SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 27 July 2022

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-2022-25759	The package convert-svg-core before 0.6.2 are vulnerable to Remote Code Injection via sending an SVG file containing the payload.	9.9	More Details
CVE-2022-32456	Digiwin BPM's function has insufficient validation for user input. An unauthenticated remote attacker can inject arbitrary SQL command to access, modify, delete database or disrupt service.	9.8	More Details
CVE-2022-24083	Password authentication bypass vulnerability for local accounts can be used to bypass local authentication checks.	9.8	More Details
CVE-2022-34981	The PyCrowdTangle package in PyPI before v0.0.1 included a code execution backdoor inserted by a third party.	9.8	More Details
CVE-2022-34982	The eziod package in PyPI before v0.0.1 included a code execution backdoor inserted by a third party.	9.8	More Details
CVE-2022-24657	Goldshell ASIC Miners v2.1.x was discovered to contain hardcoded credentials which allow attackers to remotely connect via the SSH protocol (port 22).	9.8	More Details
CVE-2022-34113	An issue in the component /api/plugin/upload of Dataease v1.11.1 allows attackers to execute arbitrary code via a crafted plugin.	9.8	More Details
CVE-2022-34115	DataEase v1.11.1 was discovered to contain a arbitrary file write vulnerability via the parameter dataSourceId.	9.8	More Details
CVE-2022-36446	software/apt-lib.pl in Webmin before 1.997 lacks HTML escaping for a UI command.	9.8	More Details
CVE-2020-28438	This affects all versions of package deferred-exec. The injection point is located in line 42 in lib/deferred-exec.js	9.8	More Details
CVE-2020-28443	This affects all versions of package sonar-wrapper. The injection point is located in lib/sonarRunner.js.	9.8	More Details
CVE-2020-28445	This affects all versions of package npm-help. The injection point is located in line 13 in index.js file in export.latestVersion() function.	9.8	More Details
CVE-2020-28446	The package ntesseract before 0.2.9 are vulnerable to Command Injection via lib/tesseract.js.	9.8	More Details
CVE-2020-28447	This affects all versions of package xopen. The injection point is located in line 14 in index.js in the exported function xopen(filepath)	9.8	More Details
CVE-2022-35649	The vulnerability was found in Moodle, occurs due to improper input validation when parsing PostScript code. An omitted execution parameter results in a remote code execution risk for sites running GhostScript versions older than 9.50. Successful exploitation of this vulnerability may result in complete compromise of vulnerable system.	9.8	More Details
CVE-2022-35869	This vulnerability allows remote attackers to bypass authentication on affected installations of Inductive Automation Ignition 8.1.15 (b2022030114). Authentication is not required to exploit this vulnerability. The specific flaw exists within com.inductiveautomation.ignition.gateway.web.pages. The issue results from the lack of proper authentication prior to access to functionality. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-17211.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34501	The bin-collection package in PyPI before v0.1 included a code execution backdoor inserted by a third party.	9.8	More Details
CVE-2022-34907	An authentication bypass vulnerability exists in FileWave before 14.6.3 and 14.7.x before 14.7.2. Exploitation could allow an unauthenticated actor to gain access to the system with the highest authority possible and gain full control over the FileWave platform.	9.8	More Details
CVE-2022-34577	A vulnerability in adm.cgi of WAVLINK WN535 G3 M35G3R.V5030.180927 allows attackers to execute arbitrary code via a crafted POST request.	9.8	More Details
CVE-2022-34989	Fruits Bazar v1.0 was discovered to contain a SQL injection vulnerability via the recover_email parameter at user_password_recover.php.	9.8	More Details
CVE-2022-36161	Orange Station 1.0 was discovered to contain a SQL injection vulnerability via the username parameter.	9.8	More Details
CVE-2022-36412	In Zoho ManageEngine SupportCenter Plus before 11023, V3 API requests are vulnerable to authentication bypass. (An API request may, in effect, be executed with the credentials of a user who authenticated in the past.)	9.8	More Details
CVE-2022-29953	The Bently Nevada 3700 series of condition monitoring equipment through 2022-04-29 has a maintenance interface on port 4001/TCP with undocumented, hardcoded credentials. An attacker capable of connecting to this interface can thus trivially take over its functionality.	9.8	More Details
CVE-2022-29958	JTEKT TOYOPUC PLCs through 2022-04-29 do not ensure data integrity. They utilize the unauthenticated CMPLink/TCP protocol for engineering purposes, including downloading projects and control logic to the PLC. Control logic is downloaded to the PLC on a block-by-block basis with a given memory address and a blob of machine code. The logic that is downloaded to the PLC is not cryptographically authenticated, allowing an attacker to execute arbitrary machine code on the PLC's CPU module in the context of the runtime. In the case of the PC10G-CPU, and likely for other CPU modules of the TOYOPUC family, a processor without MPU or MMU is used and this no memory protection or privilege-separation capabilities are available, giving an attacker full control over the CPU.	9.8	More Details
CVE-2022-30273	The Motorola MDLC protocol through 2022-05-02 mishandles message integrity. It supports three security modes: Plain, Legacy Encryption, and New Encryption. In Legacy Encryption mode, traffic is encrypted via the Tiny Encryption Algorithm (TEA) block-cipher in ECB mode. This mode of operation does not offer message integrity and offers reduced confidentiality above the block level, as demonstrated by an ECB Penguin attack against any block ciphers.	9.8	More Details
CVE-2022-31206	The Omron SYSMAC Nx product family PLCs (NJ series, NY series, NX series, and PMAC series) through 2022-005-18 lack cryptographic authentication. These PLCs are programmed using the SYMAC Studio engineering software (which compiles IEC 61131-3 conformant POU code to native machine code for execution by the PLC's runtime). The resulting machine code is executed by a runtime, typically controlled by a real-time operating system. The logic that is downloaded to the PLC does not seem to be cryptographically authenticated, allowing an attacker to manipulate transmitted object code to the PLC and execute arbitrary machine code on the processor of the PLC's CPU module in the context of the runtime. In the case of at least the NJ series, an RTOS and hardware combination is used that would potentially allow for memory protection and privilege separation and thus limit the impact of code execution. However, it was not confirmed whether these sufficiently segment the runtime from the rest of the RTOS.	9.8	More Details
CVE-2022-31207	The Omron SYSMAC Cx product family PLCs (CS series, CJ series, and CP series) through 2022-05-18 lack cryptographic authentication. They utilize the Omron FINS (9600/TCP) protocol for engineering purposes, including downloading projects and control logic to the PLC. This protocol has authentication flaws as reported in FSCT-2022-0057. Control logic is downloaded to PLC volatile memory using the FINS Program Area Read and Program Area Write commands or to non-volatile memory using other commands from where it can be loaded into volatile memory for execution. The logic that is loaded into and executed from the user program area exists in compiled object code form. Upon execution, these object codes are first passed to a dedicated ASIC that determines whether the object code is to be executed by the ASIC or the microprocessor. In the former case, the object code is interpreted by the ASIC whereas in the latter case the object code is passed to the microprocessor for object code interpretation by a ROM interpreter. In the abnormal case where the object code cannot be handled by either, an abnormal condition is triggered and the PLC is halted. The logic that is downloaded to the PLC does not seem to be cryptographically authenticated, thus allowing an attacker to manipulate transmitted object code to the PLC and either execute arbitrary object code commands on the ASIC or on the microprocessor interpreter.	9.8	More Details
CVE-2022-30270	The Motorola ACE1000 RTU through 2022-05-02 has default credentials. It exposes an SSH interface on port 22/TCP. This interface is used for remote maintenance and for SFTP file-transfer operations that are part of engineering software functionality. Access to this interface is controlled by 5 preconfigured accounts (root, abuilder, acelogin, cappl, ace), all of which come with default credentials. Although the ACE1000 documentation mentions the root, abuilder and acelogin accounts and instructs users to change the default credentials, the cappl and ace accounts remain undocumented and thus are unlikely to have their credentials changed.	9.8	More Details
CVE-2022-30271	The Motorola ACE1000 RTU through 2022-05-02 ships with a hardcoded SSH private key and initialization scripts (such as /etc/init.d/sshd_service) only generate a new key if no private-key file exists. Thus, this hardcoded key is likely to be used by default.	9.8	More Details
CVE-2022-30274	The Motorola ACE1000 RTU through 2022-05-02 uses ECB encryption unsafely. It can communicate with an XRT LAN-to-radio gateway by means of an embedded client. Credentials for accessing this gateway are stored after being encrypted with the Tiny Encryption Algorithm (TEA) in ECB mode using a hardcoded key. Similarly, the ACE1000 RTU can route MDLC traffic over Extended Command and Management Protocol (XCMP) and Network Layer (XNL) networks via the MDLC driver. Authentication to the XNL port is protected by TEA in ECB mode using a hardcoded key.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34509	The wikifaces package in PyPI v1.0 included a code execution backdoor inserted by a third party.	9.8	More Details
CVE-2022-34983	The scu-captcha package in PyPI v0.0.1 to v0.0.4 included a code execution backdoor inserted by a third party.	9.8	More Details
CVE-2022-34500	The bin-collect package in PyPI before v0.1 included a code execution backdoor inserted by a third party.	9.8	More Details
CVE-2022-34045	Wavlink WN530HG4 M30HG4.V5030.191116 was discovered to contain a hardcoded encryption/decryption key for its configuration files at /etc_ro/lighttpd/www/cgi-bin/ExportAllSettings.sh.	9.8	More Details
CVE-2022-34604	H3C Magic R200 R200V200R004L02 was discovered to contain a stack overflow via the INTF parameter at /dotrace.asp.	9.8	More Details
CVE-2022-34603	H3C Magic R200 R200V200R004L02 was discovered to contain a stack overflow via the DelDNSHnList interface at /goform/aspForm.	9.8	More Details
CVE-2022-34607	H3C Magic R200 R200V200R004L02 was discovered to contain a stack overflow via the HOST parameter at /doping.asp.	9.8	More Details
CVE-2022-34608	H3C Magic R200 R200V200R004L02 was discovered to contain a stack overflow via the ajaxmsg parameter at /AJAX/ajaxget.	9.8	More Details
CVE-2022-34609	H3C Magic R200 R200V200R004L02 was discovered to contain a stack overflow via the INTF parameter at /doping.asp.	9.8	More Details
CVE-2022-34610	H3C Magic R200 R200V200R004L02 was discovered to contain a stack overflow via the URL /ihomers/app.	9.8	More Details
CVE-2022-34602	H3C Magic R200 R200V200R004L02 was discovered to contain a stack overflow via the ipqos_lanip_editlist interface at /goform/aspForm.	9.8	More Details
CVE-2022-2107	The MiCODUS MV720 GPS tracker API server has an authentication mechanism that allows devices to use a hard-coded master password. This may allow an attacker to send SMS commands directly to the GPS tracker as if they were coming from the GPS owner's mobile number.	9.8	More Details
CVE-2022-2141	SMS-based GPS commands can be executed by MiCODUS MV720 GPS tracker without authentication.	9.8	More Details
CVE-2022-33318	Deserialization of Untrusted Data vulnerability in ICONICS GENESIS64 versions 10.97.1 and prior and Mitsubishi Electric MC Works64 versions 4.04E (10.95.210.01) and prior allows a remote unauthenticated attacker to execute an arbitrary malicious code by sending specially crafted packets to the GENESIS64 server.	9.8	More Details
CVE-2022-2143	The affected product is vulnerable to two instances of command injection, which may allow an attacker to remotely execute arbitrary code.	9.8	More Details
CVE-2022-34605	H3C Magic R200 R200V200R004L02 was discovered to contain a stack overflow via the HOST parameter at /dotrace.asp.	9.8	More Details
CVE-2022-34601	H3C Magic R200 R200V200R004L02 was discovered to contain a stack overflow via the Delstlist interface at /goform/aspForm.	9.8	More Details
CVE-2022-26136	A vulnerability in multiple Atlassian products allows a remote, unauthenticated attacker to bypass Servlet Filters used by first and third party apps. The impact depends on which filters are used by each app, and how the filters are used. This vulnerability can result in authentication bypass and cross-site scripting. Atlassian has released updates that fix the root cause of this vulnerability, but has not exhaustively enumerated all potential consequences of this vulnerability. Atlassian Bamboo versions are affected before 8.0.9, from 8.1.0 before 8.1.8, and from 8.2.0 before 8.2.4. Atlassian Bitbucket versions are affected before 7.6.16, from 7.7.0 before 7.17.8, from 7.18.0 before 7.19.5, from 7.20.0 before 7.20.2, from 7.21.0 before 7.21.2, and versions 8.0.0 and 8.1.0. Atlassian Confluence versions are affected before 7.4.17, from 7.5.0 before 7.13.7, from 7.14.0 before 7.14.3, from 7.15.0 before 7.15.2, from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and version 7.21.0. Atlassian Crowd versions are affected before 4.3.8, from 4.4.0 before 4.4.2, and version 5.0.0. Atlassian Fisheye and Crucible versions before 4.8.10 are affected. Atlassian Jira versions are affected before 8.13.22, from 8.14.0 before 8.20.10, and from 8.21.0 before 8.22.4. Atlassian Jira Service Management versions are affected before 4.13.22, from 4.14.0 before 4.20.10, and from 4.21.0 before 4.22.4.	9.8	More Details
CVE-2022-26138	The Atlassian Questions For Confluence app for Confluence Server and Data Center creates a Confluence user account in the confluence-users group with the username disabledsystemuser and a hardcoded password. A remote, unauthenticated attacker with knowledge of the hardcoded password could exploit this to log into Confluence and access all content accessible to users in the confluence-users group. This user account is created when installing versions 2.7.34, 2.7.35, and 3.0.2 of the app.	9.8	More Details
CVE-2022-20857	Multiple vulnerabilities in Cisco Nexus Dashboard could allow an unauthenticated, remote attacker to execute arbitrary commands, read or upload container image files, or perform a cross-site request forgery attack. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2022-20858	Multiple vulnerabilities in Cisco Nexus Dashboard could allow an unauthenticated, remote attacker to execute arbitrary commands, read or upload container image files, or perform a cross-site request forgery attack. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20861	Multiple vulnerabilities in Cisco Nexus Dashboard could allow an unauthenticated, remote attacker to execute arbitrary commands, read or upload container image files, or perform a cross-site request forgery attack. For more information about these vulnerabilities, see the Details section of this advisory.	9.8	More Details
CVE-2022-34600	H3C Magic R200 R200V200R004L02 was discovered to contain a stack overflow via the EditSTList interface at /goform/aspForm.	9.8	More Details
CVE-2022-33198	Unauthenticated WordPress Options Change vulnerability in Biplob Adhikari's Accordions plugin <= 2.0.2 at WordPress.	9.8	More Details
CVE-2022-34487	Unauthenticated Arbitrary Option Update vulnerability in biplob018's Shortcode Addons plugin <= 3.0.2 at WordPress.	9.8	More Details
CVE-2022-34599	H3C Magic R200 R200V200R004L02 was discovered to contain a stack overflow via the EdittriggerList interface at /goform/aspForm.	9.8	More Details
CVE-2022-34606	H3C Magic R200 R200V200R004L02 was discovered to contain a stack overflow via the EditvsList parameter at /dotrace.asp.	9.8	More Details
CVE-2022-1309	Insufficient policy enforcement in developer tools in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2022-1312	Use after free in storage in Google Chrome prior to 100.0.4896.88 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	9.6	More Details
CVE-2022-0973	Use after free in Safe Browsing in Google Chrome prior to 99.0.4844.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	9.6	More Details
CVE-2022-0977	Use after free in Browser UI in Google Chrome on Chrome OS prior to 99.0.4844.74 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.	9.6	More Details
CVE-2020-28435	This affects all versions of package ffmpeg-sdk. The injection point is located in line 9 in index.js.	9.4	More Details
CVE-2022-33965	Multiple Unauthenticated SQL Injection (SQLi) vulnerabilities in Osamaesh WP Visitor Statistics plugin <= 5.7 at WordPress.	9.3	More Details
CVE-2022-33319	Out-of-bounds Read vulnerability in ICONICS GENESIS64 versions 10.97.1 and prior and Mitsubishi Electric MC Works64 versions 4.04E (10.95.210.01) and prior allows a remote unauthenticated attacker to disclose information on memory or cause a Denial of Service (DoS) condition by sending specially crafted packets to the GENESIS64 server.	9.1	More Details
CVE-2022-29952	Bently Nevada condition monitoring equipment through 2022-04-29 mishandles authentication. It utilizes the TDI command and data protocols (60005/TCP, 60007/TCP) for communications between the monitoring controller and System 1 and/or Bently Nevada Monitor Configuration (BNMC) software. These protocols provide configuration management and historical data related functionality. Neither protocol has any authentication features, allowing any attacker capable of communicating with the ports in question to invoke (a subset of) desired functionality.	9.1	More Details
CVE-2022-29951	JTEKT TOYOPUC PLCs through 2022-04-29 mishandle authentication. They utilize the CMPLink/TCP protocol (configurable on ports 1024-65534 on either TCP or UDP) for a wide variety of engineering purposes such as starting and stopping the PLC, downloading and uploading projects, and changing configuration settings. This protocol does not have any authentication features, allowing any attacker capable of communicating with the port in question to invoke (a subset of) desired functionality.	9.1	More Details
CVE-2022-0670	A flaw was found in Openstack manilla owning a Ceph File system "share", which enables the owner to read/write any manilla share or entire file system. The vulnerability is due to a bug in the "volumes" plugin in Ceph Manager. This allows an attacker to compromise Confidentiality and Integrity of a file system. Fixed in RHCS 5.2 and Ceph 17.2.2.	9.1	More Details
CVE-2022-28700	Authenticated Arbitrary File Creation via Export function vulnerability in GiveWP's GiveWP plugin <= 2.20.2 at WordPress.	9.1	More Details
CVE-2022-30998	Multiple Authenticated (subscriber or higher user role) SQL Injection (SQLi) vulnerabilities in WooPlugins.co's Homepage Product Organizer for WooCommerce plugin <= 1.1 at WordPress.	9.1	More Details
CVE-2022-36129	HashiCorp Vault Enterprise 1.7.0 through 1.9.7, 1.10.4, and 1.11.0 clusters using Integrated Storage expose an unauthenticated API endpoint that could be abused to override the voter status of a node within a Vault HA cluster, introducing potential for future data loss or catastrophic failure. Fixed in Vault Enterprise 1.9.8, 1.10.5, and 1.11.1.	9.1	More Details
CVE-2022-35131	Joplin v2.8.8 allows attackers to execute arbitrary commands via a crafted payload injected into the Node titles.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2022-1136	Use after free in Tab Strip in Google Chrome prior to 100.0.4896.60 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap gestures.

