 9.0.1, a malicious Matrix server can use a foreign user's MXID in an OpenID exchange, allowing a bad actor to impersonate users when using the provisioning API. The library does not check that the servername part of the `sub` parameter (containing the user's *claimed* MXID) is the the same as the servername we are talking to. A malicious actor could spin up a server on any given domain, respond with a `sub` parameter according to the user they want to act as and use the resulting token to perform provisioning requests. Versions 8.1.2 and 9.0.1 contain a patch. As a workaround, disable the provisioning API.	5.0	More Details
CVE-2023-0264	A flaw was found in Keycloaks OpenID Connect user authentication, which may incorrectly authenticate requests. An authenticated attacker who could obtain information from a user request within the same realm could use that data to impersonate the victim and generate new session tokens. This issue could impact confidentiality, integrity, and availability.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38698	Ethereum Name Service (ENS) is a distributed, open, and extensible naming system based on the Ethereum blockchain. According to the documentation, controllers are allowed to register new domains and extend the expiry of existing domains, but they cannot change the ownership or reduce the expiration time of existing domains. However, a preliminary analysis suggests that an attacker-controlled controller may be able to reduce the expiration time of existing domains due to an integer overflow in the renew function. The vulnerability resides `@ensdomains/ens-contracts` prior to version 0.0.22. If successfully exploited, this vulnerability would enable attackers to force the expiration of any ENS record, ultimately allowing them to claim the affected domains for themselves. Currently, it would require a malicious DAO to exploit it. Nevertheless, any vulnerability present in the controllers could potentially render this issue exploitable in the future. An additional concern is the possibility of renewal discounts. Should ENS decide to implement a system that offers unlimited .eth domains for a fixed fee in the future, the vulnerability could become exploitable by any user due to the reduced attack cost. Version 0.0.22 contains a patch for this issue. As long as registration cost remains linear or superlinear based on registration duration, or limited to a reasonable maximum (eg, 1 million years), this vulnerability could only be exploited by a malicious DAO. The interim workaround is thus to take no action.	4.9	More Details
CVE-2023-37492	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack.	4.9	More Details
CVE-2023-3569	In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an authenticated remote attacker with admin privileges could upload a crafted XML file which causes a denial-of-service.	4.9	More Details
CVE-2023-3993	An issue has been discovered in GitLab EE affecting all versions starting from 14.3 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. Access tokens may have been logged when a query was made to a specific endpoint.	4.9	More Details
CVE-2023-37690	Maid Hiring Management System v1.0 was discovered to contain a SQL injection vulnerability in the Search Maid page.	4.8	More Details
CVE-2023-3401	An issue has been discovered in GitLab affecting all versions before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. The main branch of a repository with a specially designed name allows an attacker to create repositories with malicious code.	4.8	More Details
CVE-2023-3650	The Bubble Menu WordPress plugin before 3.0.5 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in multisite setup).	4.8	More Details
CVE-2023-37683	Online Nurse Hiring System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the Profile Page of the Admin.	4.8	More Details
CVE-2023-37684	Online Nurse Hiring System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the Search Report Details of the Admin portal.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37685	Online Nurse Hiring System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the Search Report Page of the Admin portal.	4.8	More Details
CVE-2023-37686	Online Nurse Hiring System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the Add Nurse Page in the Admin portal.	4.8	More Details
CVE-2023-37688	Maid Hiring Management System v1.0 was discovered to contain a SQL injection vulnerability in the Admin page.	4.8	More Details
CVE-2023-37689	Maid Hiring Management System v1.0 was discovered to contain a SQL injection vulnerability in the Booking Request page.	4.8	More Details
CVE-2023-4189	Cross-site Scripting (XSS) - Reflected in GitHub repository instantsoft/icms2 prior to 2.16.1-git.	4.8	More Details
CVE-2023-26961	Alteryx Server 2022.1.1.42590 does not employ file type verification for uploaded files. This vulnerability allows attackers to upload arbitrary files (e.g., JavaScript content for stored XSS) via the type field in a JSON document within a PUT /gallery/api/media request.	4.8	More Details