CVE Number	Description
CVE-2022-35285	IBM Security Verify Information Queue 10.0.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions tr website trusts. IBM X-Force ID: 230812.
CVE-2022-1314	Type confusion in V8 in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0972	Use after free in Extensions in Google Chrome prior to 99.0.4844.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit hea page.
CVE-2022-0974	Use after free in Splitscreen in Google Chrome on Chrome OS prior to 99.0.4844.74 allowed a remote attacker who convinced a user to engage in specific user interac corruption via a crafted HTML page.
CVE-2022-26307	LibreOffice supports the storage of passwords for web connections in the user's configuration database. The stored passwords are encrypted with a single master key LibreOffice existed where master key was poorly encoded resulting in weakening its entropy from 128 to 43 bits making the stored passwords vulerable to a brute force the users stored config. This issue affects: The Document Foundation LibreOffice 7.2 versions prior to 7.2.7; 7.3 versions prior to 7.3.3.
CVE-2022-0975	Use after free in ANGLE in Google Chrome prior to 99.0.4844.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0976	Heap buffer overflow in GPU in Google Chrome prior to 99.0.4844.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-34114	Dataease v1.11.1 was discovered to contain a SQL injection vulnerability via the parameter dataSourceId.
CVE-2022-34588	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via the grade parameter at /school/view/timetable_insert_form.php.
CVE-2022-1364	Type confusion in V8 Turbofan in Google Chrome prior to 100.0.4896.127 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-34586	itsourcecode Advanced School Management System v1.0 is vulnerable to SQL Injection via the grade parameter at /school/view/student_grade_wise.php.
CVE-2022-0980	Use after free in New Tab Page in Google Chrome prior to 99.0.4844.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit interactions.
CVE-2022-0979	Use after free in Safe Browsing in Google Chrome on Android prior to 99.0.4844.74 allowed a remote attacker who convinced a user to engage in specific user interact corruption via a crafted HTML page.
CVE-2022-26137	A vulnerability in multiple Atlassian products allows a remote, unauthenticated attacker to cause additional Servlet Filters to be invoked when the application processes has confirmed and fixed the only known security issue associated with this vulnerability: Cross-origin resource sharing (CORS) bypass. Sending a specially crafted HT Filter used to respond to CORS requests, resulting in a CORS bypass. An attacker that can trick a user into requesting a malicious URL can access the vulnerable app Atlassian Bamboo versions are affected before 8.0.9, from 8.1.0 before 8.1.8, and from 8.2.0 before 8.2.4. Atlassian Bitbucket versions are affected before 7.6.16, from before 7.19.5, from 7.20.0 before 7.20.2, from 7.21.0 before 7.21.2, and versions 8.0.0 and 8.1.0. Atlassian Confluence versions are affected before 7.4.17, from 7.5.0 7.14.3, from 7.15.0 before 7.15.2, from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and version 7.21.0. Atlassian Crowd versions are affected before 4.3.8, from 4.4 Atlassian Fisheye and Crucible versions before 4.8.10 are affected. Atlassian Jira versions are affected before 8.13.22, from 8.14.0 before 8.20.10, and from 8.21.0 bef Management versions are affected before 4.13.22, from 4.14.0 before 4.20.10, and from 4.21.0 before 4.22.4.
CVE-2022-0978	Use after free in ANGLE in Google Chrome prior to 99.0.4844.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-31879	Online Fire Reporting System 1.0 is vulnerable to SQL Injection via the date parameter.
CVE-2022-33745	insufficient TLB flush for x86 PV guests in shadow mode For migration as well as to work around kernels unaware of L1TF (see XSA-273), PV guests may be run in sh XSA-401, code was moved inside a function in Xen. This code movement missed a variable changing meaning / value between old and new code positions. The now w a wrong TLB flush condition, omitting flushes where such are necessary.
CVE-2022-1313	Use after free in tab groups in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE Number	Description
CVE-2022-1311	Use after free in shell in Google Chrome on ChromeOS prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page
CVE-2022-1310	Use after free in regular expressions in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page
CVE-2022-1308	Use after free in BFCache in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1133	Use after free in WebRTC Perf in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1134	Type confusion in V8 in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1135	Use after free in Shopping Cart in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via standard feature user inter
CVE-2022-1141	Use after free in File Manager in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to engage in specific user interaction to poten specific user gesture.
CVE-2022-1142	Heap buffer overflow in WebUI in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to engage in specific user interaction to pote specific input into DevTools.
CVE-2022-1143	Heap buffer overflow in WebUI in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to engage in specific user interaction to pote specific input into DevTools.
CVE-2022-1144	Use after free in WebUI in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially e input into DevTools.
CVE-2022-1127	Use after free in QR Code Generator in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to engage in specific user interaction t via user interaction.
CVE-2022-1125	Use after free in Portals in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially e interaction.
CVE-2022-1096	Type confusion in V8 in Google Chrome prior to 99.0.4844.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1539	The Exports and Reports WordPress plugin before 0.9.2 does not sanitize and validate data when generating the CSV to export, which could lead to a CSV injection, b function, or to leak data via maliciously injected hyperlinks.
CVE-2022-2240	The Request a Quote WordPress plugin through 2.3.7 does not validate uploaded CSV files, allowing unauthenticated users to attach a malicious CSV file to a quote, w once an admin download and open it
CVE-2022-0971	Use after free in Blink Layout in Google Chrome on Android prior to 99.0.4844.74 allowed a remote attacker who had compromised the renderer process to potentially HTML page.
CVE-2022-1232	Type confusion in V8 in Google Chrome prior to 100.0.4896.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1305	Use after free in storage in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-35286	IBM Security Verify Information Queue 10.0.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions tr website trusts. IBM X-Force ID: 230814.

CVE Number	Description
CVE-2022-1131	Use after free in Cast UI in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1634	Use after free in Browser UI in Google Chrome prior to 101.0.4951.64 allowed a remote attacker who had convinced a user to engage in specific UI interaction to poten specific user interactions.
CVE-2022-1635	Use after free in Permission Prompts in Google Chrome prior to 101.0.4951.64 allowed a remote attacker who convinced a user to engage in specific UI interactions to via specific user interactions.
CVE-2022-2136	The affected product is vulnerable to multiple SQL injections that require low privileges for exploitation and may allow an unauthorized attacker to disclose information.
CVE-2022-1489	Out of bounds memory access in UI Shelf in Google Chrome on Chrome OS, Lacros prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corrup
CVE-2022-1490	Use after free in Browser Switcher in Google Chrome prior to 101.0.4951.41 allowed a remote attacker who convinced a user to engage in specific user interaction to p a crafted HTML page.
CVE-2022-1491	Use after free in Bookmarks in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via specific and direct user intera
CVE-2022-1493	Use after free in Dev Tools in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via specific and direct user interac
CVE-2022-1484	Heap buffer overflow in Web UI Settings in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML p
CVE-2022-1483	Heap buffer overflow in WebGPU in Google Chrome prior to 101.0.4951.41 allowed a remote attacker who had compromised the renderer process to potentially exploit page.
CVE-2022-1481	Use after free in Sharing in Google Chrome on Mac prior to 101.0.4951.41 allowed a remote attacker who convinced a user to engage in specific user interaction to pot crafted HTML page.
CVE-2022-1496	Use after free in File Manager in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via specific and direct user inte
CVE-2022-1479	Use after free in ANGLE in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1633	Use after free in Sharesheet in Google Chrome on Chrome OS prior to 101.0.4951.64 allowed a remote attacker who convinced a user to engage in specific UI interact corruption via specific user interactions.
CVE-2022-1486	Type confusion in V8 in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted
CVE-2022-1636	Use after free in Performance APIs in Google Chrome prior to 101.0.4951.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1638	Heap buffer overflow in V8 Internationalization in Google Chrome prior to 101.0.4951.64 allowed a remote attacker to potentially exploit heap corruption via a crafted H
CVE-2022-1639	Use after free in ANGLE in Google Chrome prior to 101.0.4951.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1640	Use after free in Sharing in Google Chrome prior to 101.0.4951.64 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially e HTML page.

CVE Number	Description
CVE-2022-1641	Use after free in Web UI Diagnostics in Google Chrome on Chrome OS prior to 101.0.4951.64 allowed a remote attacker who convinced a user to engage in specific UI heap corruption via specific user interaction.
CVE-2022-1478	Use after free in SwiftShader in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1477	Use after free in Vulkan in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-30269	Motorola ACE1000 RTUs through 2022-05-02 mishandle application integrity. They allow for custom application installation via either STS software, the C toolkit, or the case of the Easy Configurator, application images (as PLX/DAT/APP/CRC files) are uploaded via the Web UI. In case of the C toolkit, they are transferred and installed application images were found to have no authentication (in the form of firmware signing) and only relied on insecure checksums for regular integrity checks.
CVE-2020-7678	This affects all versions of package node-import. The "params" argument of module function can be controlled by users without any sanitization.b. This is then provided 79 in the index file "index.js".
CVE-2020-7677	This affects the package thenify before 3.3.1. The name argument provided to the package can be controlled by users without any sanitization, and this is provided to th sanitization.
CVE-2022-36444	An issue was discovered in Atos Unify OpenScape SBC 9 and 10 before 10R2.2.1, Atos Unify OpenScape Branch 9 and 10 before version 10R2.1.1, and Atos Unify O 10R9.12.1. A remote code execution vulnerability may allow an unauthenticated attacker (with network access to the admin interface) to disrupt system availability or p confidentiality and integrity of the system.
CVE-2022-33960	Multiple Authenticated (subscriber or higher user role) SQL Injection (SQLi) vulnerabilities in Social Share Buttons by Supsystic plugin <= 2.2.3 at WordPress.
CVE-2022-2131	OpenKM Community Edition in its 6.3.10 version and before was using XMLReader parser in XMLTextExtractor.java file without the required security flags, allowing an entity injection attack.
CVE-2022-22999	Western Digital My Cloud devices are vulnerable to a cross side scripting vulnerability that can allow a malicious user with elevated privileges access to drives being ba JavaScript payloads into an authenticated user's browser. As a result, it may be possible to gain control over the authenticated session, steal data, modify settings, or r websites. The scope of impact can extend to other components.
CVE-2022-2138	The affected product is vulnerable due to missing authentication, which may allow an attacker to read or modify sensitive data and execute arbitrary code, resulting in a
CVE-2022-1041	In Zephyr bluetooth mesh core stack, an out-of-bound write vulnerability can be triggered during provisioning.
CVE-2022-1042	In Zephyr bluetooth mesh core stack, an out-of-bound write vulnerability can be triggered during provisioning.
CVE-2022-2493	Data Access from Outside Expected Data Manager Component in GitHub repository openemr/openemr prior to 7.0.0.
CVE-2022-2142	The affected product is vulnerable to a SQL injection with high attack complexity, which may allow an unauthorized attacker to disclose information.
CVE-2022-0902	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Neutralization of Special Elements used in a Command ('Command Injection') remote controller products of ABB (RMC-100 (Standard), RMC-100-LITE, XIO, XFCG5 , XRCG5 , uFLOG5 , UDC) allows an attacker who successfully exploited this v arbitrary code in an affected system node.
CVE-2022-31234	Dell EMC PowerStore, contain(s) an Improper Restriction of Excessive Authentication Attempts Vulnerability in PowerStore Manager GUI. A remote unauthenticated at vulnerability, leading to password brute-forcing. Account takeover is possible if weak passwords are used by users.
CVE-2022-2225	By using warp-cli subcommands (disable-ethernet, disable-wifi), it was possible for a user without admin privileges to bypass configured Zero Trust security policies (e.g and features such as 'Lock WARP switch'.
CVE-2022-1130	Insufficient validation of trust input in WebOTP in Google Chrome on Android prior to 100.0.4896.60 allowed a remote attacker to send arbitrary intents from any app via

CVE Number	Description
CVE-2022-2486	A vulnerability, which was classified as critical, was found in WAVLINK WN535K2 and WN535K3. This affects an unknown part of the file /cgi-bin/mesh.cgi?page=upgra argument key leads to os command injection. The exploit has been disclosed to the public and may be used.
CVE-2022-36450	Obsidian 0.14.x and 0.15.x before 0.15.5 allows obsidian://hook-get-address remote code execution because window.open is used without checking the URL.
CVE-2022-2487	A vulnerability has been found in WAVLINK WN535K2 and WN535K3 and classified as critical. This vulnerability affects unknown code of the file /cgi-bin/nightled.cgi. T start_hour leads to os command injection. The exploit has been disclosed to the public and may be used.
CVE-2022-2488	A vulnerability was found in WAVLINK WN535K2 and WN535K3 and classified as critical. This issue affects some unknown processing of the file /cgi-bin/touchlist_sync argument IP leads to os command injection. The exploit has been disclosed to the public and may be used.
CVE-2022-34571	An access control issue in Wavlink WiFi-Repeater RPTA2-77W.M4300.01.GD.2017Sep19 allows attackers to obtain the system key information and execute arbitrary c syslog.shtml.
CVE-2021-46829	GNOME GdkPixbuf (aka GDK-PixBuf) before 2.42.8 allows a heap-based buffer overflow when compositing or clearing frames in GIF files, as demonstrated by io-gif-an overflow is controllable and could be abused for code execution, especially on 32-bit systems.
CVE-2021-33453	An issue was discovered in lrzip version 0.641. There is a use-after-free in ucompthread() in stream.c:1538.
CVE-2022-34866	Passage Drive versions v1.4.0 to v1.5.1.0 and Passage Drive for Box version v1.0.0 contain an insufficient data verification vulnerability for interprocess communicatior an arbitrary OS command may be executed with LocalSystem privilege of the Windows system where the product is running.
CVE-2022-33967	squashfs filesystem implementation of U-Boot versions from v2020.10-rc2 to v2022.07-rc5 contains a heap-based buffer overflow vulnerability due to a defect in the me specially crafted squashfs image may lead to a denial-of-service (DoS) condition or arbitrary code execution.
CVE-2022-35899	There is an unquoted service path in ASUSTeK Aura Ready Game SDK service (GameSDK.exe) 1.0.0.4. This might allow a local user to escalate privileges by creating %PROGRAMFILES(X86)%\ASUS\GameSDK.exe file.
CVE-2022-36415	A DLL hijacking vulnerability exists in the uninstaller in Scooter Beyond Compare 1.8a through 4.4.2 before 4.4.3 when installed via the EXE installer. The uninstaller at Windows Temp folder. If a standard user places malicious DLLs in the C:\Windows\Temp\ folder, and then the uninstaller is run as SYSTEM, the DLLs will execute with
CVE-2022-33315	Deserialization of Untrusted Data vulnerability in ICONICS GENESIS64 versions 10.97.1 and prior and Mitsubishi Electric MC Works64 versions 4.04E (10.95.210.01) a attacker to execute an arbitrary malicious code by leading a user to load a monitoring screen file including malicious XAML codes.
CVE-2022-22221	An Improper Neutralization of Special Elements vulnerability in the download manager of Juniper Networks Junos OS on SRX Series and EX Series allows a locally au privileges to take full control over the device. One aspect of this vulnerability is that the attacker needs to be able to execute any of the "request ..." or "show system do affects Juniper Networks Junos OS on SRX Series and EX Series: All versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S4; 20.3 versions prior to 20.3R3-S3; 20.4 versions prior to 20.4R3-S2, 20.4R3-S3; 21.1 versions prior to 21.1R3-S1; 21.2 ve 21.3 versions prior to 21.3R2, 21.3R3; 21.4 versions prior to 21.4R1-S1, 21.4R2.
CVE-2022-29957	The Emerson DeltaV Distributed Control System (DCS) through 2022-04-29 mishandles authentication. It utilizes several proprietary protocols for a wide variety of func Firmware upgrade (18508/TCP, 18518/TCP); Plug-and-Play (18510/UDP); Hawk services (18507/UDP); Management (18519/TCP); Cold restart (18512/UDP); SIS cor Wireless Gateway Protocol (18515/UDP). None of these protocols have any authentication features, allowing any attacker capable of communicating with the ports in q desired functionality.
CVE-2022-33317	Inclusion of Functionality from Untrusted Control Sphere vulnerability in ICONICS GENESIS64 versions 10.97.1 and prior and Mitsubishi Electric MC Works64 versions allows an unauthenticated attacker to execute an arbitrary malicious code by leading a user to load a monitoring screen file including malicious script codes.
CVE-2022-33320	Deserialization of Untrusted Data vulnerability in ICONICS GENESIS64 versions 10.97.1 and prior and Mitsubishi Electric MC Works64 versions 4.04E (10.95.210.01) a attacker to execute an arbitrary malicious code by leading a user to load a project configuration file including malicious XML codes.
CVE-2022-35870	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition 8.1.15 (b2022030114). Although authentica vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within com.inductiveautomation.metro.impl. The issue results from the la supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN
CVE-2022-2522	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0061.
CVE-2022-35873	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition 8.1.15 (b2022030114). User interaction is r that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of ZIP files. Crafted data in a ZIP file can cause the app scripts. The user interface fails to provide sufficient indication of the hazard. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was

CVE Number	Description
CVE-2022-33316	Deserialization of Untrusted Data vulnerability in ICONICS GENESIS64 versions 10.97.1 and prior and Mitsubishi Electric MC Works64 versions 4.04E (10.95.210.01) a attacker to execute an arbitrary malicious code by leading a user to load a monitoring screen file including malicious XAML codes.
CVE-2022-35872	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition 8.1.15 (b2022030114). User interaction is r that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of ZIP files. The issue results from the lack of proper valida can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-17115.
CVE-2022-35871	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition 8.1.15 (b2022030114). Authentication is no The specific flaw exists within the authenticateAdSso method. The issue results from the lack of authentication prior to allowing the execution of python code. An attack execute code in the context of SYSTEM. Was ZDI-CAN-17206.
CVE-2022-32958	A remote attacker with general user privilege can send a message to Teamplus Pro's chat group that exceeds message size limit, to terminate other recipients' Teampl
CVE-2022-31164	Tovy is a a staff management system for Roblox groups. A vulnerability in versions prior to 0.7.51 allows users to log in as other users, including privileged users such a problem has been patched in version 0.7.51.
CVE-2022-31163	TZInfo is a Ruby library that provides access to time zone data and allows times to be converted using time zone rules. Versions prior to 0.36.1, as well as those prior t data source tzinfo-data, are vulnerable to relative path traversal. With the Ruby data source, time zones are defined in Ruby files. There is one file per time zone. Time on demand. In the affected versions, `TZInfo::Timezone.get` fails to validate time zone identifiers correctly, allowing a new line character within the identifier. With Ruby `TZInfo::Timezone.get` can be made to load unintended files with `require`, executing them within the Ruby process. Versions 0.3.61 and 1.2.10 include fixes to correct Versions 2.0.0 and later are not vulnerable. Version 0.3.61 can still load arbitrary files from the Ruby load path if their name follows the rules for a valid time zone identi `tzinfo/definition` within a directory in the load path. Applications should ensure that untrusted files are not placed in a directory on the load path. As a workaround, the t before passing to `TZInfo::Timezone.get` by ensuring it matches the regular expression `\A[A-Za-z0-9+\-_]+(?:\/[A-Za-z0-9+\-_]+)*\z`.
CVE-2022-2135	The affected product is vulnerable to multiple SQL injections, which may allow an unauthorized attacker to disclose information.
CVE-2022-31170	OpenZeppelin Contracts is a library for smart contract development. Versions 4.0.0 until 4.7.1 are vulnerable to ERC165Checker reverting instead of returning `false`. ` is designed to always successfully return a boolean, and under no circumstance revert. However, an incorrect assumption about Solidity 0.8's `abi.decode` allows some contract that doesn't implement EIP-165 as expected, specifically if it returns a value other than 0 or 1. The contracts that may be affected are those that use `ERC165(interface and then handle the lack of support in a way other than reverting. The issue was patched in version 4.7.1.
CVE-2022-31172	OpenZeppelin Contracts is a library for smart contract development. Versions 4.1.0 until 4.7.1 are vulnerable to the SignatureChecker reverting. `SignatureChecker.isV revert. However, an incorrect assumption about Solidity 0.8's `abi.decode` allows some cases to revert, given a target contract that doesn't implement EIP-1271 as exp affected are those that use `SignatureChecker` to check the validity of a signature and handle invalid signatures in a way other than reverting. The issue was patched ir
CVE-2022-2327	io_uring use work_flags to determine which identity need to grab from the calling process to make sure it is consistent with the calling process when executing IORING_ some types, which can lead to incorrect reference counts which can then lead to a double free. We recommend upgrading the kernel past commit df3f3bb5059d20ef09
CVE-2020-14114	information leakage vulnerability exists in the Xiaomi SmartHome APP. This vulnerability is caused by illegal calls of some sensitive JS interfaces, which can be exploit information.
CVE-2022-34037	An out-of-bounds read in the rewrite function at /modules/caddyhttp/rewrite/rewrite.go in Caddy v2.5.1 allows attackers to cause a Denial of Service (DoS) via a crafted as a bug, not a security vulnerability, in the Caddy web server that emerged when an administrator's bad configuration containing a malformed request URI caused the instead of a valid HTTP response to the client.
CVE-2020-14126	Information leakage vulnerability exists in the Mi Sound APP. This vulnerability is caused by illegal calls of some sensitive JS interfaces, which can be exploited by atta
CVE-2022-35287	IBM Security Verify Information Queue 10.0.2 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authenticati external components, or encryption of internal data. IBM X-Force ID: 230817.
CVE-2022-32458	Digiwin BPM has a XML External Entity Injection (XXE) vulnerability due to insufficient validation for user input. An unauthenticated remote attacker can perform XML ir system files.
CVE-2022-34749	In mistune through 2.0.2, support of inline markup is implemented by using regular expressions that can involve a high amount of backtracking on certain edge cases. T catastrophic backtracking.
CVE-2021-40180	In the WeChat application 8.0.10 for Android and iOS, a mini program can obtain sensitive information from a user's address book via wx.searchContacts.