CVE-2023-3500	An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.0 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. A reflected XSS was possible when creating specific PlantUML diagrams that allowed the attacker to perform arbitrary actions on behalf of victims.	4.8	More Details
CVE-2023-4187	Cross-site Scripting (XSS) - Stored in GitHub repository instantsoft/icms2 prior to 2.16.1-git.	4.8	More Details
CVE-2023-30958	A security defect was identified in Foundry Frontend that enabled users to potentially conduct DOM XSS attacks if Foundry's CSP were to be bypassed. This defect was resolved with the release of Foundry Frontend 6.225.0.	4.7	More Details
CVE-2023-20569	A side channel vulnerability on some of the AMD CPUs may allow an attacker to influence the return address prediction. This may result in speculative execution at an attacker-controlled address, potentially leading to information disclosure.	4.7	More Details
CVE-2023-39075	Renault Zoe EV 2021 automotive infotainment system versions 283C35202R to 283C35519R (builds 11.10.2021 to 16.01.2023) allows attackers to crash the infotainment system by sending arbitrary USB data via a USB device.	4.6	More Details
CVE-2023-35394	Azure HDInsight Jupyter Notebook Spoofing Vulnerability	4.6	More Details
CVE-2023-35393	Azure Apache Hive Spoofing Vulnerability	4.5	More Details
CVE-2023-36881	Azure Apache Ambari Spoofing Vulnerability	4.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36877	Azure Apache Oozie Spoofing Vulnerability	4.5	More Details
CVE-2023-38188	Azure Apache Hadoop Spoofing Vulnerability	4.5	More Details
CVE-2023-36494	Audit logs on F5OS-A may contain undisclosed sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.4	More Details
CVE-2023-20818	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540.	4.4	More Details
CVE-2023-20793	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818.	4.4	More Details
CVE-2023-20796	In power, there is a possible memory corruption due to an incorrect bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07929790; Issue ID: ALPS07929790.	4.4	More Details
CVE-2023-20798	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076.	4.4	More Details
CVE-2023-20813	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549.	4.4	More Details
CVE-2023-20812	In wlan driver, there is a possible out of bounds write due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944987; Issue ID: ALPS07944987.	4.4	More Details
CVE-2023-20810	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061.	4.4	More Details
CVE-2023-39440	In SAP BusinessObjects Business Intelligence - version 420, If a user logs in to a particular program, under certain specific conditions memory might not be cleared up properly, due to which attacker might be able to get access to user credentials. For a successful attack, the attacker needs to have local access to the system. There is no impact on availability and integrity.	4.4	More Details
CVE-2023-20790	In nvram, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07740194; Issue ID: ALPS07740194.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20216	A vulnerability in the privilege management functionality of all Cisco BroadWorks server types could allow an authenticated, local attacker to elevate privileges to root on an affected system. This vulnerability is due to incorrect implementation of user role permissions. An attacker could exploit this vulnerability by authenticating to the application as a user with the BWORKS or BWSUPERADMIN role and issuing crafted commands on an affected system. A successful exploit could allow the attacker to execute commands beyond the sphere of their intended access level, including initiating installs or running operating system commands with elevated permissions. There are workarounds that address this vulnerability.	4.4	More Details
CVE-2023-20782	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550103.	4.4	More Details
CVE-2023-20781	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323.	4.4	More Details
CVE-2023-20789	In jpeg, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07693193; Issue ID: ALPS07693193.	4.4	More Details
CVE-2023-20780	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS08017756.	4.4	More Details
CVE-2022-47350	In camera driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2022-47351	In camera driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-4172	A vulnerability, which was classified as problematic, has been found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0. This issue affects some unknown processing of the file \Service\FileHandler.ashx. The manipulation of the argument FileDirectory leads to absolute path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-236207.	4.3	More Details
CVE-2023-36482	An issue was discovered in Samsung NFC S3NRN4V, S3NSN4V, S3NSEN4, SEN82AB, and S3NRN82. A buffer copy without checking its input size can cause an NFC service restart.	4.3	More Details