CVE Number	Description
CVE-2021-33057	The QQ application 8.7.1 for Android and iOS does not enforce the permission requirements (e.g., android.permission.ACCESS_FINE_LOCATION) for determining the attacker can use qq.createMapContext to create a MapContext object, use MapContext.moveToLocation to move the center of the map to the device's location, and us get the latitude and longitude of the current map center.
CVE-2022-31205	In Omron CS series, CJ series, and CP series PLCs through 2022-05-18, the password for access to the Web UI is stored in memory area D1449...D1452 and can be r protocol without any further authentication.
CVE-2022-31204	Omron CS series, CJ series, and CP series PLCs through 2022-05-18 use cleartext passwords. They feature a UM Protection setting that allows users or system integ order to restrict sensitive engineering operations (such as project/logic uploads and downloads). This password is set using the OMRON FINS command Program Area command Program Area Protect Clear, both of which are transmitted in cleartext.
CVE-2022-30275	The Motorola MOSCAD Toolbox software through 2022-05-02 relies on a cleartext password. It utilizes an MDLC driver to communicate with MOSCAD/ACE RTUs for these communications is protected by a password stored in cleartext in the wmdlcdrv.ini driver configuration file. In addition, this password is used for access control to with the Legacy Password feature. In this case, an insecure CRC of the password is present in the project file: this CRC is validated against the password in the driver
CVE-2022-1487	Use after free in Ozone in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via running a Wayland test.
CVE-2022-1485	Use after free in File System API in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-35639	IBM Sterling Partner Engagement Manager 6.1, 6.2, and Cloud 22.2 do not limit the length of a connection which could cause the server to become unresponsive. IBM
CVE-2022-34067	Warehouse Management System v1.0 was discovered to contain a SQL injection vulnerability via the cari parameter.
CVE-2022-33977	untangle is a python library to convert XML data to python objects. untangle versions 1.2.0 and earlier improperly restricts recursive entity references in DTDs. By explo unauthenticated attacker may cause a denial-of-service (DoS) condition on the server where the product is running.
CVE-2022-31471	untangle is a python library to convert XML data to python objects. untangle versions 1.2.0 and earlier improperly restricts XML external entity references. By exploiting unauthenticated attacker may read the contents of local files.
CVE-2022-34576	A vulnerability in /cgi-bin/ExportAllSettings.sh of WAVLINK WN535 G3 M35G3R.V5030.180927 allows attackers to execute arbitrary code via a crafted POST request.
CVE-2022-1145	Use after free in Extensions in Google Chrome prior to 100.0.4896.60 allowed an attacker who convinced a user to install a malicious extension to potentially exploit he interaction and profile destruction.
CVE-2022-34570	WAVLINK WN579 X3 M79X3.V5030.191012/M79X3.V5030.191012 contains an information leak which allows attackers to obtain the key information via accessing the
CVE-2022-34906	A hard-coded cryptographic key is used in FileWave before 14.6.3 and 14.7.x before 14.7.2. Exploitation could allow an unauthenticated actor to decrypt sensitive infor send crafted requests.
CVE-2022-34966	OpenTeknik LLC OSSN OPEN SOURCE SOCIAL NETWORK v6.3 LTS was discovered to contain an HTML injection vulnerability via the location parameter at http://ip
CVE-2022-35284	IBM Security Verify Information Queue 10.0.2 could disclose sensitive information due to a missing or insecure SameSite attribute for a sensitive cookie. IBM X-Force I
CVE-2022-24992	A vulnerability in the component process.php of QR Code Generator v5.2.7 allows attackers to perform directory traversal.
CVE-2022-35650	The vulnerability was found in Moodle, occurs due to input validation error when importing lesson questions. This insufficient path checks results in arbitrary file read ris attacker to perform directory traversal attacks. The capability to access this feature is only available to teachers, managers and admins by default.
CVE-2022-26306	LibreOffice supports the storage of passwords for web connections in the user's configuration database. The stored passwords are encrypted with a single master key LibreOffice existed where the required initialization vector for encryption was always the same which weakens the security of the encryption making them vulnerable if configuration data. This issue affects: The Document Foundation LibreOffice 7.2 versions prior to 7.2.7; 7.3 versions prior to 7.3.1.

CVE Number	Description
CVE-2022-26305	An Improper Certificate Validation vulnerability in LibreOffice existed where determining if a macro was signed by a trusted author was done by only matching the serial used certificate with that of a trusted certificate. This is not sufficient to verify that the macro was actually signed with the certificate. An adversary could therefore create number and an issuer string identical to a trusted certificate which LibreOffice would present as belonging to the trusted author, potentially leading to the user to execut improperly trusted. This issue affects: The Document Foundation LibreOffice 7.2 versions prior to 7.2.7; 7.3 versions prior to 7.3.1.
CVE-2021-23373	All versions of package set-deep-prop are vulnerable to Prototype Pollution via the main functionality.
CVE-2022-29709	CommuniLink Internet Limited CLink Office v2.0 was discovered to contain multiple SQL injection vulnerabilities via the username and password parameters.
CVE-2022-24294	A regular expression used in Apache MXNet (incubating) is vulnerable to a potential denial-of-service by excessive resource consumption. The bug could be exploited MXNet that has a specially crafted operator name that would cause the regular expression evaluation to use excessive resources to attempt a match. This issue affects 1.9.1.
CVE-2022-31162	Slack Morphism is an async client library for Rust. Prior to 0.41.0, it was possible for Slack OAuth client information to leak in application debug logs. Stricter and more introduced in v0.41.0 for OAuth secret types to reduce the possibility of printing sensitive information in application logs. As a workaround, do not print/output requests configurations in logs.
CVE-2022-30276	The Motorola MOSCAD and ACE line of RTUs through 2022-05-02 omit an authentication requirement. They feature IP Gateway modules which allow for interfacing be Communication (MDLC) networks (potentially over a variety of serial, RF and/or Ethernet links) and TCP/IP networks. Communication with RTUs behind the gateway is IPGW protocol (5001/TCP). This protocol does not have any authentication features, allowing any attacker capable of communicating with the port in question to invoke
CVE-2022-22205	A Missing Release of Memory after Effective Lifetime vulnerability in the Application Quality of Experience (appqoe) subsystem of the PFE of Juniper Networks Junos C unauthenticated network based attacker to cause a Denial of Service (DoS). Upon receiving specific traffic a memory leak will occur. Sustained processing of such spe out of memory condition that prevents all services from continuing to function, and requires a manual restart to recover. A device is only vulnerable when advance(d) po configured and AppQoE (sla rule) is not configured for these APBR rules. This issue affects Juniper Networks Junos OS on SRX Series: 20.3 versions prior to 20.3R3-S 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R1-S2, 21.3R2. This issue does not affect Juniper Networks Junos C
CVE-2021-46828	In libtirpc before 1.3.3rc1, remote attackers could exhaust the file descriptors of a process that uses libtirpc because idle TCP connections are mishandled. This can, in without accepting new connections.
CVE-2022-22209	A Missing Release of Memory after Effective Lifetime vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated network based attacker to cau Junos platforms, the Kernel Routing Table (KRT) queue can get stuck due to a memory leak triggered by interface flaps or route churn leading to RIB and PFEs getting causes RTNEXTHOP/route and next-hop memory pressure issue and the KRT queue will eventually get stuck with the error- 'ENOMEM -- Cannot allocate memory'. Th FIB can be seen with the "show route" and "show route forwarding-table" command. This issue will lead to failures for adding new routes. The KRT queue status can be "show krt queue": user@host > show krt state High-priority add queue: 1 queued ADD nhtype Router index 0 (31212) error 'ENOMEM -- Cannot allocate memory' kqp ' will be observed in /var/log/messages, which indicate high memory for routes/nexthops: host rpd[16279]: RPD_RT_HWM_NOTICE: New RIB highwatermark for routes rpd[16279]: RPD_KRT_Q_RETRIES: nexthop ADD: Cannot allocate memory host rpd[16279]: RPD_KRT_Q_RETRIES: nexthop ADD: Cannot allocate memory host k rts_veto_net_delayed_unref_limit: Route/nexthop memory is severe pressure. User Application to perform recovery actions. O p 8 err 12, rtsm_id 0:-1, msg type 10, ve rts_veto_net_delayed_unref_limit: Memory usage of M_RTNEXTHOP type = (806321208) Max size possible for M_RTNEXTHOP type = (689432176) Current delayed this platform = (120000) Current delayed weight unref = (0) Max delayed weight unref on this platform = (400000) curproc = rpd. This issue affects: Juniper Networks Ju 21.2R3; 21.3 versions prior to 21.3R2-S1, 21.3R3; 21.4 versions prior to 21.4R1-S2, 21.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 21
CVE-2022-22207	A Use After Free vulnerability in the Advanced Forwarding Toolkit (AFT) manager process (aftmand) of Juniper Networks Junos OS allows an unauthenticated network due to intensive polling of Abstracted Fabric (AF) interface statistics and thereby a Denial of Service (DoS). Continued gathering of AF interface statistics will create a s condition. This issue affects Juniper Networks Junos OS on MX Series: 20.1 versions later than 20.1R1; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3 21.1 versions prior to 21.1R2; 21.2 versions prior to 21.2R2.
CVE-2022-32430	An access control issue in Lin CMS Spring Boot v0.2.1 allows attackers to access the backend information and functions within the application.
CVE-2021-29755	IBM QRadar SIEM 7.3, 7.4, and 7.5 does not preform proper certificate validation for some inter-host communications. IBM X-Force ID: 202015.
CVE-2022-22206	A Buffer Overflow vulnerability in the PFE of Juniper Networks Junos OS on SRX series allows an unauthenticated network based attacker to cause a Denial of Service specific traffic is scanned by Enhanced Web Filtering safe-search feature of UTM (Unified Threat management). Continued receipt of this specific traffic will create a su condition. This issue affects Juniper Networks Junos OS: 20.2 versions prior to 20.2R3-S4 on SRX Series; 20.3 versions prior to 20.3R3-S3 on SRX Series; 20.4 versio Series; 21.1 versions prior to 21.1R3-S1 on SRX Series; 21.2 versions prior to 21.2R2-S2, 21.2R3 on SRX Series; 21.3 versions prior to 21.3R2 on SRX Series; 21.4 v Series. This issue does not affect Juniper Networks Junos OS versions prior to 20.2R1.
CVE-2022-22212	An Allocation of Resources Without Limits or Throttling vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved allows unauthentica a Denial of Service (DoS). On all Junos Evolved platforms hostbound protocols will be impacted by a high rate of specific hostbound traffic from ports on a PFE. Contin will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS Evolved: 21.2 versions prior to 21.2R3-EVO; 21.3 versions prio not affect Juniper Networks Junos OS Evolved versions prior to 21.2R1.
CVE-2022-32556	An issue was discovered in Couchbase Server before 7.0.4. A private key is leaked to the log files with certain crashes.

CVE Number	Description
CVE-2022-34047	An access control issue in Wavlink WN530HG4 M30HG4.V5030.191116 allows attackers to obtain usernames and passwords via view-source:http://IP_ADDRESS/set searching for [var syspasswd].
CVE-2022-24660	The debug interface of Goldshell ASIC Miners v2.2.1 and below was discovered to be exposed publicly on the web interface, allowing attackers to access passwords a plaintext.
CVE-2022-34046	An access control issue in Wavlink WN533A8 M33A8.V5030.190716 allows attackers to obtain usernames and passwords via view-source:http://IP_ADDRESS/sysinit. [logincheck(user);].
CVE-2020-21405	An issue was discovered in H96 Smart TV Box H96 Pro Plus allows attackers to corrupt files via calls to the saveDeepColorAttr service.unk
CVE-2022-1766	Anchore Enterprise anchorectl version 0.1.4 improperly stored credentials when generating a Software Bill of Materials. anchorectl will add the credentials used to acce Software Bill of Materials (SBOM) generated by anchorectl. Users of anchorectl version 0.1.4 should upgrade to anchorectl version 0.1.5 to resolve this issue.
CVE-2022-29834	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ICONICS GENESIS64 versions 10.97 to 10.97.1 allows a remote unauthe arbitrary files in the GENESIS64 server and disclose information stored in the files by embedding a malicious URL parameter in the URL of the monitoring screen delive monitoring application and accessing the monitoring screen.
CVE-2022-24659	Goldshell ASIC Miners v2.2.1 and below was discovered to contain a path traversal vulnerability which allows unauthenticated attackers to retrieve arbitrary files from tl
CVE-2020-21406	An issue was discovered in RK Smart TV Box MAX and V88 SmartTV box that allows attackers to cause a denial of service via the switchNextDisplayInterface service.
CVE-2022-2199	The main MiCODUS MV720 GPS tracker web server has a reflected cross-site scripting vulnerability that could allow an attacker to gain control by tricking a user into n
CVE-2022-20860	A vulnerability in the SSL/TLS implementation of Cisco Nexus Dashboard could allow an unauthenticated, remote attacker to alter communications with associated con This vulnerability exists because SSL server certificates are not validated when Cisco Nexus Dashboard is establishing a connection to Cisco Application Policy Infrastr Cloud APIC, or Cisco Nexus Dashboard Fabric Controller, formerly Data Center Network Manager (DCNM) controllers. An attacker could exploit this vulnerability by us intercept the traffic between the affected device and the controllers, and then using a crafted certificate to impersonate the controllers. A successful exploit could allow t between devices or view sensitive information, including Administrator credentials for these controllers.
CVE-2022-23000	The Western Digital My Cloud Web App [https://os5.mycloud.com/] uses a weak SSLContext when attempting to configure port forwarding rules. This was enabled to m outdated home routers. By using an "SSL" context instead of "TLS" or specifying stronger validation, deprecated or insecure protocols are permitted. As a result, a loca this vulnerability and jeopardize the integrity, confidentiality and authenticity of information transmitted. The scope of impact cannot extend to other components and no vulnerability.
CVE-2016-15004	A vulnerability was found in InfiniteWP Client Plugin 1.5.1.3/1.6.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipu can be launched remotely. Upgrading to version 1.6.1.1 is able to address this issue. It is recommended to upgrade the affected component.
CVE-2020-28471	This affects the package properties-reader before 2.2.0.
CVE-2020-28462	This affects all versions of package ion-parser. If an attacker submits a malicious INI file to an application that parses it with parse , they will pollute the prototype on the further depending on the context.
CVE-2020-28461	This affects the package js-ini before 1.3.0. If an attacker submits a malicious INI file to an application that parses it with parse , they will pollute the prototype on the ap further depending on the context.
CVE-2020-28455	This affects all versions of package markdown-it-toc. The title of the generated toc and the contents of the header are not escaped.
CVE-2020-28441	This affects the package conf-cfg-ini before 1.2.2. If an attacker submits a malicious INI file to an application that parses it with decode, they will pollute the prototype or exploited further depending on the context.
CVE-2020-28436	This affects all versions of package google-cloudstorage-commands.

CVE Number	Description
CVE-2020-28459	This affects all versions of package markdown-it-decorate. An attacker can add an event handler or use javascript:xxx for the link.
CVE-2022-33969	Authenticated WordPress Options Change vulnerability in Biplob Adhikari's Flipbox plugin <= 2.6.0 at WordPress.
CVE-2022-34042	Barangay Management System v1.0 was discovered to contain a SQL injection vulnerability via the hidden_id parameter at /pages/household/household.php.
CVE-2022-30272	The Motorola ACE1000 RTU through 2022-05-02 mishandles firmware integrity. It utilizes either the STS software suite or ACE1000 Easy Configurator for performing fi Configurator, firmware updates are performed through access to the Web UI where file system, kernel, package, bundle, or application images can be installed. Firmwa Processor (FEP) module are performed via access to the SSH interface (22/TCP), where a .hex file image is transferred and a bootloader script invoked. File system, k are supplied as RPM (RPM Package Manager) files while FEP updates are supplied as S-rec files. In all cases, firmware images were found to have no authentication only relied on insecure checksums for regular integrity checks.
CVE-2022-34590	Hospital Management System v1.0 was discovered to contain a SQL injection vulnerability via the editid parameter in /HMS/admin.php.
CVE-2022-36375	Authenticated (high role user) WordPress Options Change vulnerability in Biplob Adhikari's Tabs plugin <= 3.6.0 at WordPress.
CVE-2022-2219	The Unyson WordPress plugin before 2.7.27 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting
CVE-2022-34965	OpenTeknik LLC OSSN OPEN SOURCE SOCIAL NETWORK v6.3 LTS was discovered to contain an arbitrary file upload vulnerability via the component /ossn/admini vulnerability allows attackers to execute arbitrary code via a crafted PHP file. Note: The project owner believes this is intended behavior of the application as it only allo files.
CVE-2022-31250	A UNIX Symbolic Link (Symlink) Following vulnerability in keylime of openSUSE Tumbleweed allows local attackers to escalate from the keylime user to root. This issu keylime versions prior to 6.4.2-1.1.
CVE-2022-34150	The main MiCODUS MV720 GPS tracker web server has an authenticated insecure direct object reference vulnerability on endpoint and parameter device IDs, which a further verification.
CVE-2022-1651	A memory leak flaw was found in the Linux kernel in acrn_dev_ioctl in the drivers/virt/acrn/hsm.c function in how the ACRN Device Model emulates virtual NICs in VM. attacker to leak unauthorized kernel information, causing a denial of service.
CVE-2022-1671	A NULL pointer dereference flaw was found in rxrpc_preparse_s in net/rxrpc/server_key.c in the Linux kernel. This flaw allows a local attacker to crash the system or le
CVE-2022-32960	HiCOS' client-side citizen digital certificate component has a stack-based buffer overflow vulnerability when reading IC card due to insufficient parameter length validati unauthenticated physical attacker can exploit this vulnerability to execute arbitrary code, manipulate system data or terminate service.
CVE-2022-32959	HiCOS' client-side citizen digital certificate component has a stack-based buffer overflow vulnerability when reading IC card due to insufficient parameter length validati unauthenticated physical attacker can exploit this vulnerability to execute arbitrary code, manipulate system data or terminate service.
CVE-2022-1264	The affected product may allow an attacker with access to the Ignition web configuration to run arbitrary code.
CVE-2022-32961	HICOS' client-side citizen digital certificate component has a stack-based buffer overflow vulnerability when reading IC card due to insufficient parameter length validati unauthenticated physical attacker can exploit this vulnerability to execute arbitrary code, manipulate system data or terminate service.
CVE-2022-32962	HiCOS' client-side citizen certificate component has a double free vulnerability. An unauthenticated physical attacker can exploit this vulnerability to corrupt memory an system data or terminate service.
CVE-2022-36414	There is an elevation of privilege breakout vulnerability in the Windows EXE installer in Scooter Beyond Compare 4.2.0 through 4.4.2 before 4.4.3. Affected versions all applications with elevated privileges via the Clipboard Compare tray app after installation.

CVE Number	Description
CVE-2022-22210	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on QFX5000 Series and MX Series allows an unauthe a Denial of Service (DoS). On QFX5K Series and MX Series, when the PFE receives a specific VxLAN packet the Layer 2 Address Learning Manager (L2ALM) proces Continued receipt of this specific packet will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX5000 Series, M 20.3R3-S3; 20.4 versions prior to 20.4R3-S2; 21.2 versions prior to 21.2R2-S1. This issue does not affect Juniper Networks Junos OS: All versions prior to 20.3R1; 21.
CVE-2022-33944	The main MiCODUS MV720 GPS tracker web server has an authenticated insecure direct object references vulnerability on endpoint and POST parameter “Device ID,
CVE-2022-1146	Inappropriate implementation in Resource Timing in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to leak cross-origin data via a crafted HTML pag
CVE-2022-1138	Inappropriate implementation in Web Cursor in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who had compromised the renderer process to obscu bar) via a crafted HTML page.
CVE-2022-1139	Inappropriate implementation in Background Fetch API in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to leak cross-origin data via a crafted HTMI
CVE-2022-22686	Cross-Site Request Forgery (CSRF) vulnerability in webapi component in Synology Calendar before 2.3.4-0631 allows remote authenticated users to hijack the authen unspecified vectors.
CVE-2022-1129	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 100.0.4896.60 allowed a remote attacker to spoof the contents of the Omnibo page.
CVE-2022-1128	Inappropriate implementation in Web Share API in Google Chrome on Windows prior to 100.0.4896.60 allowed an attacker on the local network segment to leak cross-
CVE-2021-23451	The package otp-generator before 3.0.0 are vulnerable to Insecure Randomness due to insecure generation of random one-time passwords, which may allow a brute-f
CVE-2022-1137	Inappropriate implementation in Extensions in Google Chrome prior to 100.0.4896.60 allowed an attacker who convinced a user to install a malicious extension to leak crafted HTML page.
CVE-2022-35288	IBM Security Verify Information Queue 10.0.2 could allow a user to obtain sensitive information that could be used in further attacks against the system. IBM X-Force ID
CVE-2022-1482	Inappropriate implementation in WebGL in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML p
CVE-2022-34112	An access control issue in the component /api/plugin/uninstall Dataease v1.11.1 allows attackers to arbitrarily uninstall the plugin, a right normally reserved for the adm
CVE-2022-22203	An Incorrect Comparison vulnerability in PFE of Juniper Networks Junos OS allows an adjacent unauthenticated attacker to cause a Denial of Service (DoS). On QFX5 EX4650 platforms, the fxpc process will crash followed by the FPC reboot upon receipt of a specific hostbound packet. Continued receipt of these specific packets will c (DoS) condition. This issue only affects Juniper Networks Junos OS 19.4 version 19.4R3-S4.
CVE-2022-22214	An Improper Input Validation vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent attacker to Denial of Service (DoS). An FPC will crash and reboot after receiving a specific transit IPv6 packet over MPLS. Continued receipt of this packet will create a sustained This issue does not affect systems configured for IPv4 only. This issue affects: Juniper Networks Junos OS All versions prior to 12.3R12-S21; 15.1 versions prior to 15. 17.3R3-S12; 18.3 versions prior to 18.3R3-S6; 18.4 versions prior to 18.4R2-S9, 18.4R3-S9; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R to 19.3R2-S7, 19.3R3-S4; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3; 20.4 versior versions prior to 21.1R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S3-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-S prior to 21.4R2-EVO.
CVE-2022-22215	A Missing Release of File Descriptor or Handle after Effective Lifetime vulnerability in plugable authentication module (PAM) of Juniper Networks Junos OS and Junos authenticated attacker with low privileges to cause a Denial of Service (DoS). It is possible that after the termination of a gRPC connection the respective/var/run/<pid>. if occurring repeatedly can cause inode exhaustion. Inode exhaustion can present itself in two different ways: 1. The following log message can be observed: host kern inumber <number> on /.mount/var: out of inodes which by itself is a clear indication. 2. The following log message can be observed: host <process>[<pid>]: ... : No spa deterministic and just a representation of a write error which could have several reasons. So the following check needs to be done: user@host> show system storage r Avail Capacity Mounted on /dev/ada1p1 475M 300M 137M 69% /.mount/var which indicates that the write error is not actually due to a lack of disk space. If either 1. or output of: user@host> file list /var/run/*.env l count need to be checked and if it indicates a high (>10000) number of files the system has been affected by this issue. TI Junos OS All versions prior to 19.1R3-S8; 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S5; 19.4 versions prior to 19.4R2-S6, 19.4R3-S7; 20.1 versio versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. Juniper Netw prior to 20.4R3-EVO; 21.1 versions prior to 21.1R3-S1-EVO; 21.2 versions prior to 21.2R1-S1-EVO, 21.2R2-EVO.