CVE-2023-4119	A vulnerability has been found in Academy LMS 6.0 and classified as problematic. This vulnerability affects unknown code of the file /academy/home/courses. The manipulation of the argument query/sort_by leads to cross site scripting. The attack can be initiated remotely. VDB-235966 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-29505	An issue was discovered in Zoho ManageEngine Network Configuration Manager 12.6.165. The WebSocket endpoint allows Cross-site WebSocket hijacking.	4.3	More Details
CVE-2023-3426	The organization selector in Liferay Portal 7.4.3.81 through 7.4.3.85, and Liferay DXP 7.4 update 81 through 85 does not check user permission, which allows remote authenticated users to obtain a list of all organizations.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26438	External service lookups for a number of protocols were vulnerable to a time-of-check/time-of-use (TOCTOU) weakness, involving the JDK DNS cache. Attackers that were timing DNS cache expiry correctly were able to inject configuration that would bypass existing network deny-lists. Attackers could exploit this weakness to discover the existence of restricted network infrastructure and service availability. Improvements were made to include deny-lists not only during the check of the provided connection data, but also during use. No publicly available exploits are known.	4.3	More Details
CVE-2023-4183	A vulnerability has been found in SourceCodester Inventory Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file edit_update.php of the component Password Handler. The manipulation of the argument user_id leads to improper access controls. The attack can be initiated remotely. VDB-236218 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2023-3900	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. An invalid 'start_sha' value on merge requests page may lead to Denial of Service as Changes tab would not load.	4.3	More Details
CVE-2023-4168	A vulnerability was found in Templatecookie Adlisting 2.14.0. It has been classified as problematic. Affected is an unknown function of the file /ad-list of the component Redirect Handler. The manipulation leads to information disclosure. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-236184. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-4011	An issue has been discovered in GitLab EE affecting all versions from 15.11 prior to 16.2.2 which allows an attacker to spike the resource consumption resulting in DoS.	4.3	More Details
CVE-2023-38990	An issue in the delete function in the MenuController class of jeesite v1.2.6 allows authenticated attackers to arbitrarily delete menus created by the Administrator.	4.3	More Details
CVE-2023-2022	An issue has been discovered in GitLab CE/EE affecting all versions starting before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2, which leads to developers being able to create pipeline schedules on protected branches even if they don't have access to merge	4.3	More Details
CVE-2023-4116	A vulnerability classified as problematic was found in PHP Jabbers Taxi Booking 2.0. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation of the argument index leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-235963. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-4115	A vulnerability classified as problematic has been found in PHP Jabbers Cleaning Business 1.0. Affected is an unknown function of the file /index.php. The manipulation of the argument index leads to cross site scripting. It is possible to launch the attack remotely. VDB-235962 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-4114	A vulnerability was found in PHP Jabbers Night Club Booking Software 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /index.php. The manipulation of the argument index leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-235961 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4113	A vulnerability was found in PHP Jabbers Service Booking Script 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /index.php. The manipulation of the argument index leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-235960. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-4112	A vulnerability was found in PHP Jabbers Shuttle Booking Software 1.0. It has been classified as problematic. This affects an unknown part of the file /index.php. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-235959. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-4111	A vulnerability was found in PHP Jabbers Bus Reservation System 1.1 and classified as problematic. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument index/pickup_id leads to cross site scripting. The attack may be launched remotely. VDB-235958 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-4171	A vulnerability classified as problematic was found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0. This vulnerability affects unknown code of the file \Service\FileDownload.ashx. The manipulation of the argument Files leads to path traversal: '../filedir'. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-236206 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2023-38419	An authenticated attacker with guest privileges or higher can cause the iControl SOAP process to terminate by sending undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.3	More Details