CVE Number	Description
CVE-2022-1497	Inappropriate implementation in Input in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to spoof the contents of cross-origin websites via a crafted H
CVE-2022-1500	Insufficient data validation in Dev Tools in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2022-1655	An Incorrect Permission Assignment for Critical Resource flaw was found in Horizon on Red Hat OpenStack. Horizon session cookies are created without the HttpOnly being set to true in the environmental files, possibly leading to a loss of confidentiality and integrity.
CVE-2022-1551	The SP Project & Document Manager WordPress plugin before 4.58 uses an easily guessable path to store user files, bad actors could use that to access other users'
CVE-2022-1501	Inappropriate implementation in iframe in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-2139	The affected product is vulnerable to directory traversal, which may allow an attacker to access unauthorized files and execute arbitrary code.
CVE-2022-2179	The X-Frame-Options header in Rockwell Automation MicroLogix 1100/1400 Versions 21.007 and prior is not configured in the HTTP response, which could allow click
CVE-2022-34503	QPDF v8.4.2 was discovered to contain a heap buffer overflow via the function QPDF::processXRefStream. This vulnerability allows attackers to cause a Denial of Ser
CVE-2022-22202	An Improper Handling of Exceptional Conditions vulnerability on specific PTX Series devices, including the PTX1000, PTX3000 (NextGen), PTX5000, PTX10002-60C, in Juniper Networks Junos OS allows an unauthenticated MPLS-based attacker to cause a Denial of Service (DoS) by triggering the dcpfe process to crash and FPC to devices, processing specific MPLS packets received on an interface with multiple units configured may cause FPC to restart unexpectedly. Continued receipt and proce sustained Denial of Service (DoS) condition. This issue only affects PTX Series devices utilizing specific FPCs found on PTX1000, PTX3000 (NextGen), PTX5000, PTX PTX10016 Series devices, only if multiple units are configured on the ingress interface, and at least one unit has 'family mpls' *not* configured. See the configuration sa other platforms are affected by this vulnerability. This issue affects: Juniper Networks Junos OS on PTX Series: All versions prior to 19.1R3-S9; 19.2 versions prior to 1 19.3R3-S6; 19.4 versions prior to 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior t 21.1R3-S2; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2; 22.1 versions prior to 22.1R2.
CVE-2022-31146	Wasmtime is a standalone runtime for WebAssembly. There is a bug in the Wasmtime's code generator, Cranelift, where functions using reference types may be incorr runtime garbage collection. This means that if a GC happens at runtime then the GC pass will mistakenly think these functions do not have live references to GC'd valu them. The function will then subsequently continue to use the values assuming they had not been GC'd, leading later to a use-after-free. This bug was introduced in the allocator that occurred in the Wasmtime 0.37.0 release on 2022-05-20. This bug has been patched and users should upgrade to Wasmtime version 0.38.2. Mitigations disabling the reference types proposal by passing `false` to `wasmtime::Config::wasm_reference_types` or downgrading to Wasmtime 0.36.0 or prior.
CVE-2020-28422	All versions of package git-archive are vulnerable to Command Injection via the exports function.
CVE-2022-33923	Dell PowerStore, versions prior to 3.0.0.0, contains an OS Command Injection vulnerability in PowerStore T environment. A locally authenticated attacker could potenti to the execution of arbitrary OS command on the PowerStore underlying OS. Exploiting may lead to a system take over by an attacker.
CVE-2017-20143	A vulnerability, which was classified as critical, has been found in Itech Movie Portal Script 7.36. This issue affects some unknown processing of the file /film-rating.php leads to sql injection (Error). The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-2490	A vulnerability classified as critical has been found in SourceCodester Simple E-Learning System 1.0. Affected is an unknown function of the file search.php. The manip with the input 1'||(SELECT 0x74666264 WHERE 5610=5610 AND (SELECT 7504 FROM(SELECT COUNT(*),CONCAT(0x7171627a71,(SELECT (ELT(7504=7504,1))),0x71717a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))||' leads to sql injection. It is possible to laun has been disclosed to the public and may be used.
CVE-2017-20141	A vulnerability classified as critical has been found in Itech Movie Portal Script 7.36. This affects an unknown part of the file /movie.php. The manipulation of the argume is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-34573	An access control issue in Wavlink WiFi-Repeater RPTA2-77W.M4300.01.GD.2017Sep19 allows attackers to arbitrarily configure device settings via accessing the pag
CVE-2017-20139	A vulnerability was found in Itech Movie Portal Script 7.36. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /show_ne argument id with the input AND (SELECT 1222 FROM(SELECT COUNT(*),CONCAT(0x71786b7a71,(SELECT (ELT(1222=1222,1))),0x717a627871,FLOOR(RAND(0) INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) leads to sql injection (Error). The attack can be launched remotely. The exploit has been disclosed to

CVE Number	Description
CVE-2022-27235	Multiple Broken Access Control vulnerabilities in Social Share Buttons by Supsystic plugin <= 2.2.3 at WordPress.
CVE-2022-2492	A vulnerability was found in SourceCodester Library Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /index.pl argument RollNo with the input admin' AND (SELECT 2625 FROM (SELECT(SLEEP(5)))MdIL) AND 'KXmq'='KXmq&Password=1231312312 leads to sql injection. The The exploit has been disclosed to the public and may be used.
CVE-2022-2491	A vulnerability has been found in SourceCodester Library Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file lab.php. Section with the input 1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x71716b7171,0x546e4444736b7743575a666d4873746a6450616261527a6762794442694650724566414369 4c6a4c,0x716 leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2017-20144	A vulnerability has been found in Anvsoft PDFMate PDF Converter Pro 1.7.5.0 and classified as critical. The manipulation leads to memory corruption. The attack can b has been disclosed to the public and may be used.
CVE-2017-20145	A vulnerability was found in Tecrail Responsive Filemanger up to 9.10.x and classified as critical. The manipulation leads to path traversal. The attack may be launched disclosed to the public and may be used. Upgrading to version 9.11.0 is able to address this issue. It is recommended to upgrade the affected component.
CVE-2017-20142	A vulnerability classified as critical was found in Itech Movie Portal Script 7.36. This vulnerability affects unknown code of the file /artist-display.php. The manipulation o injection (Union). The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-2489	A vulnerability was found in SourceCodester Simple E-Learning System 1.0. It has been rated as critical. This issue affects some unknown processing of the file classR argument classCode with the input 1'll(SELECT 0x6770715a WHERE 8795=8795 AND (SELECT 8342 FROM(SELECT COUNT(*),CONCAT(0x7171786b71,(SELECT (ELT(8342=8342,1))),0x717a7a7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))ll' leads to sql injection. The attack may be i been disclosed to the public and may be used.
CVE-2022-1499	Inappropriate implementation in WebAuthentication in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to bypass same origin policy via a crafted HTM
CVE-2022-2514	The time and filter parameters in Fava prior to v1.22 are vulnerable to reflected XSS due to the lack of escaping of error messages which contained the parameters in v
CVE-2022-35651	A stored XSS and blind SSRF vulnerability was found in Moodle, occurs due to insufficient sanitization of user-supplied data in the SCORM track details. A remote atta specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website to steal potentially sensitive information, change app perform phishing and drive-by-download attacks.
CVE-2022-36131	The Better PDF Exporter add-on 10.0.0 for Atlassian Jira is prone to stored XSS via a crafted description to the PDF Templates overview page.
CVE-2022-35652	An open redirect issue was found in Moodle due to improper sanitization of user-supplied data in mobile auto-login feature. A remote attacker can create a link that lead when clicked, it redirects the victims to arbitrary URL/domain. Successful exploitation of this vulnerability may allow a remote attacker to perform a phishing attack and s information.
CVE-2022-35653	A reflected XSS issue was identified in the LTI module of Moodle. The vulnerability exists due to insufficient sanitization of user-supplied data in the LTI module. A remo follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website to steal potentially sensitive information, cha can perform phishing and drive-by-download attacks. This vulnerability does not impact authenticated users.
CVE-2022-20916	A vulnerability in the web-based management interface of Cisco IoT Control Center could allow an unauthenticated, remote attacker to conduct a cross-site scripting (X interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerabi interface 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, b
CVE-2022-2470	Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.2.21.
CVE-2022-2189	The WP Video Lightbox WordPress plugin before 1.9.5 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which co Scripting in old web browsers
CVE-2022-2523	Cross-site Scripting (XSS) - Reflected in GitHub repository beancount/fava prior to 1.22.2.
CVE-2022-1494	Insufficient data validation in Trusted Types in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to bypass trusted types policy via a crafted HTML page
CVE-2018-25045	Django REST framework (aka django-rest-framework) before 3.9.1 allows XSS because the default DRF Browsable API view templates disable autoescaping.

CVE Number	Description
CVE-2022-1132	Inappropriate implementation in Virtual Keyboard in Google Chrome on Chrome OS prior to 100.0.4896.60 allowed a local attacker to bypass navigation restrictions via
CVE-2022-34048	Wavlink WN533A8 M33A8.V5030.190716 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the login_page parameter.
CVE-2022-2072	The Name Directory WordPress plugin before 1.25.3 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site payload is also saved into the database after the request, it leads to a Stored XSS as well
CVE-2022-1492	Insufficient data validation in Blink Editing in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to inject arbitrary scripts or HTML via a crafted HTML pa
CVE-2022-2115	The Popup Anything WordPress plugin before 2.1.7 does not sanitise and escape a parameter before outputting it back in a frontend page, leading to a Reflected Cros
CVE-2022-31160	jQuery UI is a curated set of user interface interactions, effects, widgets, and themes built on top of jQuery. Versions prior to 1.13.2 are potentially vulnerable to cross-s checkboxradio widget on an input enclosed within a label makes that parent label contents considered as the input label. Calling `.checkboxradio( "refresh" )` on such a contained encoded HTML entities will make them erroneously get decoded. This can lead to potentially executing JavaScript code. The bug has been patched in jQuery someone who can change the initial HTML can wrap all the non-input contents of the `label` in a `span`.
CVE-2022-22217	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent unaut Denial of Service (DoS). The issue is caused by malformed MLD packets looping on a multi-homed Ethernet Segment Identifier (ESI) when VXLAN is configured. Thes homed ESI are sent to the peer, and then incorrectly forwarded out the same ESI, violating the split horizon rule. This issue only affects QFX10K Series switches, inclu QFX10016. Other products and platforms are unaffected by this vulnerability. This issue affects Juniper Networks Junos OS on QFX10K Series: All versions prior to 19 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3 S2; 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2-S1, 21.2R3; 21.3 versions prior to 21.3R2.
CVE-2022-0899	The Header Footer Code Manager WordPress plugin before 1.1.24 does not escape generated URLs before outputting them back in attributes in an admin page, leadi Scripting.
CVE-2022-30706	Open redirect vulnerability in Booked versions prior to 3.3 allows a remote unauthenticated attacker to redirect a user to an arbitrary web site and conduct a phishing at specially crafted URL.
CVE-2022-2071	The Name Directory WordPress plugin before 1.25.4 does not have CSRF check when importing names, and is also lacking sanitisation as well as escaping in some o allow attackers to make a logged in admin import arbitrary names with XSS payloads in them.
CVE-2022-20906	Multiple vulnerabilities in Cisco Nexus Dashboard could allow an authenticated, local attacker to elevate privileges on an affected device. These vulnerabilities are due CLI command execution on an affected device. An attacker could exploit these vulnerabilities by authenticating as the rescue-user and executing vulnerable CLI comm successful exploit could allow the attacker to elevate privileges to root on an affected device.
CVE-2022-20907	Multiple vulnerabilities in Cisco Nexus Dashboard could allow an authenticated, local attacker to elevate privileges on an affected device. These vulnerabilities are due CLI command execution on an affected device. An attacker could exploit these vulnerabilities by authenticating as the rescue-user and executing vulnerable CLI comm successful exploit could allow the attacker to elevate privileges to root on an affected device.
CVE-2022-20908	Multiple vulnerabilities in Cisco Nexus Dashboard could allow an authenticated, local attacker to elevate privileges on an affected device. These vulnerabilities are due CLI command execution on an affected device. An attacker could exploit these vulnerabilities by authenticating as the rescue-user and executing vulnerable CLI comm successful exploit could allow the attacker to elevate privileges to root on an affected device.
CVE-2022-20909	Multiple vulnerabilities in Cisco Nexus Dashboard could allow an authenticated, local attacker to elevate privileges on an affected device. These vulnerabilities are due CLI command execution on an affected device. An attacker could exploit these vulnerabilities by authenticating as the rescue-user and executing vulnerable CLI comm successful exploit could allow the attacker to elevate privileges to root on an affected device.
CVE-2022-22555	Dell EMC PowerStore, contains an OS command injection Vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to the executi PowerStore underlying OS, with the privileges of the vulnerable application. Exploitation may lead to an elevation of privilege.
CVE-2022-29923	Cross-site Scripting (XSS) vulnerability in ThingsForRestaurants Quick Restaurant Reservations (WordPress plugin) allows Reflected XSS.This issue affects Quick Res plugin): from n/a through 1.4.1.
CVE-2022-28861	The server in Citilog 8.0 allows an attacker (in a man in the middle position between the server and its smart camera Axis M1125) to see FTP credentials in a cleartext FTP access to the server.