CVE-2023-39343	Sulu is an open-source PHP content management system based on the Symfony framework. It allows over the Admin Login form to detect which user (username, email) exists and which one do not exist. Sulu Installation not using the old Symfony 5.4 security System and previous version are not impacted by this Security issue. The vulnerability has been patched in version 2.5.10.	4.3	More Details
CVE-2023-4117	A vulnerability, which was classified as problematic, has been found in PHP Jabbers Rental Property Booking 2.0. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument index leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-235964. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-25524	NVIDIA Omniverse Workstation Launcher for Windows and Linux contains a vulnerability in the authentication flow, where a user’s access token is displayed in the browser user's address bar. An attacker could use this token to impersonate the user to access launcher resources. A successful exploit of this vulnerability may lead to information disclosure.	4.0	More Details
CVE-2023-36926	Due to missing authentication check in SAP Host Agent - version 7.22, an unauthenticated attacker can set an undocumented parameter to a particular compatibility value and in turn call read functions. This allows the attacker to gather some non-sensitive information about the server. There is no impact on integrity or availability.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39342	Dangerzone is software for converting potentially dangerous PDFs, office documents, or images to safe PDFs. The Dangerzone CLI (`dangerzone-cli` command) logs output from the container where the file sanitization takes place, to the user's terminal. Prior to version 0.4.2, if the container is compromised and can return attacker-controlled strings, then the attacker may be able to spoof messages in the user's terminal or change the window title. Besides logging output from containers, it also logs the names of the files it sanitizes. If these files contain ANSI escape sequences, then the same issue applies. Dangerzone is predominantly a GUI application, so this issue should leave most of our users unaffected. Nevertheless, we always suggest updating to the newest version. This issue is fixed in Dangerzone 0.4.2.	3.6	More Details
CVE-2023-4170	A vulnerability was found in DedeBIZ 6.2.10. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Article Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-236186 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-4173	A vulnerability, which was classified as problematic, was found in mooSocial mooStore 3.1.6. Affected is an unknown function of the file /search/index. The manipulation of the argument q leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-236208.	3.5	More Details
CVE-2023-4175	A vulnerability was found in mooSocial mooTravel 3.1.8 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. The attack may be launched remotely. VDB-236210 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-38700	matrix-appservice-irc is a Node.js IRC bridge for Matrix. Prior to version 1.0.1, it was possible to craft an event such that it would leak part of a targeted message event from another bridged room. This required knowing an event ID to target. Version 1.0.1n fixes this issue. As a workaround, set the `matrixHandler.eventCacheSize` config value to `0`. This workaround may impact performance.	3.5	More Details
CVE-2023-4167	A vulnerability was found in Media Browser Emby Server 4.7.13.0 and classified as problematic. This issue affects some unknown processing of the file /web/. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-236183.	3.5	More Details
CVE-2023-26430	Attackers with access to user accounts can inject arbitrary control characters to SIEVE mail-filter rules. This could be abused to access SIEVE extension that are not allowed by App Suite or to inject rules which would break per-user filter processing, requiring manual cleanup of such rules. We have added sanitization to all mail-filter APIs to avoid forwardning control characters to subsystems. No publicly available exploits are known.	3.5	More Details
CVE-2023-4174	A vulnerability has been found in mooSocial mooStore 3.1.6 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. The attack can be launched remotely. The identifier VDB-236209 was assigned to this vulnerability.	3.5	More Details
CVE-2023-4118	A vulnerability, which was classified as problematic, was found in Cute Http File Server 2.0. This affects an unknown part of the component Search. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235965 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4110	A vulnerability has been found in PHP Jabbers Availability Booking Calendar 5.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation of the argument session_id leads to cross site scripting. The attack can be launched remotely. The identifier VDB-235957 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3669	A missing Brute-Force protection in CODESYS Development System prior to 3.5.19.20 allows a local attacker to have unlimited attempts of guessing the password within an import dialog.	3.3	More Details
CVE-2023-38532	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions < V14.3.0.3). The affected application contains a stack exhaustion vulnerability while parsing a specially crafted X_T file. This could allow an attacker to cause denial of service condition.	3.3	More Details
CVE-2023-38524	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions < V14.3.0.3). The affected applications contain null pointer dereference while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	3.3	More Details
CVE-2023-39978	ImageMagick before 6.9.12-91 allows attackers to cause a denial of service (memory consumption) in Magick::Draw.	3.3	More Details
CVE-2023-26442	In case Cacheservice was configured to use a sproxyd object-storage backend, it would follow HTTP redirects issued by that backend. An attacker with access to a local or restricted network with the capability to intercept and replay HTTP requests to sproxyd (or who is in control of the sproxyd service) could perform a server-side request-forgery attack and make Cacheservice connect to unexpected resources. We have disabled the ability to follow HTTP redirects when connecting to sproxyd resources. No publicly available exploits are known.	3.2	More Details
CVE-2023-1210	An issue has been discovered in GitLab affecting all versions starting from 12.9 before 16.0.8, all versions starting from 16.1 before 16.1.3, all versions starting from 16.2 before 16.2.2. It was possible to leak a user's email via an error message for groups that restrict membership by email domain.	3.1	More Details
CVE-2023-23476	IBM Robotic Process Automation 21.0.0 through 21.0.7.latest is vulnerable to unauthorized access to data due to insufficient authorization validation on some API routes. IBM X-Force ID: 245425.	3.1	More Details
CVE-2023-26979	Bluetens Electrostimulation Device BluetensQ device app version 4.3.15 is vulnerable to Man-in-the-middle attacks in the BLE channel. It allows attackers to decrease or increase the intensity of the stimulator by hijacking the BLE communication.	3.1	More Details
CVE-2023-4177	A vulnerability was found in EmpowerID up to 7.205.0.0. It has been rated as problematic. This issue affects some unknown processing of the component Multi-Factor Authentication Code Handler. The manipulation leads to information disclosure. The complexity of an attack is rather high. The exploitation is known to be difficult. Upgrading to version 7.205.0.1 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-236213 was assigned to this vulnerability.	2.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4016	Under some circumstances, this weakness allows a user who has access to run the “ps” utility on a machine, the ability to write almost unlimited amounts of unfiltered data into the process heap.	2.5	More Details
CVE-2023-38814	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not in the allowed scope of that CNA's CVE ID assignments. Notes: none.	N/A	More Details
CVE-2023-38815	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-40042. Reason: This candidate is a reservation duplicate of CVE-2023-40042. Notes: All CVE users should reference CVE-2023-40042 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-38707	Rejected reason: This CVE has been rejected because of [CNA rule 7.4.7] (https://www.cve.org/ResourcesSupport/AllResources/CNARules#section_7_assignment_rules): ``` 7.4.7 CNAs SHOULD NOT assign CVE IDs to vulnerabilities in products that are not publicly available or licensable. ``` The repository with the vulnerable code is private, and therefore the product is not publicly available.	N/A	More Details
CVE-2023-39552	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-0527. Reason: This candidate is a reservation duplicate of CVE-2023-0527. Notes: All CVE users should reference CVE-2023-0527 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-38812	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-2230	Rejected reason: Accidental Assignment	N/A	More Details
CVE-2023-36546	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-42986	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-39122. Reason: This candidate is a reservation duplicate of CVE-2023-39122. Notes: All CVE users should reference CVE-2023-39122 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-38696	Rejected reason: This CVE has been rejected because it is unclear whether the issue rests in the original repository `microsoft/ContosoAir`, the forked repository `Apetree100122/ContosoAir`, or both. If the Microsoft repository is vulnerable, [Microsoft] (https://www.cve.org/PartnerInformation/ListofPartners/partner/microsoft) is the appropriate CVE Numbering Authority.	N/A	More Details
CVE-2023-39977	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-3268. Reason: This candidate is a reservation duplicate of CVE-2023-3268. Notes: All CVE users should reference CVE-2023-3268 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-4205	Rejected reason: This was deemed as a false positive both by the reporter and upstream kernel.	N/A	More Details