CVE Number	Description
CVE-2022-31169	Wasmtime is a standalone runtime for WebAssembly. There is a bug in Wasmtime's code generator, Cranelift, for AArch64 targets where constant divisors can result ir This affects Wasmtime prior to version 0.38.2 and Cranelift prior to 0.85.2. This issue only affects the AArch64 platform. Other platforms are not affected. The translatio account whether sign or zero-extension should happen which resulted in an incorrect value being placed into a register when a division was encountered. The impact o within the WebAssembly sandbox would not behave according to the WebAssembly specification. This means that it is hypothetically possible for execution within the s WebAssembly programs could produce unexpected results. This should not impact hosts executing WebAssembly but does affect the correctness of guest programs. T Wasmtime version 0.38.2 and cranelift-codegen 0.85.2. There are no known workarounds.
CVE-2022-34767	Web page which "wizardpwd.asp" ALLNET Router model WR0500AC is prone to Authorization bypass vulnerability – the password, located at "admin" allows changing Does not validate the user's identity and can be accessed publicly.
CVE-2022-22213	A vulnerability in Handling of Undefined Values in the routing protocol daemon (RPD) process of Juniper Networks Junos OS and Junos OS Evolved may allow an una to crash the RPD process by sending a specific BGP update while the system is under heavy load, leading to a Denial of Service (DoS). Continued receipt and process sustained Denial of Service (DoS) condition. Malicious exploitation of this issue requires a very specific combination of load, timing, and configuration of the vulnerable control of the attacker. Internal reproduction has only been possible through artificially created load and specially instrumented source code. Systems are only vulnerab enabled. Routers not configured for BGP multipath are not vulnerable to this issue. This issue affects: Juniper Networks Junos OS: 21.1 versions prior to 21.1R3-S1; 21 21.2R3; 21.3 versions prior to 21.3R2, 21.3R3; 21.4 versions prior to 21.4R1-S1, 21.4R2. Juniper Networks Junos OS Evolved: 21.1 versions prior to 21.1R3-S1-EVO; versions; 21.3 versions prior to 21.3R3-EVO; 21.4 versions prior to 21.4R1-S1-EVO, 21.4R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prio OS Evolved versions prior to 21.1-EVO.
CVE-2022-28860	An authentication downgrade in the server in Citilog 8.0 allows an attacker (in a man in the middle position between the server and its smart camera Axis M1125) to acl
CVE-2022-34839	Authentication Bypass vulnerability in CodexShaper's WP OAuth2 Server plugin <= 1.0.1 at WordPress.
CVE-2021-43959	Affected versions of Atlassian Jira Service Management Server and Data Center allow authenticated remote attackers to access the content of internal network resourc Forgery (SSRF) vulnerability in the CSV importing feature of JSM Insight. When running in an environment like Amazon EC2, this flaw may be used to access to a meta credentials and other potentially confidential information. The affected versions are before version 4.13.20, from version 4.14.0 before 4.20.8, and from version 4.21.0 b
CVE-2022-34572	An access control issue in Wavlink WiFi-Repeater RPTA2-77W.M4300.01.GD.2017Sep19 allows attackers to obtain the telnet password via accessing the page tftp.txt
CVE-2022-1648	Pandora FMS v7.0NG.760 and below allows a relative path traversal in File Manager where a privileged user could upload a .php file outside the intended images direc the .php file. The impact could lead to a Remote Code Execution with running application privilege.
CVE-2022-34574	An access control issue in Wavlink WiFi-Repeater RPTA2-77W.M4300.01.GD.2017Sep19 allows attackers to obtain the key information of the device via accessing Tft
CVE-2022-34575	An access control issue in Wavlink WiFi-Repeater RPTA2-77W.M4300.01.GD.2017Sep19 allows attackers to obtain the key information of the device via accessing fct
CVE-2021-23397	All versions of package @ianwalter/merge are vulnerable to Prototype Pollution via the main (merge) function. Maintainer suggests using @generates/merger instead.
CVE-2021-33442	An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in json_printf() in mjs.c.
CVE-2021-33443	An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is stack buffer overflow in mjs_execute() in mjs.c.
CVE-2021-33441	An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in exec_expr() in mjs.c.
CVE-2021-33440	An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_bcode_commit() in mjs.c.
CVE-2021-33452	An issue was discovered in NASM version 2.16rc0. There are memory leaks in nasm_malloc() in nasmlib/alloc.c.
CVE-2021-33444	An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in getprop_builtin_foreign() in mjs.

CVE Number	Description
CVE-2021-33439	An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is Integer overflow in gc_compact_strings() in mjs.c.
CVE-2021-33447	An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_print() in mjs.c.
CVE-2021-33438	An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is stack buffer overflow in json_parse_array() in mjs.c.
CVE-2021-33437	An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There are memory leaks in frozen_cb() in mjs.c.
CVE-2021-33449	An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_bcode_part_get_by_offset(
CVE-2021-33451	An issue was discovered in lrzip version 0.641. There are memory leaks in fill_buffer() in stream.c.
CVE-2021-33450	An issue was discovered in NASM version 2.16rc0. There are memory leaks in nasm_calloc() in nasmlib/alloc.c.
CVE-2021-33448	An issue was discovered in mjs(mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is stack buffer overflow at 0x7fffe9049390.
CVE-2021-33455	An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in do_directive() in modules/preprocs/nasm/nasm-pp.c.
CVE-2022-22424	IBM QRadar SIEM 7.3, 7.4, and 7.5 could allow a local user to obtain sensitive information from the TLS key file due to incorrect file permissions. IBM X-Force ID: 2235
CVE-2021-33454	An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in yasm_expr_get_intnum() in libyasm/expr.c.
CVE-2021-33445	An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_string_char_code_at() in m
CVE-2021-33456	An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in hash() in modules/preprocs/nasm/nasm-pp.c.
CVE-2021-33467	An issue was discovered in yasm version 1.3.0. There is a use-after-free in pp_getline() in modules/preprocs/nasm/nasm-pp.c.
CVE-2022-29965	The Emerson DeltaV Distributed Control System (DCS) controllers and IO cards through 2022-04-29 misuse passwords. Access to privileged operations on the mainte (23/TCP) on M-series and SIS (CSLS/LSNB/LSNG) nodes is controlled by means of utility passwords. These passwords are generated using a deterministic, insecure composed of a day/hour/minute timestamp with less than 16 bits of entropy. The seed value is fed through a lookup table and a series of permutation operations resulti passwords corresponding to different privilege levels. An attacker can easily reconstruct these passwords and thus gain access to privileged maintenance operations. N 2014-2350.
CVE-2022-29964	The Emerson DeltaV Distributed Control System (DCS) controllers and IO cards through 2022-04-29 misuse passwords. WIOC SSH provides access to a shell as root, credentials. NOTE: this is different from CVE-2014-2350.
CVE-2022-29963	The Emerson DeltaV Distributed Control System (DCS) controllers and IO cards through 2022-04-29 misuse passwords. TELNET on port 18550 provides access to a r This affects S-series, P-series, and CIOC/EIOC nodes. NOTE: this is different from CVE-2014-2350.
CVE-2022-29962	The Emerson DeltaV Distributed Control System (DCS) controllers and IO cards through 2022-04-29 misuse passwords. FTP has hardcoded credentials (but may ofter affects S-series, P-series, and CIOC/EIOC nodes. NOTE: this is different from CVE-2014-2350.
CVE-2022-29960	Emerson OpenBSI through 2022-04-29 uses weak cryptography. It is an engineering environment for the ControlWave and Bristol Babcock line of RTUs. DES with har for protection of certain system credentials, engineering files, and sensitive utilities.

CVE Number	Description
CVE-2022-34502	Radare2 v5.7.0 was discovered to contain a heap buffer overflow via the function consume_encoded_name_new at format/wasm/wasm.c. This vulnerability allows atta (DoS) via a crafted binary file.
CVE-2022-34520	Radare2 v5.7.2 was discovered to contain a NULL pointer dereference via the function r_bin_file_xtr_load_buffer at bin/bfile.c. This vulnerability allows attackers to cau crafted binary file.
CVE-2022-31475	Authenticated (custom plugin role) Arbitrary File Read via Export function vulnerability in GiveWP's GiveWP plugin <= 2.20.2 at WordPress.
CVE-2022-36313	An issue was discovered in the file-type package before 16.5.4 and 17.x before 17.1.3 for Node.js. A malformed MKV file could cause the file type detector to get caugh the application become unresponsive and could be used to cause a DoS attack.
CVE-2021-33457	An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in expand_mmac_params() in modules/preprocs/nasm/nasm-pp.c.
CVE-2022-32498	Dell EMC PowerStore, Versions prior to v3.0.0.0 contain a DLL Hijacking vulnerability in PSTCLI. A local attacker can potentially exploit this vulnerability to execute arb bypass software allow list solutions, leading to system takeover or IP exposure.
CVE-2021-33468	An issue was discovered in yasm version 1.3.0. There is a use-after-free in error() in modules/preprocs/nasm/nasm-pp.c.
CVE-2021-33446	An issue was discovered in mjs (mJS: Restricted JavaScript engine), ES6 (JavaScript version 6). There is NULL pointer dereference in mjs_next() in mjs.c.
CVE-2021-33458	An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in find_cc() in modules/preprocs/nasm/nasm-pp.c.
CVE-2021-33465	An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in expand_mmacro() in modules/preprocs/nasm/nasm-pp.c.
CVE-2021-33459	An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in nasm_parser_directive() in modules/parsers/nasm/nasm-parse.c.
CVE-2021-33464	An issue was discovered in yasm version 1.3.0. There is a heap-buffer-overflow in inc_fopen() in modules/preprocs/nasm/nasm-pp.c.
CVE-2021-33460	An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in if_condition() in modules/preprocs/nasm/nasm-pp.c.
CVE-2021-33463	An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in yasm_expr__copy_except() in libyasm/expr.c.
CVE-2021-33461	An issue was discovered in yasm version 1.3.0. There is a use-after-free in yasm_intnum_destroy() in libyasm/intnum.c.
CVE-2021-33466	An issue was discovered in yasm version 1.3.0. There is a NULL pointer dereference in expand_smacro() in modules/preprocs/nasm/nasm-pp.c.
CVE-2021-33462	An issue was discovered in yasm version 1.3.0. There is a use-after-free in expr_traverse_nodes_post() in libyasm/expr.c.
CVE-2022-21802	The package grapesjs before 0.19.5 are vulnerable to Cross-site Scripting (XSS) due to an improper sanitization of the class name in Selector Manager.
CVE-2022-27105	InMailX Outlook Plugin < 3.22.0101 is vulnerable to Cross Site Scripting (XSS). InMailX Connection names are not sanitzed in the Outlook tab, which allows a local use execute HTML / Javascript in the Outlook of users.

CVE Number	Description
CVE-2022-2494	Cross-site Scripting (XSS) - Stored in GitHub repository openemr/openemr prior to 7.0.0.
CVE-2022-31168	Zulip is an open source team chat tool. Due to an incorrect authorization check in Zulip Server 5.4 and earlier, a member of an organization could craft an API call that g privileges to one of their bots. The vulnerability is fixed in Zulip Server 5.5. Members who don't own any bots, and lack permission to create them, can't exploit the vulne vulnerability, an organization administrator can restrict the `Who can create bots` permission to administrators only, and change the ownership of existing bots.
CVE-2022-34962	OpenTeknik LLC OSSN OPEN SOURCE SOCIAL NETWORK v6.3 LTS was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Group Timeli
CVE-2022-34961	OpenTeknik LLC OSSN OPEN SOURCE SOCIAL NETWORK v6.3 LTS was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Users Timeli
CVE-2022-29495	Cross-Site Request Forgery (CSRF) vulnerability in Sygnoos Popup Builder plugin <= 4.1.11 at WordPress allows an attacker to update plugin settings.
CVE-2021-31858	DotNetNuke (DNN) 9.9.1 CMS is vulnerable to a Stored Cross-Site Scripting vulnerability in the user profile biography section which allows remote authenticated users payload.
CVE-2022-36322	In JetBrains TeamCity before 2022.04.2 build parameter injection was possible
CVE-2020-36290	The Livesearch macro in Confluence Server and Data Center before version 7.4.5, from version 7.5.0 before 7.6.3, and from version 7.7.0 before version 7.7.4 allows r edit a page or blog to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the page excerpt functionality.
CVE-2022-30337	Cross-Site Request Forgery (CSRF) vulnerability in JoomUnited WP Meta SEO plugin <= 4.4.8 at WordPress allows an attacker to update the social settings.
CVE-2022-32289	Cross-Site Request Forgery (CSRF) vulnerability in Sygnoos Popup Builder plugin <= 4.1.0 at WordPress leading to popup status change.
CVE-2022-2299	The Allow SVG Files WordPress plugin through 1.1 does not sanitise uploaded SVG files, which could allow users with a role as low as Author to upload a malicious S\
CVE-2022-34991	Paymoney v3.3 was discovered to contain multiple reflected cross-site scripting (XSS) vulnerabilities via the first_name and last_name parameters.
CVE-2022-34988	Inout Blockchain AltExchanger v1.2.1 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /admin/js.
CVE-2022-34367	Dell EMC Data Protection Central versions 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, contain(s) a Cross-Site Request Forgery Vulnerability. A(n) remote unauthenticated attack vulnerability, leading to processing of unintended server operations.
CVE-2022-34963	OpenTeknik LLC OSSN OPEN SOURCE SOCIAL NETWORK v6.3 LTS was discovered to contain a stored cross-site scripting (XSS) vulnerability via the News Feed r
CVE-2022-22204	An Improper Release of Memory Before Removing Last Reference vulnerability in the Session Initiation Protocol (SIP) Application Layer Gateway (ALG) of Juniper Net unauthenticated network-based attacker to cause a partial Denial of Service (DoS). On all MX and SRX platforms, if the SIP ALG is enabled, receipt of a specific SIP pa Sustained receipt of such packets will cause the SIP call table to eventually fill up and cause a DoS for all SIP traffic. The SIP call usage can be monitored by "show se the SIP ALG needs to be enabled, either implicitly / by default or by way of configuration. Please verify on SRX with: user@host> show security alg status | match sip S whether the following is configured: [services ... rule <rule-name> (term <term-name>) from/match application/application-set <name>] where either a. name = junos-s refers to SIP: b. [applications application <name> application-protocol sip] or c. [applications application-set <name> application junos-sip] This issue affects Juniper and MX Series: 20.4 versions prior to 20.4R3-S2; 21.1 versions prior to 21.1R3-S2; 21.2 versions prior to 21.2R2-S2; 21.2 versions prior to 21.2R3; 21.3 versions prior 21.4R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1. Juniper SIRT is not aware of any malicious exploitation of this vulnerability.
CVE-2022-32457	Digiwin BPM has inadequate filtering for URL parameter. An unauthenticated remote attacker can perform Blind SSRF attack to discover internal network topology bas
CVE-2022-34049	An access control issue in Wavlink WN530HG4 M30HG4.V5030.191116 allows unauthenticated attackers to download log files and configuration data.

CVE Number	Description
CVE-2022-0594	The Professional Social Sharing Buttons, Icons & Related Posts WordPress plugin before 9.7.6 does not have proper authorisation check in one of the AJAX action, av 9.7.5) and author+ (in v9.7.5) users, allowing them to call it and retrieve various information such as the list of active plugins, various version like PHP, cURL, WP etc.
CVE-2022-28666	Broken Access Control vulnerability in YIKES Inc. Custom Product Tabs for WooCommerce plugin <= 1.7.7 at WordPress leading to &yikes-the-content-toggle option u
CVE-2021-36200	Under certain circumstances an unauthenticated user could access the the web API for Metasys ADS/ADX/OAS 10 versions prior to 10.1.6 and 11 versions prior to 11.
CVE-2022-33901	Unauthenticated Arbitrary File Read vulnerability in MultiSafepay plugin for WooCommerce plugin <= 4.13.1 at WordPress.
CVE-2020-36557	A race condition in the Linux kernel before 5.6.2 between the VT_DISALLOCATE ioctl and closing/opening of ttys could lead to a use-after-free.
CVE-2020-36558	A race condition in the Linux kernel before 5.5.7 involving VT_RESIZEX could lead to a NULL pointer dereference and general protection fault.
CVE-2021-40335	A vulnerability exists in the HTTP web interface where the web interface does not sufficiently verify if a well-formed, valid, consistent request was intentionally provided request. This cause a Cross Site Request Forgery (CSRF), which if exploited could lead an attacker to gain unauthorized access to the web application and perform an knowledge of the legitimate user. An attacker, who successfully makes an MSM user who has already established a session to MSM web interface clicks a forged link t sent per E-Mail, could perform harmful command on MSM through its web server interface. This issue affects: Hitachi Energy MSM V2.2 and prior versions.
CVE-2021-40336	A vulnerability exists in the http web interface where the web interface does not validate data in an HTTP header. This causes a possible HTTP response splitting, whic to channel down harmful code into the user's web browser, such as to steal the session cookies. Thus, an attacker who successfully makes an MSM user who has alre web interface clicks a forged link to the MSM web interface, e.g., the link is sent per E-Mail, could trick the user into downloading malicious software onto his computer. MSM V2.2 and prior versions.
CVE-2020-7649	This affects the package snyk-broker before 4.73.0. It allows arbitrary file reads for users with access to Snyk's internal network via directory traversal.
CVE-2022-2137	The affected product is vulnerable to two SQL injections that require high privileges for exploitation and may allow an unauthorized attacker to disclose information
CVE-2021-38936	IBM QRadar SIEM 7.3, 7.4, and 7.5 could disclose highly sensitive information to a privileged user. IBM X-Force ID: 210893.
CVE-2022-20913	A vulnerability in Cisco Nexus Dashboard could allow an authenticated, remote attacker to write arbitrary files on an affected device. This vulnerability is due to insuffici management interface of Cisco Nexus Dashboard. An attacker with Administrator credentials could exploit this vulnerability by uploading a crafted file. A successful exp overwrite arbitrary files on an affected device.
CVE-2022-34964	OpenTeknik LLC OSSN OPEN SOURCE SOCIAL NETWORK v6.3 LTS was discovered to contain a stored cross-site scripting (XSS) vulnerability via the SitePages m
CVE-2022-2239	The Request a Quote WordPress plugin before 2.3.9 does not sanitise and escape some of its settings, allowing high privilege users such as admin to perform cross-S unfiltered_html capability is disallowed.
CVE-2022-35569	Blogifier v3.0 was discovered to contain an arbitrary file upload vulnerability at /api/storage/upload/PostImage. This vulnerability allows attackers to execute arbitrary we
CVE-2022-2340	The W-DALIL WordPress plugin through 2.0 does not sanitise and escape some of its fields, which could allow high privilege users such as admin to perform Stored Cr unfiltered_html capability is disallowed (for example in multisite setup)
CVE-2022-2495	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.2.21.
CVE-2022-2341	The Simple Page Transition WordPress plugin through 1.4.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to attacks when the unfiltered_html capability is disallowed (for example in multisite setup)
CVE-2022-30628	It was possible to download all receipts without authentication. Must first access the API https://XXXX.supersmart.me/services/v4/customer/signin to get a TOKEN. The provides invoice images based on the URL https://XXXX.supersmart.me/services/v4/invoiceImg?orderId=XXXXX

CVE Number	Description
CVE-2022-20894	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20891	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20892	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20893	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20899	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20895	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20896	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20897	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20898	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20888	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20900	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20901	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.

CVE Number	Description
CVE-2022-20902	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20903	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20904	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20910	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20911	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20889	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20890	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20887	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20882	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20873	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20874	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20875	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.

CVE Number	Description
CVE-2022-20876	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20877	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20878	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20879	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20880	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20886	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20881	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20912	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20884	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20883	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-20885	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticate arbitrary code on an affected device or cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. These vulnerabilities are due to insuffic incoming HTTP packets. An attacker could exploit these vulnerabilities by sending a crafted request to the web-based management interface. A successful exploit coul arbitrary commands on an affected device with root-level privileges or to cause the device to restart unexpectedly, resulting in a DoS condition. To exploit these vulnera have valid Administrator credentials on the affected device. Cisco has not released software updates that address these vulnerabilities.
CVE-2022-22412	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a user with access to the local host (client machine) to obtain a login access token. IBM X-Forc
CVE-2022-1637	Inappropriate implementation in Web Contents in Google Chrome prior to 101.0.4951.64 allowed a remote attacker to leak cross-origin data via a crafted HTML page.

CVE Number	Description
CVE-2022-2511	Cross-site Scripting (XSS) vulnerability in the "commonuserinterface" component of BlueSpice allows an attacker to inject arbitrary HTML into a page using the title par
CVE-2022-28877	This vulnerability allows local user to delete arbitrary file in the system and bypassing security protection which can be abused for local privilege escalation on affected endpoint products. An attacker must have code execution rights on the victim machine prior to successful exploitation.
CVE-2022-1495	Incorrect security UI in Downloads in Google Chrome on Android prior to 101.0.4951.41 allowed a remote attacker to spoof the APK downloads dialog via a crafted HTI
CVE-2022-28878	A Denial-of-Service vulnerability was discovered in the F-Secure Atlant and in certain WithSecure products while scanning fuzzed APK file it is possible that can crash t
CVE-2022-28879	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant and in certain WithSecure products whereby the scanning the aepack.dll component can cras
CVE-2022-2510	Cross-site Scripting (XSS) vulnerability in "Extension:ExtendedSearch" of Hallo Welt! GmbH BlueSpice allows attacker to inject arbitrary HTML (XSS) on page "Special term in the URL.
CVE-2022-1488	Inappropriate implementation in Extensions API in Google Chrome prior to 101.0.4951.41 allowed an attacker who convinced a user to install a malicious extension to I Chrome Extension.
CVE-2022-22216	An Exposure of Sensitive Information to an Unauthorized Actor vulnerability in the PFE of Juniper Networks Junos OS on PTX Series and QFX10k Series allows an adj gain access to sensitive information. PTX1000 and PTX10000 Series, and QFX10000 Series and PTX5000 Series devices sometimes do not reliably pad Ethernet pac contain fragments of system memory or data from previous packets. This issue is also known as 'Etherleak' and often detected as CVE-2003-0001. This issue affects: PTX1000 and PTX10000 Series: All versions prior to 18.4R3-S11; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 ver versions prior to 19.4R2-S5, 19.4R3-S6; 20.1 versions prior to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20. 21.1R2-S1, 21.1R3; 21.2 versions prior to 21.2R1-S1, 21.2R2. Juniper Networks Junos OS on QFX10000 Series and PTX5000 Series: All versions prior to 18.3R3-S6; 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S8, 19.2R3-S4; 19.3 versions prior to 19.3R3-S4; 19.4 versions prior to 19.4R to 20.1R3-S2; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3-S1; 21.1 versions prior to 21.1R2-S1, 21.1R3; 21.2 ver
CVE-2017-20140	A vulnerability was found in Itech Movie Portal Script 7.36. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /movie.php. with the input <img src=i onerror=prompt(1)> leads to basic cross site scripting (Reflected). The attack may be launched remotely. The exploit has been disclosed to the
CVE-2022-1307	Inappropriate implementation in full screen in Google Chrome on Android prior to 100.0.4896.88 allowed a remote attacker to spoof the contents of the Omnibox (URL b
CVE-2022-1306	Inappropriate implementation in compositing in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a
CVE-2022-1498	Inappropriate implementation in HTML Parser in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-36321	In JetBrains TeamCity before 2022.04.2 the private SSH key could be written to the build log in some cases
CVE-2022-33191	Authenticated (contributor or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in Chinmoy Paul's Testimonials plugin <= 3.0.1 at WordPress.
CVE-2022-34853	Multiple Authenticated (contributor or higher user role) Persistent Cross-Site Scripting (XSS) vulnerabilities in wpWax Team plugin <= 1.2.6 at WordPress.
CVE-2022-34650	Multiple Authenticated (contributor or higher user role) Stored Cross-Site Scripting (XSS) vulnerabilities in wpWax Team plugin <= 1.2.6 at WordPress.
CVE-2022-31151	Authorization headers are cleared on cross-origin redirect. However, cookie headers which are sensitive headers and are official headers found in the spec, remain unc cookie headers in undici. This may lead to accidental leakage of cookie to a 3rd-party site or a malicious attacker who can control the redirection target (ie. an open red party site. This was patched in v5.7.1. By default, this vulnerability is not exploitable. Do not enable redirections, i.e. `maxRedirections: 0` (the default).
CVE-2022-2032	In Pandora FMS v7.0NG.761 and below, in the file manager section, the dirname parameter is vulnerable to a Stored Cross Site-Scripting. This vulnerability can be exp administrator privileges logged in the system.

CVE Number	Description
CVE-2022-2059	In Pandora FMS v7.0NG.761 and below, in the agent creation section, the alias parameter is vulnerable to a Stored Cross Site-Scripting. This vulnerability can be explo administrator privileges logged in the system.
CVE-2022-30536	Authenticated Stored Cross-Site Scripting (XSS) vulnerability in Florent Maillefaud's WP Maintenance plugin <= 6.0.7 at WordPress.
CVE-2021-36849	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in René Hermenau's Social Media Share Buttons plugin <= 3.8.1 at WordPress.
CVE-2022-29454	Cross-Site Request Forgery (CSRF) vulnerability in WordPlus Better Messages plugin <= 1.9.9.148 at WordPress allows attackers to upload files. File attachment to m
CVE-2022-36408	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-31181. Reason: This candidate is a duplicate of CVE-2022-31181. A typo cause CVE users should reference CVE-2022-31181 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usa
CVE-2022-2209	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This CVE has been rejected as it was incorrectly assigned. All references and descriptions in th prevent accidental usage
CVE-2022-31171	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-31159. Reason: This candidate is a reservation duplicate of CVE-2022-31159. N CVE-2022-31159 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage