SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 14 December 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-2022-46742	Code injection in paddle.audio.functional.get_window in PaddlePaddle 2.4.0-rc0 allows arbitrary code execution.	10.0	More Details
CVE-2022-4390	A network misconfiguration is present in versions prior to 1.0.9.90 of the NETGEAR RAX30 AX2400 series of routers. IPv6 is enabled for the WAN interface by default on these devices. While there are firewall restrictions in place that define access restrictions for IPv4 traffic, these restrictions do not appear to be applied to the WAN interface for IPv6. This allows arbitrary access to any services running on the device that may be inadvertently listening via IPv6, such as the SSH and Telnet servers spawned on ports 22 and 23 by default. This misconfiguration could allow an attacker to interact with services only intended to be accessible by clients on the local network.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41267	SAP Business Objects Platform - versions 420, and 430, allows an attacker with normal BI user privileges to upload/replace any file on Business Objects server at the operating system level, enabling the attacker to take full control of the system causing a high impact on confidentiality, integrity, and availability of the application.	9.9	More Details
CVE-2022-41272	An unauthenticated attacker over the network can attach to an open interface exposed through JNDI by the User Defined Search (UDS) of SAP NetWeaver Process Integration (PI) - version 7.50 and make use of an open naming and directory API to access services which can be used to perform unauthorized operations affecting users and data across the entire system. This allows the attacker to have full read access to user data, make limited modifications to user data, and degrade the performance of the system, leading to a high impact on confidentiality and a limited impact on the availability and integrity of the application.	9.9	More Details
CVE-2022-45010	Simple Phone Book/Directory Web App v1.0 was discovered to contain a SQL injection vulnerability via the editid parameter at /PhoneBook/edit.php.	9.8	More Details
CVE-2022-4446	PHP Remote File Inclusion in GitHub repository tsolucio/corebos prior to 8.0.	9.8	More Details
CVE-2021-3942	Certain HP Print products and Digital Sending products may be vulnerable to potential remote code execution and buffer overflow with use of Link-Local Multicast Name Resolution or LLMNR.	9.8	More Details
CVE-2022-37897	There is a command injection vulnerability that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2022-3900	The Cooked Pro WordPress plugin before 1.7.5.7 does not properly validate or sanitize the recipe_args parameter before unserializing it in the cooked_loadmore action, allowing an unauthenticated attacker to trigger a PHP Object injection vulnerability.	9.8	More Details
CVE-2022-3915	The Dokan WordPress plugin before 3.7.6 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by unauthenticated users	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3921	The Listingo WordPress theme before 3.2.7 does not validate files to be uploaded via an AJAX action available to unauthenticated users, which could allow them to upload arbitrary files and lead to RCE	9.8	More Details
CVE-2022-3982	The Booking calendar, Appointment Booking System WordPress plugin before 3.2.2 does not validate uploaded files, which could allow unauthenticated users to upload arbitrary files, such as PHP and achieve RCE	9.8	More Details
CVE-2022-4314	Improper Privilege Management in GitHub repository ikus060/rdiffweb prior to 2.5.2.	9.8	More Details
CVE-2022-20472	In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239210579	9.8	More Details
CVE-2022-45025	Markdown Preview Enhanced v0.6.5 and v0.19.6 for VSCode and Atom was discovered to contain a command injection vulnerability via the PDF file import function.	9.8	More Details
CVE-2022-20473	In toLanguageTag of LocaleListCache.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239267173	9.8	More Details
CVE-2022-43724	A vulnerability has been identified in SICAM PAS/PQS (All versions < V7.0). Affected software transmits the database credentials for the inbuilt SQL server in cleartext. In combination with the by default enabled xp_cmdshell feature unauthenticated remote attackers could execute custom OS commands. At the time of assigning the CVE, the affected firmware version of the component has already been superseded by succeeding mainline versions.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46353	A vulnerability has been identified in SCALANCE X204RNA (HSR) (All versions < V3.2.7), SCALANCE X204RNA (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (HSR) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP/HSR) (All versions < V3.2.7). The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions.	9.8	More Details
CVE-2022-27518	Unauthenticated remote arbitrary code execution	9.8	More Details
CVE-2022-46364	A SSRF vulnerability in parsing the href attribute of XOP:Include in MTOM requests in versions of Apache CXF before 3.5.5 and 3.4.10 allows an attacker to perform SSRF style attacks on webservices that take at least one parameter of any type.	9.8	More Details
CVE-2022-45005	IP-COM EW9 V15.11.0.14(9732) was discovered to contain a command injection vulnerability in the cmd_get_ping_output function.	9.8	More Details
CVE-2022-46404	A command injection vulnerability has been identified in Atos Unify OpenScape 4000 Assistant and Unify OpenScape 4000 Manager (8 before R2.22.18, 10 before 0.28.13, and 10 R1 before R1.34.4) that may allow an unauthenticated attacker to upload arbitrary files and achieve administrative access to the system.	9.8	More Details
CVE-2022-2660	Delta Industrial Automation DIALink versions 1.4.0.0 and prior are vulnerable to the use of a hard-coded cryptographic key which could allow an attacker to decrypt sensitive data and compromise the machine.	9.8	More Details
CVE-2022-2757	Due to the lack of adequately implemented access-control rules, all versions Kingspan TMS300 CS are vulnerable to an attacker viewing and modifying the application settings without authenticating by accessing a specific uniform resource locator (URL) on the webserver.	9.8	More Details
CVE-2021-3919	A potential security vulnerability has been identified in OMEN Gaming Hub and in HP Command Center which may allow escalation of privilege and/or denial of service. HP has released software updates to mitigate the potential vulnerability.	9.8	More Details
CVE-2021-3821	A potential security vulnerability has been identified for certain HP multifunction printers (MFPs). The vulnerability may lead to Denial of Service when running HP Workpath solutions on potentially affected products.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3437	Potential security vulnerabilities have been identified in an OMEN Gaming Hub SDK package which may allow escalation of privilege and/or denial of service. HP is releasing software updates to mitigate the potential vulnerabilities.	9.8	More Details
CVE-2022-3485	In IFM Moneo Appliance with version up to 1.9.3 an unauthenticated remote attacker can reset the administrator password by only supplying the serial number and thus gain full control of the device.	9.8	More Details
CVE-2022-45026	An issue in Markdown Preview Enhanced v0.6.5 and v0.19.6 for VSCode and Atom allows attackers to execute arbitrary commands during the GFM export process.	9.8	More Details
CVE-2022-42458	Authentication bypass using an alternate path or channel vulnerability in bingo!CMS version1.7.4.1 and earlier allows a remote unauthenticated attacker to upload an arbitrary file. As a result, an arbitrary script may be executed and/or a file may be altered.	9.8	More Details
CVE-2022-44371	hope-boot 1.0.0 has a deserialization vulnerability that can cause Remote Code Execution (RCE).	9.8	More Details
CVE-2022-44351	Skycaiji v2.5.1 was discovered to contain a deserialization vulnerability via /SkycaijiApp/admin/controller/Mystore.php.	9.8	More Details
CVE-2022-45550	AyaCMS 3.1.2 is vulnerable to Remote Code Execution (RCE).	9.8	More Details
CVE-2022-45497	Tenda W6-S v1.0.0.4(510) was discovered to contain a command injection vulnerability in the tpi_get_ping_output function at /goform/exeCommand.	9.8	More Details
CVE-2022-45506	Tenda W30E v1.0.1.25(633) was discovered to contain a command injection vulnerability via the fileNameMit parameter at /goform/delFileName.	9.8	More Details
CVE-2022-44938	Weak reset token generation in SeedDMS v6.0.20 and v5.1.7 allows attackers to execute a full account takeover via a brute force attack.	9.8	More Details
CVE-2022-33186	A vulnerability in Brocade Fabric OS software v9.1.1, v9.0.1e, v8.2.3c, v7.4.2j, and earlier versions could allow a remote unauthenticated attacker to execute on a Brocade Fabric OS switch commands capable of modifying zoning, disabling the switch, disabling ports, and modifying the switch IP address.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41653	Daikin SVMPC1 version 2.1.22 and prior and SVMPC2 version 1.2.3 and prior are vulnerable to an attacker obtaining user login credentials and control the system.	9.8	More Details
CVE-2022-4170	The rxvt-unicode package is vulnerable to a remote code execution, in the Perl background extension, when an attacker can control the data written to the user's terminal and certain options are set.	9.8	More Details
CVE-2022-45145	egg-compile.scm in CHICKEN 5.x before 5.3.1 allows arbitrary OS command execution during package installation via escape characters in a .egg file.	9.8	More Details
CVE-2022-46682	Jenkins Plot Plugin 2.1.11 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	9.8	More Details
CVE-2022-23510	cube-js is a headless business intelligence platform. In version 0.31.23 all authenticated Cube clients could bypass SQL row-level security and run arbitrary SQL via the newly introduced /v1/sql-runner endpoint. This issue has been resolved in version 0.31.24. Users are advised to either upgrade to 0.31.24 or to downgrade to 0.31.22. There are no known workarounds for this vulnerability.	9.6	More Details
CVE-2022-41271	An unauthenticated user can attach to an open interface exposed through JNDI by the Messaging System of SAP NetWeaver Process Integration (PI) - version 7.50. This user can make use of an open naming and directory API to access services that could perform unauthorized operations. The vulnerability affects local users and data, leading to a considerable impact on confidentiality as well as availability and a limited impact on the integrity of the application. These operations can be used to: * Read any information * Modify sensitive information * Denial of Service attacks (DoS) * SQL Injection	9.4	More Details
CVE-2022-23478	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a Out of Bound Write in xrdp_mm_trans_process_drdynvc_channel_open() function. There are no known workarounds for this issue. Users are advised to upgrade.	9.1	More Details
CVE-2022-23479	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a buffer over flow in xrdp_mm_chan_data_in() function. There are no known workarounds for this issue. Users are advised to upgrade.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23480	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a buffer over flow in devredir_proc_client_devlist_announce_req() function. There are no known workarounds for this issue. Users are advised to upgrade.	9.1	More Details
CVE-2022-23493	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a Out of Bound Read in xrdp_mm_trans_process_drdynvc_channel_close() function. There are no known workarounds for this issue. Users are advised to upgrade.	9.1	More Details
CVE-2022-41561	The JNDI Data Sources component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server - Community Edition, TIBCO JasperReports Server - Developer Edition, TIBCO JasperReports Server for AWS Marketplace, TIBCO JasperReports Server for AWS Marketplace, TIBCO JasperReports Server for Microsoft Azure, and TIBCO JasperReports Server for Microsoft Azure contains an easily exploitable vulnerability that allows a privileged/administrative attacker with network access to execute Remote Code Execution to obtain a reverse shell on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions 8.0.2 and below, TIBCO JasperReports Server: version 8.1.0, TIBCO JasperReports Server - Community Edition: versions 8.1.0 and below, TIBCO JasperReports Server - Developer Edition: versions 8.1.0 and below, TIBCO JasperReports Server for AWS Marketplace: versions 8.0.2 and below, TIBCO JasperReports Server for AWS Marketplace: version 8.1.0, TIBCO JasperReports Server for Microsoft Azure: versions 8.0.2 and below, and TIBCO JasperReports Server for Microsoft Azure: version 8.1.0.	9.1	More Details
CVE-2022-45290	Kbase Doc v1.0 was discovered to contain an arbitrary file deletion vulnerability via the component /web/IndexController.java.	9.1	More Details
CVE-2022-23477	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a buffer over flow in audin_send_open() function. There are no known workarounds for this issue. Users are advised to upgrade.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41563	The Dashboard component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server - Developer Edition, TIBCO JasperReports Server for AWS Marketplace, TIBCO JasperReports Server for AWS Marketplace, TIBCO JasperReports Server for Microsoft Azure, and TIBCO JasperReports Server for Microsoft Azure contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute Stored Cross Site Scripting (XSS) on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions 8.0.2 and below, TIBCO JasperReports Server: version 8.1.0, TIBCO JasperReports Server - Developer Edition: versions 8.1.0 and below, TIBCO JasperReports Server for AWS Marketplace: versions 8.0.2 and below, TIBCO JasperReports Server for AWS Marketplace: version 8.1.0, TIBCO JasperReports Server for Microsoft Azure: versions 8.0.2 and below, and TIBCO JasperReports Server for Microsoft Azure: version 8.1.0.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-29580	There exists a path traversal vulnerability in the Android Google Search app. This is caused by the incorrect usage of uri.getLastPathSegment. A symbolic encoded string can bypass the path logic to get access to unintended directories. An attacker can manipulate paths that could lead to code execution on the device. We recommend upgrading beyond version 13.41	8.9	More Details
CVE-2022-43464	Hidden functionality vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings.	8.8	More Details
CVE-2022-45937	A vulnerability has been identified in APOGEE PXC Compact (BACnet) (All versions < V3.5.5), APOGEE PXC Compact (P2 Ethernet) (All versions < V2.8.20), APOGEE PXC Modular (BACnet) (All versions < V3.5.5), APOGEE PXC Modular (P2 Ethernet) (All versions < V2.8.20), TALON TC Compact (BACnet) (All versions < V3.5.5), TALON TC Modular (BACnet) (All versions < V3.5.5). A low privilege authenticated attacker with network access to the integrated web server could download sensitive information from the device containing user account credentials.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44606	OS command injection vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings.	8.8	More Details
CVE-2022-44620	Improper authentication vulnerability in UDR-JA1604/UDR-JA1608/UDR-JA1616 firmware versions 71x10.1.107112.43A and earlier allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings.	8.8	More Details
CVE-2022-20411	In avdt_msg_asmbl of avdt_msg.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-232023771	8.8	More Details
CVE-2022-44690	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
	Authentication bypass vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to bypass authentication and access the device. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WRM-D2133HP firmware Ver. 2.85 and earlier, WRM-D2133HS firmware Ver. 2.96 and earlier, WTR-M2133HP firmware Ver. 2.85 and earlier, WTR-M2133HS firmware Ver. 2.96 and earlier, WXR-1900DHP firmware Ver. 2.50 and earlier, WXR-1900DHP2 firmware Ver. 2.59 and earlier, WXR-1900DHP3 firmware Ver. 2.63 and earlier, WXR-5950AX12 firmware Ver. 3.40 and earlier, WXR-6000AX12B firmware Ver. 3.40 and earlier, WXR-6000AX12S firmware Ver. 3.40 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-1750DHP2 firmware Ver. 2.31 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-		

CVE Number	Description	Base Score	Reference
	HP-G302H firmware Ver. 1.86 and earlier, WEM-1266 firmware Ver. 2.85 and earlier, WEM-1266WP firmware Ver. 2.85 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40		
CVE-2022-40966	and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WXR-1750DHP firmware Ver. 2.60 and earlier, WXR-1750DHP2 firmware Ver. 2.60 and earlier, WZR-1166DHP firmware Ver. 2.18 and earlier, WZR-1166DHP2 firmware Ver. 2.18 and earlier, WZR-1750DHP firmware Ver. 2.30 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-600DHP3 firmware Ver. 2.19 and earlier, WZR-900DHP2 firmware Ver. 2.19 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, WZR-HP-G450H firmware Ver. 1.90 and earlier, WZR-S1750DHP firmware Ver. 2.32 and earlier, WZR-S600DHP firmware Ver. 2.19 and earlier, and WZR-S900DHP firmware Ver. 2.19 and earlier.	8.8	More Details
CVE-2022-45760	SENS v1.0 is vulnerable to Incorrect Access Control vulnerability.	8.8	More Details
CVE-2022-45977	Tenda AX12 V22.03.01.21_CN was found to have a command injection vulnerability via /goform/setMacFilterCfg function.	8.8	More Details
CVE-2022-44693	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45759	SENS v1.0 has a file upload vulnerability.	8.8	More Details
CVE-2022-44373	A stack overflow vulnerability exists in TrendNet Wireless AC Easy-Upgrader TEW-820AP (Version v1.0R, firmware version 1.01.B01) which may result in remote code execution.	8.8	More Details
CVE-2022-3981	The Icegram Express WordPress plugin before 5.5.1 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by any authenticated users, such as subscriber	8.8	More Details
CVE-2022-37932	A potential security vulnerability has been identified in Hewlett Packard Enterprise OfficeConnect 1820, 1850, and 1920S Network switches. The vulnerability could be remotely exploited to allow authentication bypass. HPE has made the following software updates to resolve the vulnerability in Hewlett Packard Enterprise OfficeConnect 1820, 1850 and 1920S Network switches versions: Prior to PT.02.14; Prior to PC.01.22; Prior to PO.01.21; Prior to PD.02.22;	8.8	More Details
CVE-2022-46792	Hasura GraphQL Engine before 2.15.2 mishandles row-level authorization in the Update Many API for Postgres backends. The fixed versions are 2.10.2, 2.11.3, 2.12.1, 2.13.2, 2.14.1, and 2.15.2. (Versions before 2.10.0 are unaffected.)	8.8	More Details
CVE-2022-3989	The Motors WordPress plugin before 1.4.4 does not properly validate uploaded files for dangerous file types (such as .php) in an AJAX action, allowing an attacker to sign up on a victim's WordPress instance, upload a malicious PHP file and attempt to launch a brute-force attack to discover the uploaded payload.	8.8	More Details
CVE-2022-3641	Elevation of privilege in the Azure SQL Data Source in Devolutions Remote Desktop Manager 2022.3.13 to 2022.3.24 allows an authenticated user to spoof a privileged account.	8.8	More Details
CVE-2022-31696	VMware ESXi contains a memory corruption vulnerability that exists in the way it handles a network socket. A malicious actor with local access to ESXi may exploit this issue to corrupt memory leading to an escape of the ESXi sandbox.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41264	Due to the unrestricted scope of the RFC function module, SAP BASIS - versions 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, 791, allows an authenticated non-administrator attacker to access a system class and execute any of its public methods with parameters provided by the attacker. On successful exploitation the attacker can have full control of the system to which the class belongs, causing a high impact on the integrity of the application.	8.8	More Details
CVE-2022-44849	A Cross-Site Request Forgery (CSRF) in the Administrator List of MetInfo v7.7 allows attackers to arbitrarily add Super Administrator account.	8.8	More Details
CVE-2022-3359	The Shortcodes and extra features for Phlox theme WordPress plugin before 2.10.7 unserializes the content of an imported file, which could lead to PHP object injection when a user imports (intentionally or not) a malicious file and a suitable gadget chain is present on the blog.	8.8	More Details
CVE-2022-4223	The pgAdmin server includes an HTTP API that is intended to be used to validate the path a user selects to external PostgreSQL utilities such as pg_dump and pg_restore. The utility is executed by the server to determine what PostgreSQL version it is from. Versions of pgAdmin prior to 6.17 failed to properly secure this API, which could allow an unauthenticated user to call it with a path of their choosing, such as a UNC path to a server they control on a Windows machine. This would cause an appropriately named executable in the target path to be executed by the pgAdmin server.	8.8	More Details
CVE-2022-45915	ILIAS before 7.16 allows OS Command Injection.	8.8	More Details
CVE-2022-45043	Tenda AX12 V22.03.01.16_cn is vulnerable to command injection via goform/fast_setting_internet_set.	8.8	More Details
CVE-2022-42716	An issue was discovered in the Arm Mali GPU Kernel Driver. There is a use-after-free. A non-privileged user can make improper GPU processing operations to gain access to already freed memory. This affects Valhall r29p0 through r40P0.	8.8	More Details
CVE-2022-20469	In avct_lcb_msg_asmbl of avct_lcb_act.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-230867224	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41622	In all versions, BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.8	More Details
CVE-2022-45968	Alist v3.4.0 is vulnerable to File Upload. A user with only file upload permission can upload any file to any folder (even a password protected one).	8.8	More Details
CVE-2022-46157	Akeneo PIM is an open source Product Information Management (PIM). Akeneo PIM Community Edition versions before v5.0.119 and v6.0.53 allows remote authenticated users to execute arbitrary PHP code on the server by uploading a crafted image. Akeneo PIM Community Edition after the versions aforementioned provides patched Apache HTTP server configuration file, for docker setup and in documentation sample, to fix this vulnerability. Community Edition users must change their Apache HTTP server configuration accordingly to be protected. The patch for Cloud Based Akeneo PIM Services customers has been applied since 30th October 2022. Users are advised to upgrade. Users unable to upgrade may Replace any reference to `<FilesMatch \.php$>` in their apache httpd configurations with: `<Location "/index.php">`.	8.8	More Details
CVE-2022-45980	Tenda AX12 V22.03.01.21_CN was discovered to contain a Cross-Site Request Forgery (CSRF) via /goform/SysToolRestoreSet .	8.8	More Details
CVE-2022-41800	In all versions of BIG-IP, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2022-2993	There is an error in the condition of the last if-statement in the function smp_check_keys. It was rejecting current keys if all requirements were unmet.	8.6	More Details
CVE-2022-38656	HCL Commerce, when using Elasticsearch, can allow a remote attacker to cause a denial of service attack on the site and make administrative changes.	8.6	More Details
CVE-2022-41127	Microsoft Dynamics NAV and Microsoft Dynamics 365 Business Central (On Premises) Remote Code Execution Vulnerability	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41076	PowerShell Remote Code Execution Vulnerability	8.5	More Details
CVE-2022-41268	In some SAP standard roles in SAP Business Planning and Consolidation - versions - SAP_BW 750, 751, 752, 753, 754, 755, 756, 757, DWCORE 200, 300, CPMBPC 810, a transaction code reserved for the customer is used. By implementing such transaction code, a malicious user may execute unauthorized transaction functionality. Under specific circumstances, a successful attack could enable an adversary to escalate their privileges to be able to read, change or delete system data.	8.5	More Details
CVE-2022-25695	Memory corruption in MODEM due to Improper Validation of Array Index while processing GSTK Proactive commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2022-25697	Memory corruption in i2c buses due to improper input validation while reading address configuration from i2c driver in Snapdragon Mobile, Snapdragon Wearables	8.4	More Details
CVE-2022-37018	A potential vulnerability has been identified in the system BIOS for certain HP PC products which may allow escalation of privileges and code execution. HP is releasing firmware updates to mitigate the potential vulnerability.	8.4	More Details
CVE-2022-41562	The HTML escaping component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server, TIBCO JasperReports Server - Community Edition, TIBCO JasperReports Server - Developer Edition, TIBCO JasperReports Server for AWS Marketplace, TIBCO JasperReports Server for AWS Marketplace, TIBCO JasperReports Server for Microsoft Azure, and TIBCO JasperReports Server for Microsoft Azure contains an easily exploitable vulnerability that allows a privileged/administrative attacker with network access to execute an XSS attack on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions 8.0.2 and below, TIBCO JasperReports Server: version 8.1.0, TIBCO JasperReports Server - Community Edition: versions 8.1.0 and below, TIBCO JasperReports Server - Developer Edition: versions 8.1.0 and below, TIBCO JasperReports Server for AWS Marketplace: versions 8.0.2 and below, TIBCO JasperReports Server for AWS Marketplace: version 8.1.0, TIBCO JasperReports Server for Microsoft Azure: versions 8.0.2 and below, and TIBCO JasperReports Server for Microsoft Azure: version 8.1.0.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25698	Memory corruption in SPI buses due to improper input validation while reading address configuration from spi buses in Snapdragon Mobile, Snapdragon Wearables	8.4	More Details
CVE-2022-25682	Memory corruption in MODEM UIM due to usage of out of range pointer offset while decoding command from card in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-3661	A potential security vulnerability has been identified in certain HP Workstation BIOS (UEFI firmware) which may allow arbitrary code execution. HP is releasing firmware mitigations for the potential vulnerability.	8.4	More Details
CVE-2022-25681	Possible memory corruption in kernel while performing memory access due to hypervisor not correctly invalidated the processor translation caches in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details
CVE-2022-44708	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45877	OpenHarmony-v3.1.4 and prior versions had an vulnerability. PIN code is transmitted to the peer device in plain text during cross-device authentication, which reduces the difficulty of man-in-the-middle attacks.	8.3	More Details
CVE-2022-23484	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a Integer Overflow in xrdp_mm_process_rail_update_window_text() function. There are no known workarounds for this issue. Users are advised to upgrade.	8.2	More Details
CVE-2022-33268	Information disclosure due to buffer over-read in Bluetooth HOST while pairing and connecting A2DP. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	8.2	More Details
CVE-2022-33235	Information disclosure due to buffer over-read in WLAN firmware while parsing security context info attributes. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	8.2	More Details
CVE-2022-37916	Vulnerabilities in the AirWave Management Platform web-based management interface exist which expose some URLs to a lack of proper access controls. These vulnerabilities could allow a remote attacker with limited privileges to gain access to sensitive information and/or change network configurations with privileges at a higher effective level in Aruba AirWave Management Platform version(s): 8.2.15.0 and below.	8.1	More Details
CVE-2022-37917	Vulnerabilities in the AirWave Management Platform web-based management interface exist which expose some URLs to a lack of proper access controls. These vulnerabilities could allow a remote attacker with limited privileges to gain access to sensitive information and/or change network configurations with privileges at a higher effective level in Aruba AirWave Management Platform version(s): 8.2.15.0 and below.	8.1	More Details
CVE-2022-37918	Vulnerabilities in the AirWave Management Platform web-based management interface exist which expose some URLs to a lack of proper access controls. These vulnerabilities could allow a remote attacker with limited privileges to gain access to sensitive information and/or change network configurations with privileges at a higher effective level in Aruba AirWave Management Platform version(s): 8.2.15.0 and below.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45936	A vulnerability has been identified in Mendix Email Connector (All versions < V2.0.0). Affected versions of the module improperly handle access control for some module entities. This could allow authenticated remote attackers to read and manipulate sensitive information.	8.1	More Details
CVE-2022-44670	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-20968	A vulnerability in the Cisco Discovery Protocol processing feature of Cisco IP Phone 7800 and 8800 Series firmware could allow an unauthenticated, adjacent attacker to cause a stack overflow on an affected device. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device.	8.1	More Details
CVE-2022-44676	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-3262	A flaw was found in Openshift. A pod with a DNSPolicy of "ClusterFirst" may incorrectly resolve the hostname based on a service provided. This flaw allows an attacker to supply an incorrect name with the DNS search policy, affecting confidentiality and availability.	8.1	More Details
CVE-2022-44942	Casdoor before v1.126.1 was discovered to contain an arbitrary file deletion vulnerability via the uploadFile function.	8.1	More Details
CVE-2022-3999	The DPD Baltic Shipping WordPress plugin before 1.2.57 does not have authorisation and CSRF in an AJAX action, which could allow any authenticated users, such as subscriber to delete arbitrary options from the blog, which could make the blog unavailable.	8.1	More Details
CVE-2022-46664	A vulnerability has been identified in Mendix Workflow Commons (All versions < V2.4.0), Mendix Workflow Commons V2.1 (All versions < V2.1.4), Mendix Workflow Commons V2.3 (All versions < V2.3.2). Affected versions of the module improperly handle access control for some module entities. This could allow authenticated remote attackers to read or delete sensitive information.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46153	Traefik is an open source HTTP reverse proxy and load balancer. In affected versions there is a potential vulnerability in Traefik managing TLS connections. A router configured with a not well-formatted TLSOption is exposed with an empty TLSOption. For instance, a route secured using an mTLS connection set with a wrong CA file is exposed without verifying the client certificates. Users are advised to upgrade to version 2.9.6. Users unable to upgrade should check their logs to detect the error messages and fix your TLS options.	8.1	More Details
CVE-2022-37928	Insufficient Verification of Data Authenticity vulnerability in Hewlett Packard Enterprise HPE Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays.	8.0	More Details
CVE-2022-41266	Due to a lack of proper input validation, SAP Commerce Webservices 2.0 (Swagger UI) - versions 1905, 2005, 2105, 2011, 2205, allows malicious inputs from untrusted sources, which can be leveraged by an attacker to execute a DOM Cross-Site Scripting (XSS) attack. As a result, an attacker may be able to steal user tokens and achieve a full account takeover including access to administrative tools in SAP Commerce.	8.0	More Details
CVE-2022-4098	Multiple Wiesemann&Theis products of the ComServer Series are prone to an authentication bypass through IP spoofing. After a user logged in to the WBM of the Com-Server an unauthenticated attacker in the same subnet can obtain the session ID and through IP spoofing change arbitrary settings by crafting modified HTTP Get requests. This may result in a complete takeover of the device.	8.0	More Details
CVE-2022-46166	Spring boot admins is an open source administrative user interface for management of spring boot applications. All users who run Spring Boot Admin Server, having enabled Notifiers (e.g. Teams-Notifier) and write access to environment variables via UI are affected. Users are advised to upgrade to the most recent releases of Spring Boot Admin 2.6.10 and 2.7.8 to resolve this issue. Users unable to upgrade may disable any notifier or disable write access (POST request) on `/env` actuator endpoint.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38754	A potential vulnerability has been identified in Micro Focus Operations Bridge - Containerized. The vulnerability could be exploited by a malicious authenticated OBM (Operations Bridge Manager) user to run Java Scripts in the browser context of another OBM user. Please note: The vulnerability is only applicable if the Operations Bridge Manager capability is deployed. A potential vulnerability has been identified in Micro Focus Operations Bridge Manager (OBM). The vulnerability could be exploited by a malicious authenticated OBM user to run Java Scripts in the browser context of another OBM user. This issue affects: Micro Focus Micro Focus Operations Bridge Manager versions prior to 2022.11. Micro Focus Micro Focus Operations Bridge- Containerized versions prior to 2022.11.	8.0	More Details
CVE-2022-43722	A vulnerability has been identified in SICAM PAS/PQS (All versions < V7.0). Affected software does not properly secure a folder containing library files. This could allow an attacker to place a custom malicious DLL in this folder which is then run with SYSTEM rights when a service is started that requires this DLL. At the time of assigning the CVE, the affected firmware version of the component has already been superseded by succeeding mainline versions.	7.8	More Details
CVE-2022-20486	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242703118	7.8	More Details
CVE-2022-26806	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-26805	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-43517	A vulnerability has been identified in Simcenter STAR-CCM+ (All versions < V2306). The affected application improperly assigns file permissions to installation folders. This could allow a local attacker with an unprivileged account to override or modify the service executables and subsequently gain elevated privileges.	7.8	More Details
CVE-2022-26804	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20485	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242702935	7.8	More Details
CVE-2022-20487	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242703202	7.8	More Details
CVE-2022-1038	A potential security vulnerability has been identified in the HP Jumpstart software, which might allow escalation of privilege. HP is recommending that customers uninstall HP Jumpstart and use myHP software.	7.8	More Details
CVE-2022-41286	A vulnerability has been identified in JT2Go (All versions < V14.1.0.6), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.8), Teamcenter Visualization V14.0 (All versions < V14.0.0.4), Teamcenter Visualization V14.1 (All versions < V14.1.0.6). The CGM_NIST_Loader.dll contains an out of bounds write vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2022-20488	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242703217	7.8	More Details
CVE-2022-20480	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764350	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41285	A vulnerability has been identified in JT2Go (All versions < V14.1.0.6), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.8), Teamcenter Visualization V14.0 (All versions < V14.0.0.4), Teamcenter Visualization V14.1 (All versions < V14.1.0.6). The CGM_NIST_Loader.dll contains a use-after-free vulnerability that could be triggered while parsing specially crafted CGM files. An attacker could leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2022-20495	In getEnabledAccessibilityServiceList of AccessibilityManager.java, there is a possible way to hide an accessibility service due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-243849844	7.8	More Details
CVE-2022-44668	Windows Media Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-46345	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.264), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170), Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2022 (All versions), Solid Edge SE2023 (All versions < V223.0Update2). The affected applications contain an out of bounds write past the end of an allocated structure while parsing specially crafted X_B files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19070)	7.8	More Details
CVE-2022-44667	Windows Media Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-41077	Windows Fax Compose Form Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-20611	In deletePackageVersionedInternal of DeletePackageHelper.java, there is a possible way to bypass carrier restrictions due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242996180	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41089	.NET Framework Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-41094	Windows Hyper-V Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-4398	Integer Overflow or Wraparound in GitHub repository radareorg/radare2 prior to 5.8.0.	7.8	More Details
CVE-2022-46346	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.264), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170), Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2022 (All versions), Solid Edge SE2023 (All versions < V223.0Update2). The affected applications contain an out of bounds write past the end of an allocated structure while parsing specially crafted X_B files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19071)	7.8	More Details
CVE-2022-46347	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.264), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170), Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2022 (All versions), Solid Edge SE2023 (All versions < V223.0Update2). The affected applications contain an out of bounds write past the end of an allocated structure while parsing specially crafted X_B files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19079)	7.8	More Details
CVE-2022-41121	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-41284	A vulnerability has been identified in JT2Go (All versions < V14.1.0.6), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.8), Teamcenter Visualization V14.0 (All versions < V14.0.0.4), Teamcenter Visualization V14.1 (All versions < V14.1.0.6). The CGM_NIST_Loader.dll contains an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46348	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.264), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170), Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2022 (All versions), Solid Edge SE2023 (All versions < V223.0Update2). The affected applications contain an out of bounds write past the end of an allocated structure while parsing specially crafted X_B files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19383)	7.8	More Details
CVE-2022-44666	Windows Contacts Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-44671	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-46349	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.264), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.170), Solid Edge SE2022 (All versions < V222.0MP12), Solid Edge SE2022 (All versions), Solid Edge SE2023 (All versions < V223.0Update2). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_B files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19384)	7.8	More Details
CVE-2022-20484	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242702851	7.8	More Details
CVE-2022-44681	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-44675	Windows Bluetooth Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-47212	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44704	Microsoft Windows System Monitor (Sysmon) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-20474	In readLazyValue of Parcel.java, there is a possible loading of arbitrary code into the System Settings app due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-240138294	7.8	More Details
CVE-2022-44677	Windows Projected File System Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-44710	DirectX Graphics Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-3092	GE CIMPICITY versions 2022 and prior is vulnerable to an out-of-bounds write, which could allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2022-3084	GE CIMPICITY versions 2022 and prior is vulnerable when data from a faulting address controls code flow starting at gmmiObj!CGmmiRootOptionTable, which could allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2022-2952	GE CIMPICITY versions 2022 and prior is vulnerable when data from a faulting address controls code flow starting at gmmiObj!CGmmiOptionContainer, which could allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2022-2948	GE CIMPICITY versions 2022 and prior is vulnerable to a heap-based buffer overflow, which could allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2022-2002	GE CIMPICITY versions 2022 and prior is vulnerable when data from faulting address controls code flow starting at gmmiObj!CGmmiOptionContainer, which could allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2021-32415	EXEMSI MSI Wrapper Versions prior to 10.0.50 and at least since version 6.0.91 will introduce a local privilege escalation vulnerability in installers it creates.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38395	HP Support Assistant uses HP Performance Tune-up as a diagnostic tool. HP Support Assistant uses Fusion to launch HP Performance Tune-up. It is possible for an attacker to exploit the DLL hijacking vulnerability and elevate privileges when Fusion launches the HP Performance Tune-up.	7.8	More Details
CVE-2022-47211	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-47213	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-20475	In test of ResetTargetTaskHelper.java, there is a possible hijacking of any app which sets allowTaskReparenting="true" due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-240663194	7.8	More Details
CVE-2022-2947	Altair HyperView Player versions 2021.1.0.27 and prior perform operations on a memory buffer but can read from or write to a memory location outside of the intended boundary of the buffer. This hits initially as a read access violation, leading to a memory corruption situation.	7.8	More Details
CVE-2022-2949	Altair HyperView Player versions 2021.1.0.27 and prior are vulnerable to the use of uninitialized memory vulnerability during parsing of H3D files. A DWORD is extracted from an uninitialized buffer and, after sign extension, is used as an index into a stack variable to increment a counter leading to memory corruption.	7.8	More Details
CVE-2022-44649	An out-of-bounds access vulnerability in the Unauthorized Change Prevention service of Trend Micro Apex One and Apex One as a Service could allow a local attacker to elevate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2022-44650	A memory corruption vulnerability in the Unauthorized Change Prevention service of Trend Micro Apex One and Apex One as a Service could allow a local attacker to elevate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2022-43667	Stack-based buffer overflow vulnerability exists in CX-Programmer v.9.77 and earlier, which may lead to information disclosure and/or arbitrary code execution by having a user to open a specially crafted CXP file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44652	An improper handling of exceptional conditions vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2022-43509	Out-of-bounds write vulnerability exists in CX-Programmer v.9.77 and earlier, which may lead to information disclosure and/or arbitrary code execution by having a user to open a specially crafted CXP file.	7.8	More Details
CVE-2022-43508	Use-after free vulnerability exists in CX-Programmer v.9.77 and earlier, which may lead to information disclosure and/or arbitrary code execution by having a user to open a specially crafted CXP file.	7.8	More Details
CVE-2022-44653	A security agent directory traversal vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2022-2950	Altair HyperView Player versions 2021.1.0.27 and prior are vulnerable to the use of uninitialized memory vulnerability during parsing of H3D files. A DWORD is extracted from an uninitialized buffer and, after sign extension, is used as an index into a stack variable to increment a counter leading to memory corruption.	7.8	More Details
CVE-2022-2951	Altair HyperView Player versions 2021.1.0.27 and prior are vulnerable to improper validation of array index vulnerability during processing of H3D files. A DWORD value from a PoC file is extracted and used as an index to write to a buffer, leading to memory corruption.	7.8	More Details
CVE-2022-20470	In bindRemoteViewsService of AppWidgetServiceImpl.java, there is a possible way to bypass background activity launch due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-234013191	7.8	More Details
CVE-2022-44702	Windows Terminal Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20491	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242703556	7.8	More Details
CVE-2022-44689	Windows Subsystem for Linux (WSL2) Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-44680	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-20479	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764340	7.8	More Details
CVE-2022-20477	In shouldHideNotification of KeyguardNotificationVisibilityProvider.kt, there is a possible way to show hidden notifications due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-241611867	7.8	More Details
CVE-2022-41282	A vulnerability has been identified in JT2Go (All versions < V14.1.0.6), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.8), Teamcenter Visualization V14.0 (All versions < V14.0.0.4), Teamcenter Visualization V14.1 (All versions < V14.1.0.6). The CGM_NIST_Loader.dll contains an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2022-44691	Microsoft Office OneNote Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-44678	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44697	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-44692	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-44694	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-41281	A vulnerability has been identified in JT2Go (All versions < V14.1.0.6), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.8), Teamcenter Visualization V14.0 (All versions < V14.0.0.4), Teamcenter Visualization V14.1 (All versions < V14.1.0.6). The CGM_NIST_Loader.dll contains an out of bounds read vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2022-44695	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-20478	In NotificationChannel of NotificationChannel.java, there is a possible failure to persist permissions settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-241764135	7.8	More Details
CVE-2022-44687	Raw Image Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-44683	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41283	A vulnerability has been identified in JT2Go (All versions < V14.1.0.6), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.8), Teamcenter Visualization V14.0 (All versions < V14.0.0.4), Teamcenter Visualization V14.1 (All versions < V14.1.0.6). The CGM_NIST_Loader.dll contains an out of bounds write vulnerability when parsing a CGM file. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2022-44696	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-3605	The WP CSV Exporter WordPress plugin before 1.3.7 does not properly escape the fields when exporting data as CSV, leading to a CSV injection vulnerability.	7.8	More Details
CVE-2022-4291	The aswjsflt.dll library from Avast Antivirus windows contained a potentially exploitable heap corruption vulnerability that could enable an attacker to bypass the sandbox of the application it was loaded into, if applicable. This issue was fixed in version 18.0.1478 of the Script Shield Component.	7.7	More Details
CVE-2022-25685	Denial of service in Modem module due to improper authorization while error handling in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	7.5	More Details
CVE-2022-25689	Denial of service in Modem due to reachable assertion in Snapdragon Mobile	7.5	More Details
CVE-2022-25691	Denial of service in Modem due to reachable assertion while processing SIB1 with invalid SCS and bandwidth settings in Snapdragon Mobile	7.5	More Details
CVE-2022-2794	Certain HP PageWide Pro Printers may be vulnerable to a potential denial of service attack.	7.5	More Details
CVE-2022-44654	Affected builds of Trend Micro Apex One and Apex One as a Service contain a monitor engine component that is complied without the /SAFESEH memory protection mechanism which helps to monitor for malicious payloads. The affected component's memory protection mechanism has been updated to enhance product security.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44790	Interspire Email Marketer through 6.5.1 allows SQL Injection via the surveys module. An unauthenticated attacker could successfully perform an attack to extract potentially sensitive information from the database if the survey id exists.	7.5	More Details
CVE-2022-25702	Denial of service in modem due to reachable assertion while processing reconfiguration message in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	7.5	More Details
CVE-2022-45957	ZTE ZXHN-H108NS router with firmware version H108NSV1.0.7u_ZRD_GR2_A68 is vulnerable to remote stack buffer overflow.	7.5	More Details
CVE-2022-43723	A vulnerability has been identified in SICAM PAS/PQS (All versions < V7.0), SICAM PAS/PQS (All versions >= 7.0 < V8.06). Affected software does not properly validate the input for a certain parameter in the s7ontcp.dll. This could allow an unauthenticated remote attacker to send messages and create a denial of service condition as the application crashes. At the time of assigning the CVE, the affected firmware version of the component has already been superseded by succeeding mainline versions.	7.5	More Details
CVE-2022-4409	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository thorsten/phpmyfaq prior to 3.1.9.	7.5	More Details
CVE-2022-43780	Certain HP ENVY, OfficeJet, and DeskJet printers may be vulnerable to a Denial of Service attack.	7.5	More Details
CVE-2022-33238	Transient DOS due to loop with unreachable exit condition in WLAN while processing an incoming FTM frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2022-3510	A parsing issue similar to CVE-2022-3171, but with Message-Type Extensions in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3509	A parsing issue similar to CVE-2022-3171, but with textformat in protobuf-java core and lite versions prior to 3.21.7, 3.20.3, 3.19.6 and 3.16.3 can lead to a denial of service attack. Inputs containing multiple instances of non-repeated embedded messages with repeated or unknown fields causes objects to be converted back-n-forth between mutable and immutable forms, resulting in potentially long garbage collection pauses. We recommend updating to the versions mentioned above.	7.5	More Details
CVE-2022-25692	Denial of service in Modem due to reachable assertion while processing the common config procedure in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	7.5	More Details
CVE-2022-46352	A vulnerability has been identified in SCALANCE X204RNA (HSR) (All versions < V3.2.7), SCALANCE X204RNA (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (HSR) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP/HSR) (All versions < V3.2.7). Specially crafted PROFINET DCP packets could cause a denial of service condition of affected products.	7.5	More Details
CVE-2022-25672	Denial of service in MODEM due to reachable assertion while processing SIB1 with invalid Bandwidth in Snapdragon Mobile	7.5	More Details
CVE-2022-3912	The User Registration WordPress plugin before 2.2.4.1 does not properly restrict the files to be uploaded via an AJAX action available to both unauthenticated and authenticated users, which could allow unauthenticated users to upload PHP files for example.	7.5	More Details
CVE-2022-25837	Bluetooth® Pairing in Bluetooth Core Specification v1.0B through v5.3 may permit an unauthenticated MITM to acquire credentials with two pairing devices via adjacent access when at least one device supports BR/EDR Secure Connections pairing and the other BR/EDR Legacy PIN code pairing if the MITM negotiates BR/EDR Secure Simple Pairing in Secure Connections mode using the Passkey association model with the pairing Initiator and BR/EDR Legacy PIN code pairing with the pairing Responder and brute forces the Passkey entered by the user into the Responder as a 6-digit PIN code. The MITM attacker can use the identified PIN code value as the Passkey value to complete authentication with the Initiator via Bluetooth pairing method confusion.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25836	Bluetooth® Low Energy Pairing in Bluetooth Core Specification v4.0 through v5.3 may permit an unauthenticated MITM to acquire credentials with two pairing devices via adjacent access when the MITM negotiates Legacy Passkey Pairing with the pairing Initiator and Secure Connections Passkey Pairing with the pairing Responder and brute forces the Passkey entered by the user into the Initiator. The MITM attacker can use the identified Passkey value to complete authentication with the Responder via Bluetooth pairing method confusion.	7.5	More Details
CVE-2022-3996	If an X.509 certificate contains a malformed policy constraint and policy processing is enabled, then a write lock will be taken twice recursively. On some operating systems (most widely: Windows) this results in a denial of service when the affected process hangs. Policy processing being enabled on a publicly facing server is not considered to be a common setup. Policy processing is enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. Update (31 March 2023): The description of the policy processing enablement was corrected based on CVE-2023-0466.	7.5	More Details
CVE-2022-37919	A vulnerability exists in the API of Aruba EdgeConnect Enterprise. An unauthenticated attacker can exploit this condition via the web-based management interface to create a denial-of-service condition which prevents the appliance from properly responding to API requests in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below;	7.5	More Details
CVE-2022-45227	The web portal of Dragino Lora LG01 18ed40 IoT v4.3.4 has the directory listing at the URL https://10.10.20.74/lib/. This address has a backup file which can be downloaded without any authentication.	7.5	More Details
CVE-2022-25673	Denial of service in MODEM due to reachable assertion while processing configuration from network in Snapdragon Mobile	7.5	More Details
CVE-2022-46355	A vulnerability has been identified in SCALANCE X204RNA (HSR) (All versions < V3.2.7), SCALANCE X204RNA (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (HSR) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP/HSR) (All versions < V3.2.7). The affected products are vulnerable to an "Exposure of Sensitive Information to an Unauthorized Actor" vulnerability by leaking sensitive data in the HTTP Referer.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23495	go-merkledag implements the 'DAGService' interface and adds two ipld node types, Protobuf and Raw for the ipfs project. A `ProtoNode` may be modified in such a way as to cause various encode errors which will trigger a panic on common method calls that don't allow for error returns. A `ProtoNode` should only be able to encode to valid DAG-PB, attempting to encode invalid DAG-PB forms will result in an error from the codec. Manipulation of an existing (newly created or decoded) `ProtoNode` using the modifier methods did not account for certain states that would place the `ProtoNode` into an unencodeable form. Due to conformance with the [`github.com/ipfs/go-block-format#Block`] (https://pkg.go.dev/github.com/ipfs/go-block-format#Block) and [`github.com/ipfs/go-ipld-format#Node`] (https://pkg.go.dev/github.com/ipfs/go-ipld-format#Node) interfaces, certain methods, which internally require a re-encode if state has changed, will panic due to the inability to return an error. This issue has been addressed across a number of pull requests. Users are advised to upgrade to version 0.8.1 for a complete set of fixes. Users unable to upgrade may attempt to mitigate this issue by sanitising inputs when allowing user-input to set a new `CidBuilder` on a `ProtoNode` and by sanitising `Tsize` (`Link#Size`) values such that they are a reasonable byte-size for sub-DAGs where derived from user-input.	7.5	More Details
CVE-2022-45520	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/qossetting.	7.5	More Details
CVE-2022-45498	An issue in the component tpi_systool_handle(0) (/goform/SysToolReboot) of Tenda W6-S v1.0.0.4(510) allows unauthenticated attackers to arbitrarily reboot the device.	7.5	More Details
CVE-2022-45518	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/SetIpBind.	7.5	More Details
CVE-2022-45517	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/VirtualSer.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23486	libp2p-rust is the official rust language Implementation of the libp2p networking stack. In versions prior to 0.45.1 an attacker node can cause a victim node to allocate a large number of small memory chunks, which can ultimately lead to the victim's process running out of memory and thus getting killed by its operating system. When executed continuously, this can lead to a denial of service attack, especially relevant on a larger scale when run against more than one node of a libp2p based network. Users are advised to upgrade to `libp2p` `v0.45.1` or above. Users unable to upgrade should reference the DoS Mitigation page for more information on how to incorporate mitigation strategies, monitor their application, and respond to attacks: https://docs.libp2p.io/reference/dos-mitigation/.	7.5	More Details
CVE-2022-23487	js-libp2p is the official javascript Implementation of libp2p networking stack. Versions older than `v0.38.0` of js-libp2p are vulnerable to targeted resource exhaustion attacks. These attacks target libp2p's connection, stream, peer, and memory management. An attacker can cause the allocation of large amounts of memory, ultimately leading to the process getting killed by the host's operating system. While a connection manager tasked with keeping the number of connections within manageable limits has been part of js-libp2p, this component was designed to handle the regular churn of peers, not a targeted resource exhaustion attack. Users are advised to update their js-libp2p dependency to `v0.38.0` or greater. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2022-45516	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/NatStaticSetting.	7.5	More Details
CVE-2022-45515	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the entries parameter at /goform/addressNat.	7.5	More Details
CVE-2022-45514	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/webExcptypemanFilter.	7.5	More Details
CVE-2022-45513	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/P2pListFilter.	7.5	More Details
CVE-2022-44713	Microsoft Outlook for Mac Spoofing Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23492	go-libp2p is the offical libp2p implementation in the Go programming language. Version `0.18.0` and older of go-libp2p are vulnerable to targeted resource exhaustion attacks. These attacks target libp2p's connection, stream, peer, and memory management. An attacker can cause the allocation of large amounts of memory, ultimately leading to the process getting killed by the host's operating system. While a connection manager tasked with keeping the number of connections within manageable limits has been part of go-libp2p, this component was designed to handle the regular churn of peers, not a targeted resource exhaustion attack. Users are advised to upgrade their version of go-libp2p to version `0.18.1` or newer. Users unable to upgrade may consult the denial of service (dos) mitigation page for more information on how to incorporate mitigation strategies, monitor your application, and respond to attacks.	7.5	More Details
CVE-2022-45512	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/SafeEmailFilter.	7.5	More Details
CVE-2022-45511	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the PPPOEPassword parameter at /goform/QuickIndex.	7.5	More Details
CVE-2022-45510	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the mit_ssid_index parameter at /goform/AdvSetWrlsafeset.	7.5	More Details
CVE-2022-45509	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the account parameter at /goform/addUserName.	7.5	More Details
CVE-2022-23476	Nokogiri is an open source XML and HTML library for the Ruby programming language. Nokogiri `1.13.8` and `1.13.9` fail to check the return value from `xmlTextReaderExpand` in the method `Nokogiri::XML::Reader#attribute_hash`. This can lead to a null pointer exception when invalid markup is being parsed. For applications using `XML::Reader` to parse untrusted inputs, this may potentially be a vector for a denial of service attack. Users are advised to upgrade to Nokogiri `>= 1.13.10`. Users may be able to search their code for calls to either `XML::Reader#attributes` or `XML::Reader#attribute_hash` to determine if they are affected.	7.5	More Details
CVE-2022-44931	Tenda A18 v15.13.07.09 was discovered to contain a stack overflow via the security_5g parameter at /goform/WifiBasicSet.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44932	An access control issue in Tenda A18 v15.13.07.09 allows unauthenticated attackers to access the Telnet service.	7.5	More Details
CVE-2022-45508	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the new_account parameter at /goform/editUserName.	7.5	More Details
CVE-2022-45507	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the editNameMit parameter at /goform/editFileName.	7.5	More Details
CVE-2022-45505	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the cmdinput parameter at /goform/exeCommand.	7.5	More Details
CVE-2022-45504	An issue in the component tpi_systool_handle(0) (/goform/SysToolRestoreSet) of Tenda W6-S v1.0.0.4(510) allows unauthenticated attackers to arbitrarily reboot the device.	7.5	More Details
CVE-2022-45503	Tenda W6-S v1.0.0.4(510) was discovered to contain a stack overflow via the linkEn parameter at /goform/setAutoPing.	7.5	More Details
CVE-2022-45501	Tenda W6-S v1.0.0.4(510) was discovered to contain a stack overflow via the wl_radio parameter at /goform/wifiSSIDset.	7.5	More Details
CVE-2022-45519	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the Go parameter at /goform/SafeMacFilter.	7.5	More Details
CVE-2022-45499	Tenda W6-S v1.0.0.4(510) was discovered to contain a stack overflow via the wl_radio parameter at /goform/WifiMacFilterGet.	7.5	More Details
CVE-2022-45521	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/SafeUrlFilter.	7.5	More Details
CVE-2022-46770	qubes-mirage-firewall (aka Mirage firewall for QubesOS) 0.8.x through 0.8.3 allows guest OS users to cause a denial of service (CPU consumption and loss of forwarding) via a crafted multicast UDP packet (IP address range of 224.0.0.0 through 239.255.255.255).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23483	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a Out of Bound Read in libxrdp_send_to_channel() function. There are no known workarounds for this issue. Users are advised to upgrade.	7.5	More Details
CVE-2021-40365	Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial of service in the device.	7.5	More Details
CVE-2022-38355	Daikin SVMPC1 version 2.1.22 and prior and SVMPC2 version 1.2.3 and prior are vulnerable to attackers with access to the local area network (LAN) to disclose sensitive information stored by the affected product without requiring authentication.	7.5	More Details
CVE-2022-46363	A vulnerability in Apache CXF before versions 3.5.5 and 3.4.10 allows an attacker to perform a remote directory listing or code exfiltration. The vulnerability only applies when the CXFServlet is configured with both the static-resources-list and redirect-query-check attributes. These attributes are not supposed to be used together, and so the vulnerability can only arise if the CXF service is misconfigured.	7.5	More Details
CVE-2022-20483	In several functions that parse avrc response in avrc_pars_ct.cc and related files, there are possible out of bounds reads due to integer overflows. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-242459126	7.5	More Details
CVE-2022-45269	A directory traversal vulnerability in the component SCS.Web.Server.SPI/1.0 of Linx Sphere LINX 7.35.ST15 allows attackers to read arbitrary files.	7.5	More Details
CVE-2022-43468	External initialization of trusted variables or data stores vulnerability exists in WordPress Popular Posts 6.0.5 and earlier, therefore the vulnerable product accepts untrusted external inputs to update certain internal variables. As a result, the number of views for an article may be manipulated through a crafted input.	7.5	More Details
CVE-2022-45693	Jettison before v1.5.2 was discovered to contain a stack overflow via the map parameter. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23496	Yet Another UserAgent Analyzer (Yauaa) is a java library that tries to parse and analyze the useragent string and extract as many relevant attributes as possible. Applications using the Client Hints analysis feature introduced with 7.0.0 can crash because the Yauaa library throws an ArrayIndexOutOfBoundsException. If uncaught the exception will result in a program crash. Applications that do not use this feature are not affected. Users are advised to upgrade to version 7.9.0. Users unable to upgrade may catch and discard any ArrayIndexOutOfBoundsException thrown by the Yauaa library.	7.5	More Details
CVE-2022-45979	Tenda AX12 v22.03.01.21_CN was discovered to contain a stack overflow via the ssid parameter at /goform/fast_setting_wifi_set .	7.5	More Details
CVE-2022-4366	Missing Authorization in GitHub repository lirantal/daloradius prior to master branch.	7.5	More Details
CVE-2022-44608	Uncontrolled resource consumption vulnerability in Cybozu Remote Service 4.0.0 to 4.0.3 allows a remote authenticated attacker to consume huge storage space, which may result in a denial-of-service (DoS) condition.	7.5	More Details
CVE-2022-45690	A stack overflow in the org.json.JSONTokener.nextValue::JSONTokener.java component of hutool-json v5.8.10 allows attackers to cause a Denial of Service (DoS) via crafted JSON or XML data.	7.5	More Details
CVE-2022-45689	hutool-json v5.8.10 was discovered to contain an out of memory error.	7.5	More Details
CVE-2022-45688	A stack overflow in the XML.toJSONObject component of hutool-json v5.8.10 allows attackers to cause a Denial of Service (DoS) via crafted JSON or XML data.	7.5	More Details
CVE-2022-45685	A stack overflow in Jettison before v1.5.2 allows attackers to cause a Denial of Service (DoS) via crafted JSON data.	7.5	More Details
CVE-2022-45525	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the downaction parameter at /goform/CertListInfo.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41720	On Windows, restricted files can be accessed via os.DirFS and http.Dir. The os.DirFS function and http.Dir type provide access to a tree of files rooted at a given directory. These functions permit access to Windows device files under that root. For example, os.DirFS("C:/tmp").Open("COM1") opens the COM1 device. Both os.DirFS and http.Dir only provide read-only filesystem access. In addition, on Windows, an os.DirFS for the directory (the root of the current drive) can permit a maliciously crafted path to escape from the drive and access any path on the system. With fix applied, the behavior of os.DirFS("") has changed. Previously, an empty root was treated equivalently to "/", so os.DirFS("").Open("tmp") would open the path "/tmp". This now returns an error.	7.5	More Details
CVE-2022-45524	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the opttype parameter at /goform/IPSECsave.	7.5	More Details
CVE-2022-43581	IBM Content Navigator 3.0.0, 3.0.1, 3.0.2, 3.0.3, 3.0.4, 3.0.5, 3.0.6, 3.0.7, 3.0.8, 3.0.9, 3.0.10, 3.0.11, and 3.0.12 is vulnerable to missing authorization and could allow an authenticated user to load external plugins and execute code. IBM X-Force ID: 238805.	7.5	More Details
CVE-2022-45523	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/L7Im.	7.5	More Details
CVE-2022-45522	Tenda W30E V1.0.1.25(633) was discovered to contain a stack overflow via the page parameter at /goform/SafeClientFilter.	7.5	More Details
CVE-2022-3259	Openshift 4.9 does not use HTTP Strict Transport Security (HSTS) which may allow man-in-the-middle (MITM) attacks.	7.4	More Details
CVE-2022-4364	A vulnerability classified as critical has been found in Teledyne FLIR AX8 up to 1.46.16. Affected is an unknown function of the file palette.php of the component Web Service Handler. The manipulation of the argument palette leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-215118 is the identifier assigned to this vulnerability.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20442	In onCreate of ReviewPermissionsActivity.java, there is a possible way to grant permissions for a separate app with API level < 23 due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-176094367	7.3	More Details
CVE-2022-46908	SQLite through 3.40.0, when relying on --safe for execution of an untrusted CLI script, does not properly implement the azProhibitedFunctions protection mechanism, and instead allows UDF functions such as WRITEFILE.	7.3	More Details
CVE-2022-20501	In onCreate of EnableAccountPreferenceActivity.java, there is a possible way to mislead the user into enabling a malicious phone account due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-246933359	7.3	More Details
CVE-2022-37912	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities results in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2022-37920	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below.	7.2	More Details
CVE-2022-43541	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43542	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below.	7.2	More Details
CVE-2022-3925	The buddybadges WordPress plugin through 1.0.0 does not sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users	7.2	More Details
CVE-2022-44533	A vulnerability in the Aruba EdgeConnect Enterprise web management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below.	7.2	More Details
CVE-2022-45996	Tenda W20E V16.01.0.6(3392) is vulnerable to Command injection via cmd_get_ping_output.	7.2	More Details
CVE-2022-46051	The approve parameter from the AeroCMS-v0.0.1 CMS system is vulnerable to SQL injection attacks.	7.2	More Details
CVE-2022-45997	Tenda W20E V16.01.0.6(3392) is vulnerable to Buffer Overflow.	7.2	More Details
CVE-2022-37924	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37923	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below.	7.2	More Details
CVE-2022-37922	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below.	7.2	More Details
CVE-2022-37921	Vulnerabilities in the Aruba EdgeConnect Enterprise command line interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below.	7.2	More Details
CVE-2022-44393	Sanitization Management System v1.0 is vulnerable to SQL Injection via /php-sms/admin/?page=services/view_service&id=.	7.2	More Details
CVE-2022-37901	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities results in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2022-37900	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities results in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2022-44838	Automotive Shop Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /services/view_service.php.	7.2	More Details
CVE-2022-45275	An arbitrary file upload vulnerability in /queuing/admin/ajax.php?action=save_settings of Dynamic Transaction Queuing System v1.0 allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37898	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities results in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2022-37899	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities results in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2022-43660	Improper neutralization of Server-Side Includes (SSW) within a web page in Movable Type series allows a remote authenticated attacker with Privilege of 'Manage of Content Types' may execute an arbitrary Perl script and/or an arbitrary OS command. Affected products/versions are as follows: Movable Type 7 r.5301 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.5301 and earlier (Movable Type Advanced 7 Series), Movable Type Premium 1.53 and earlier, and Movable Type Premium Advanced 1.53 and earlier.	7.2	More Details
CVE-2022-45009	Online Leave Management System v1.0 was discovered to contain an arbitrary file upload vulnerability at /leave_system/classes/SystemSettings.php?f=update_settings. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	7.2	More Details
CVE-2022-37903	A vulnerability exists that allows an authenticated attacker to overwrite an arbitrary file with attacker-controlled content via the web interface. Successful exploitation of this vulnerability could lead to full compromise the underlying host operating system.	7.2	More Details
CVE-2022-37902	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities results in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2022-46741	Out-of-bounds read in gather_tree in PaddlePaddle before 2.4.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23511	A privilege escalation issue exists within the Amazon CloudWatch Agent for Windows, software for collecting metrics and logs from Amazon EC2 instances and on-premises servers, in versions up to and including v1.247354. When users trigger a repair of the Agent, a pop-up window opens with SYSTEM permissions. Users with administrative access to affected hosts may use this to create a new command prompt as NT AUTHORITY\SYSTEM. To trigger this issue, the third party must be able to access the affected host and elevate their privileges such that they're able to trigger the agent repair process. They must also be able to install the tools required to trigger the issue. This issue does not affect the CloudWatch Agent for macOS or Linux. Agent users should upgrade to version 1.247355 of the CloudWatch Agent to address this issue. There is no recommended work around. Affected users must update the installed version of the CloudWatch Agent to address this issue.	7.1	More Details
CVE-2022-39909	Insufficient verification of data authenticity vulnerability in Samsung Gear IconX PC Manager prior to version 2.1.221019.51 allows local attackers to create arbitrary file using symbolic link.	7.1	More Details
CVE-2022-46829	In JetBrains JetBrains Gateway before 2022.3 a client could connect without a valid token if the host consented.	7.1	More Details
CVE-2022-45797	An arbitrary file deletion vulnerability in the Damage Cleanup Engine component of Trend Micro Apex One and Trend Micro Apex One as a Service could allow a local attacker to escalate privileges and delete files on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.1	More Details
CVE-2022-44651	A Time-of-Check Time-Of-Use vulnerability in the Trend Micro Apex One and Apex One as a Service agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.0	More Details
CVE-2022-44669	Windows Error Reporting Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-44673	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39660	In TBD of TBD, there is a possible way to archive arbitrary code execution in kernel due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-254742984	7.0	More Details
CVE-2022-39908	TOCTOU vulnerability in Samsung decoding library for video thumbnails prior to SMR Dec-2022 Release 1 allows local attacker to perform Out-Of-Bounds Write.	6.9	More Details
CVE-2022-39907	Integer overflow vulnerability in Samsung decoding library for video thumbnails prior to SMR Dec-2022 Release 1 allows local attacker to perform Out-Of-Bounds Write.	6.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39044	Hidden functionality vulnerability in multiple Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command. The affected products/versions are as follows: WCR-300 firmware Ver. 1.87 and earlier, WHR-HP-G300N firmware Ver. 2.00 and earlier, WHR-HP-GN firmware Ver. 1.87 and earlier, WPL-05G300 firmware Ver. 1.88 and earlier, WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, WZR-HP-AG300H firmware Ver. 1.76 and earlier, WZR-HP-G302H firmware Ver. 1.86 and earlier, WLAE-AG300N firmware Ver. 1.86 and earlier, FS-600DHP firmware Ver. 3.40 and earlier, FS-G300N firmware Ver. 3.14 and earlier, FS-HP-G300N firmware Ver. 3.33 and earlier, FS-R600DHP firmware Ver. 3.40 and earlier, BHR-4GRV firmware Ver. 2.00 and earlier, DWR-HP-G300NH firmware Ver. 1.84 and earlier, DWR-PG firmware Ver. 1.83 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WER-A54G54 firmware Ver. 1.43 and earlier, WER-AG54 firmware Ver. 1.43 and earlier, WER-AM54G54 firmware Ver. 1.43 and earlier, WER-AMG54 firmware Ver. 1.43 and earlier, WHR-300 firmware Ver. 2.00 and earlier, WHR-300HP firmware Ver. 2.00 and earlier, WHR-AM54G54 firmware Ver. 1.43 and earlier, WHR-AMG54 firmware Ver. 1.43 and earlier, WHR-AMPG firmware Ver. 1.52 and earlier, WHR-G firmware Ver. 1.49 and earlier, WHR-G300N firmware Ver. 1.65 and earlier, WHR-G301N firmware Ver. 1.87 and earlier, WHR-G54S firmware Ver. 1.43 and earlier, WHR-G54S-NI firmware Ver. 1.24 and earlier, WHR-HP-AMPG firmware Ver. 1.43 and earlier, WHR-HP-G firmware Ver. 1.49 and earlier, WHR-HP-G54 firmware Ver. 1.43 and earlier, WLI-H4-D600 firmware Ver. 1.88 and earlier, WLI-TX4-AG300N firmware Ver. 1.53 and earlier, WS024BF firmware Ver. 1.60 and earlier, WS024BF-NW firmware Ver. 1.60 and earlier, WZR2-G108 firmware Ver. 1.33 and earlier, WZR2-G300N firmware Ver. 1.55 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, WZR-AGL300NH firmware Ver. 1.55 and earlier, WZR-AMPG144NH firmware Ver. 1.49 and earlier, WZR-AMPG300NH firmware Ver. 1.51 and earlier, WZR-D1100H firmware Ver. 2.00 and earlier, WZR-G144N firmware Ver. 1.48 and earlier, WZR-G144NH firmware Ver. 1.48 and earlier, WZR-HP-G300NH firmware Ver. 1.84 and earlier, WZR-HP-G301NH firmware Ver. 1.84 and earlier, and WZR-HP-G450H firmware Ver. 1.90 and earlier.	6.8	More Details
CVE-2022-39913	Exposure of Sensitive Information to an Unauthorized Actor in Persona Manager prior to Android T(13) allows local attacker to access user profiles information.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44455	The appspawn and nwebspawn services within OpenHarmony-v3.1.2 and prior versions were found to be vulnerable to buffer overflow vulnerability due to insufficient input validation. An unprivileged malicious application would be able to gain code execution within any application installed on the device or cause application crash.	6.8	More Details
CVE-2022-23491	Certifi is a curated collection of Root Certificates for validating the trustworthiness of SSL certificates while verifying the identity of TLS hosts. Certifi 2022.12.07 removes root certificates from "TrustCor" from the root store. These are in the process of being removed from Mozilla's trust store. TrustCor's root certificates are being removed pursuant to an investigation prompted by media reporting that TrustCor's ownership also operated a business that produced spyware. Conclusions of Mozilla's investigation can be found in the linked google group discussion.	6.8	More Details
CVE-2022-44682	Windows Hyper-V Denial of Service Vulnerability	6.8	More Details
CVE-2022-37930	A security vulnerability has been identified in HPE Nimble Storage Hybrid Flash Arrays and HPE Nimble Storage Secondary Flash Arrays which could potentially allow local disclosure of sensitive information.	6.7	More Details
CVE-2022-25712	Memory corruption in camera due to buffer copy without checking size of input in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wearables	6.7	More Details
CVE-2022-25677	Memory corruption in diag due to use after free while processing dci packet in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	6.7	More Details
CVE-2022-37929	Improper Privilege Management vulnerability in Hewlett Packard Enterprise Nimble Storage Hybrid Flash Arrays and Nimble Storage Secondary Flash Arrays.	6.7	More Details
CVE-2022-25711	Memory corruption in camera due to improper validation of array index in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41948	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. Affected versions are subject to a privilege escalation vulnerability. A DHIS2 user with authority to manage users can assign superuser privileges to themself by manually crafting an HTTP PUT request. Only users with the following DHIS2 user role authorities can exploit this vulnerability. Note that in many systems the only users with user admin privileges are also superusers. In these cases, the escalation vulnerability does not exist. The vulnerability is only exploitable by attackers who can authenticate as users with the user admin authority. As this is usually a small and relatively trusted set of users, exploit vectors will often be limited. DHIS2 administrators should upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. The only known workaround to this issue is to avoid the assignment of the user management authority to any users until the patch has been applied.	6.7	More Details
CVE-2022-46831	In JetBrains TeamCity between 2022.10 and 2022.10.1 connecting to AWS using the "Default Credential Provider Chain" allowed TeamCity project administrators to access AWS resources normally limited to TeamCity system administrators.	6.6	More Details
CVE-2022-41115	Microsoft Edge (Chromium-based) Update Elevation of Privilege Vulnerability	6.6	More Details
CVE-2022-37904	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system.	6.6	More Details
CVE-2022-37905	Vulnerabilities in ArubaOS running on 7xxx series controllers exist that allows an attacker to execute arbitrary code during the boot sequence. Successful exploitation could allow an attacker to achieve permanent modification of the underlying operating system.	6.6	More Details
CVE-2022-3880	The Disable Json API, Login Lockdown, XMLRPC, Pingback, Stop User Enumeration Anti Hacker Scan WordPress plugin before 4.20 does not have proper authorisation and CSRF in an AJAX action, allowing any authenticated users, such as subscriber to call it and install and activate arbitrary plugins from wordpress.org	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4016	The Booster for WooCommerce WordPress plugin before 5.6.7, Booster Plus for WooCommerce WordPress plugin before 5.6.6, Booster Elite for WooCommerce WordPress plugin before 1.1.8 does not properly check for CSRF when creating and deleting Customer roles, allowing attackers to make logged admins create and delete arbitrary custom roles via CSRF attacks	6.5	More Details
CVE-2022-20468	In BNEP_ConnectResp of bnep_api.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-228450451	6.5	More Details
CVE-2022-3946	The Welcart e-Commerce WordPress plugin before 2.8.4 does not have authorisation and CSRF in an AJAX action, allowing any logged-in user to create, update and delete shipping methods.	6.5	More Details
CVE-2022-46059	AeroCMS v0.0.1 is vulnerable to Cross Site Request Forgery (CSRF).	6.5	More Details
CVE-2022-41274	SAP Disclosure Management - version 10.1, allows an authenticated attacker to exploit certain misconfigured application endpoints to read sensitive data. These endpoints are normally exposed over the network and successful exploitation can lead to the exposure of data like financial reports.	6.5	More Details
CVE-2022-3882	The Memory Usage, Memory Limit, PHP and Server Memory Health Check and Fix Plugin WordPress plugin before 2.46 does not have proper authorisation and CSRF in an AJAX action, allowing any authenticated users, such as subscriber to call it and install and activate arbitrary plugins from wordpress.org	6.5	More Details
CVE-2022-3879	The Car Dealer (Dealership) and Vehicle sales WordPress Plugin WordPress plugin before 3.05 does not have proper authorisation and CSRF in an AJAX action, allowing any authenticated users, such as subscriber to call it and install and activate arbitrary plugins from wordpress.org	6.5	More Details
CVE-2022-3883	The Block Bad Bots and Stop Bad Bots Crawlers and Spiders and Anti Spam Protection WordPress plugin before 7.24 does not have proper authorisation and CSRF in an AJAX action, allowing any authenticated users, such as subscriber to call it and install and activate arbitrary plugins from wordpress.org	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3930	The Directorist WordPress plugin before 7.4.2.2 suffers from an IDOR vulnerability which an attacker can exploit to change the password of arbitrary users instead of his own.	6.5	More Details
CVE-2022-41915	Netty project is an event-driven asynchronous network application framework. Starting in version 4.1.83.Final and prior to 4.1.86.Final, when calling `DefaultHttpHeadesr.set` with an _iterator_ of values, header value validation was not performed, allowing malicious header values in the iterator to perform HTTP Response Splitting. This issue has been patched in version 4.1.86.Final. Integrators can work around the issue by changing the `DefaultHttpHeaders.set(CharSequence, Iterator<?>)` call, into a `remove()` call, and call `add()` in a loop over the iterator of values.	6.5	More Details
CVE-2022-3643	Guests can trigger NIC interface reset/abort/crash via netback It is possible for a guest to trigger a NIC interface reset/abort/crash in a Linux based network backend by sending certain kinds of packets. It appears to be an (unwritten?) assumption in the rest of the Linux network stack that packet protocol headers are all contained within the linear section of the SKB and some NICs behave badly if this is not the case. This has been reported to occur with Cisco (enic) and Broadcom NetXtrem II BCM5780 (bnx2x) though it may be an issue with other NICs/drivers as well. In case the frontend is sending requests with split headers, netback will forward those violating above mentioned assumption to the networking core, resulting in said misbehavior.	6.5	More Details
CVE-2022-27581	Use of a Broken or Risky Cryptographic Algorithm in SICK RFU61x firmware version <v2.25 allows a low-privileged remote attacker to decrypt the encrypted data if the user requested weak cipher suites to be used for encryption via the SSH interface. The patch and installation procedure for the firmware update is available from the responsible SICK customer contact person.	6.5	More Details
CVE-2022-44679	Windows Graphics Component Information Disclosure Vulnerability	6.5	More Details
CVE-2022-46832	Use of a Broken or Risky Cryptographic Algorithm in SICK RFU62x firmware version < 2.21 allows a low-privileged remote attacker to decrypt the encrypted data if the user requested weak cipher suites to be used for encryption via the SSH interface. The patch and installation procedure for the firmware update is available from the responsible SICK customer contact person.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46833	Use of a Broken or Risky Cryptographic Algorithm in SICK RFU63x firmware version < v2.21 allows a low-privileged remote attacker to decrypt the encrypted data if the user requested weak cipher suites to be used for encryption via the SSH interface. The patch and installation procedure for the firmware update is available from the responsible SICK customer contact person.	6.5	More Details
CVE-2022-46834	Use of a Broken or Risky Cryptographic Algorithm in SICK RFU65x firmware version < v2.21 allows a low-privileged remote attacker to decrypt the encrypted data if the user requested weak cipher suites to be used for encryption via the SSH interface. The patch and installation procedure for the firmware update is available from the responsible SICK customer contact person.	6.5	More Details
CVE-2022-4264	Incorrect Privilege Assignment in M-Files Web (Classic) in M-Files before 22.8.11691.0 allows low privilege user to change some configuration.	6.5	More Details
CVE-2022-38765	Canon Medical Informatics Vitrea Vision 7.7.76.1 does not adequately enforce access controls. An authenticated user is able to gain unauthorized access to imaging records by tampering with the vitrea-view/studies/search patientId parameter.	6.5	More Details
CVE-2022-38599	Teleport v3.2.2, Teleport v3.5.6-rc6, and Teleport v3.6.3-b2 was discovered to contain an information leak via the /user/get-role-list web interface.	6.5	More Details
CVE-2022-39902	Improper authorization in Exynos baseband prior to SMR DEC-2022 Release 1 allows remote attacker to get sensitive information including IMEI via emergency call.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46144	A vulnerability has been identified in SCALANCE SC622-2C (6GK5622-2GS00-2AC2) (All versions < V2.3), SCALANCE SC622-2C (6GK5622-2GS00-2AC2) (All versions >= V2.3 < V3.0), SCALANCE SC626-2C (6GK5626-2GS00-2AC2) (All versions < V2.3), SCALANCE SC626-2C (6GK5626-2GS00-2AC2) (All versions >= V2.3 < V3.0), SCALANCE SC632-2C (6GK5632-2GS00-2AC2) (All versions < V2.3), SCALANCE SC632-2C (6GK5632-2GS00-2AC2) (All versions >= V2.3 < V3.0), SCALANCE SC636-2C (6GK5636-2GS00-2AC2) (All versions < V2.3), SCALANCE SC636-2C (6GK5636-2GS00-2AC2) (All versions >= V2.3 < V3.0), SCALANCE SC642-2C (6GK5642-2GS00-2AC2) (All versions < V2.3), SCALANCE SC642-2C (6GK5642-2GS00-2AC2) (All versions >= V2.3 < V3.0), SCALANCE SC646-2C (6GK5646-2GS00-2AC2) (All versions < V2.3), SCALANCE SC646-2C (6GK5646-2GS00-2AC2) (All versions >= V2.3 < V3.0), SCALANCE WAB762-1 (6GK5762-1AJ00-6AA0) (All versions), SCALANCE WAM763-1 (6GK5763-1AL00-7DA0) (All versions), SCALANCE WAM763-1 (ME) (6GK5763-1AL00-7DC0) (All versions), SCALANCE WAM763-1 (US) (6GK5763-1AL00-7DB0) (All versions), SCALANCE WAM766-1 (EU) (6GK5766-1GE00-7DA0) (All versions), SCALANCE WAM766-1 (ME) (6GK5766-1GE00-7DC0) (All versions), SCALANCE WAM766-1 (US) (6GK5766-1GE00-7DB0) (All versions), SCALANCE WAM766-1 EEC (EU) (6GK5766-1GE00-7TA0) (All versions), SCALANCE WAM766-1 EEC (ME) (6GK5766-1GE00-7TC0) (All versions), SCALANCE WAM766-1 EEC (US) (6GK5766-1GE00-7TB0) (All versions), SCALANCE WUB762-1 (6GK5762-1AJ00-1AA0) (All versions), SCALANCE WUB762-1 (6GK5762-1AJ00-2AA0) (All versions), SCALANCE WUM763-1 (6GK5763-1AL00-3AA0) (All versions), SCALANCE WUM763-1 (6GK5763-1AL00-3DA0) (All versions), SCALANCE WUM763-1 (US) (6GK5763-1AL00-3AB0) (All versions), SCALANCE WUM763-1 (US) (6GK5763-1AL00-3DB0) (All versions), SCALANCE WUM766-1 (EU) (6GK5766-1GE00-3DA0) (All versions), SCALANCE WUM766-1 (ME) (6GK5766-1GE00-3DC0) (All versions), SCALANCE WUM766-1 (US) (6GK5766-1GE00-3DB0) (All versions). Affected devices do not properly process CLI commands after a user forcefully quitted the SSH connection. This could allow an authenticated attacker to make the CLI via SSH or serial interface irresponsive.	6.5	More Details
CVE-2022-39901	Improper authentication in Exynos baseband prior to SMR DEC-2022 Release 1 allows remote attacker to disable the network traffic encryption between UE and gNodeB.	6.5	More Details
CVE-2022-44707	Windows Kernel Denial of Service Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34840	Use of hard-coded credentials vulnerability in multiple Buffalo network devices allows a network-adjacent attacker to alter?configuration settings of the device. The affected products/versions are as follows: WZR-300HP firmware Ver. 2.00 and earlier, WZR-450HP firmware Ver. 2.00 and earlier, WZR-600DHP firmware Ver. 2.00 and earlier, WZR-900DHP firmware Ver. 1.15 and earlier, HW-450HP-ZWE firmware Ver. 2.00 and earlier, WZR-450HP-CWT firmware Ver. 2.00 and earlier, WZR-450HP-UB firmware Ver. 2.00 and earlier, WZR-600DHP2 firmware Ver. 1.15 and earlier, and WZR-D1100H firmware Ver. 2.00 and earlier.	6.5	More Details
CVE-2022-45113	Improper validation of syntactic correctness of input vulnerability exist in Movable Type series. Having a user to access a specially crafted URL may allow a remote unauthenticated attacker to set a specially crafted URL to the Reset Password page and conduct a phishing attack. Affected products/versions are as follows: Movable Type 7 r.5301 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.5301 and earlier (Movable Type Advanced 7 Series), Movable Type 6.8.7 and earlier (Movable Type 6 Series), Movable Type Advanced 6.8.7 and earlier (Movable Type Advanced 6 Series), Movable Type Premium 1.53 and earlier, and Movable Type Premium Advanced 1.53 and earlier.	6.5	More Details
CVE-2022-4171	The demon image annotation plugin for WordPress is vulnerable to improper input validation in versions up to, and including 5.0. This is due to the plugin improperly validating the number of characters supplied during an annotation despite there being a setting to limit the number characters input. This means that unauthenticated attackers can bypass the length restrictions and input more characters than allowed via the settings.	6.5	More Details
CVE-2022-45918	ILIAS before 7.16 allows External Control of File Name or Path.	6.5	More Details
CVE-2022-23497	FreshRSS is a free, self-hostable RSS aggregator. User configuration files can be accessed by a remote user. In addition to user preferences, such configurations contain hashed passwords (brypt with cost 9, salted) of FreshRSS Web interface. If the API is used, the configuration might contain a hashed password (brypt with cost 9, salted) of the GReader API, and a hashed password (MD5 salted) of the Fever API. Users should update to version 1.20.2 or edge. Users unable to upgrade can apply the patch manually or delete the file `./FreshRSS/p/ext.php`.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23468	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a buffer over flow in xrdp_login_wnd_create() function. There are no known workarounds for this issue. Users are advised to upgrade.	6.5	More Details
CVE-2022-41296	IBM Db2U 3.5, 4.0, and 4.5 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 237210.	6.5	More Details
CVE-2022-46140	Affected devices use a weak encryption scheme to encrypt the debug zip file. This could allow an authenticated attacker to decrypt the contents of the file and retrieve debug information about the system.	6.5	More Details
CVE-2022-42446	Starting with Sametime 12, anonymous users are enabled by default. After logging in as an anonymous user, one has the ability to browse the User Directory and potentially create chats with internal users.	6.5	More Details
CVE-2022-46688	A cross-site request forgery (CSRF) vulnerability in Jenkins Sonar Gerrit Plugin 377.v8f3808963dc5 and earlier allows attackers to have Jenkins connect to Gerrit servers (previously configured by Jenkins administrators) using attacker-specified credentials IDs obtained through another method, potentially capturing credentials stored in Jenkins.	6.5	More Details
CVE-2022-37906	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of the vulnerability results in the ability to delete arbitrary files on the underlying operating system.	6.5	More Details
CVE-2021-46846	Cross Site Scripting vulnerability in Hewlett Packard Enterprise Integrated Lights-Out 5.	6.4	More Details
CVE-2022-23485	Sentry is an error tracking and performance monitoring platform. In versions of the sentry python library prior to 22.11.0 an attacker with a known valid invite link could manipulate a cookie to allow the same invite link to be reused on multiple accounts when joining an organization. As a result an attacker with a valid invite link can create multiple users and join an organization they may not have been originally invited to. This issue was patched in version 22.11.0. Sentry SaaS customers do not need to take action. Self-hosted Sentry installs on systems which can not upgrade can disable the invite functionality until they are ready to deploy the patched version by editing their `sentry.conf.py` file (usually located at `~/.sentry/`).	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24480	Outlook for Android Elevation of Privilege Vulnerability	6.3	More Details
CVE-2022-3724	Crash in the USB HID protocol dissector in Wireshark 3.6.0 to 3.6.8 allows denial of service via packet injection or crafted capture file on Windows	6.3	More Details
CVE-2022-4322	A vulnerability, which was classified as critical, was found in maku-boot up to 2.2.0. This affects the function doExecute of the file AbstractScheduleJob.java of the component Scheduled Task Handler. The manipulation leads to injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 446eb7294332efca2bfd791bc37281cedac0d0ff. It is recommended to apply a patch to fix this issue. The identifier VDB-215013 was assigned to this vulnerability.	6.3	More Details
CVE-2022-4375	A vulnerability was found in Mingsoft MCMS up to 5.2.9. It has been classified as critical. Affected is an unknown function of the file /cms/category/list. The manipulation of the argument sqlWhere leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 5.2.10 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-215196.	6.3	More Details
CVE-2022-4416	A vulnerability was found in RainyGao DocSys. It has been declared as critical. This vulnerability affects the function getReposAllUsers of the file /DocSystem/Repos/getReposAllUsers.do. The manipulation of the argument searchWord/reposId leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-215278 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-4403	A vulnerability classified as critical was found in SourceCodester Canteen Management System. This vulnerability affects unknown code of the file ajax_represent.php. The manipulation of the argument customer_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-215272.	6.3	More Details
CVE-2022-39912	Improper handling of insufficient permissions vulnerability in setSecureFolderPolicy in PersonaManagerService prior to Android T(13) allows local attackers to set some setting value in Secure folder.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45118	OpenHarmony-v3.1.2 and prior versions had a vulnerability that telephony in communication subsystem sends public events with personal data, but the permission is not set. Malicious apps could listen to public events and obtain information such as mobile numbers and SMS data without permissions.	6.2	More Details
CVE-2022-38661	HCL Workload Automation could allow a local user to overwrite key system files which would cause the system to crash.	6.2	More Details
CVE-2022-46826	In JetBrains IntelliJ IDEA before 2022.3 the built-in web server allowed an arbitrary file to be read by exploiting a path traversal vulnerability.	6.2	More Details
CVE-2022-46061	AeroCMS v0.0.1 is vulnerable to ClickJacking.	6.1	More Details
CVE-2022-41275	In SAP Solution Manager (Enterprise Search) - versions 740, and 750, an unauthenticated attacker can generate a link that, if clicked by a logged-in user, can be redirected to a malicious page that could read or modify sensitive information, or expose the user to a phishing attack, with little impact on confidentiality and integrity.	6.1	More Details
CVE-2022-3908	The Helloprint WordPress plugin before 1.4.7 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-23499	HTML sanitizer is written in PHP, aiming to provide XSS-safe markup based on explicitly allowed tags, attributes and values. In versions prior to 1.5.0 or 2.1.1, malicious markup used in a sequence with special HTML CDATA sections cannot be filtered and sanitized due to a parsing issue in the upstream package masterminds/html5. This allows bypassing the cross-site scripting mechanism of typo3/html-sanitizer. The upstream package masterminds/html5 provides HTML raw text elements (`script`, `style`, `noframes`, `noembed` and `iframe`) as DOMText nodes, which were not processed and sanitized further. None of the mentioned elements were defined in the default builder configuration, that's why only custom behaviors, using one of those tag names, were vulnerable to cross-site scripting. This issue has been fixed in versions 1.5.0 and 2.1.1.	6.1	More Details
CVE-2021-41943	Logrhythm Web Console 7.4.9 allows for HTML tag injection through Contextualize Action -> Create a new Contextualize Action -> Inject your HTML tag in the name field.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37925	A vulnerability within the web-based management interface of Aruba EdgeConnect Enterprise could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below.	6.1	More Details
CVE-2022-45122	Cross-site scripting vulnerability in Movable Type Movable Type 7 r.5301 and earlier (Movable Type 7 Series), Movable Type Advanced 7 r.5301 and earlier (Movable Type Advanced 7 Series), Movable Type 6.8.7 and earlier (Movable Type 6 Series), Movable Type Advanced 6.8.7 and earlier (Movable Type Advanced 6 Series), Movable Type Premium 1.53 and earlier, and Movable Type Premium Advanced 1.53 and earlier allows a remote unauthenticated attacker to inject an arbitrary script.	6.1	More Details
CVE-2022-37927	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Hewlett Packard Enterprise HPE OneView Global Dashboard (OVGD).	6.1	More Details
CVE-2022-43668	Typora versions prior to 1.4.4 fails to properly neutralize JavaScript code, which may result in executing JavaScript code contained in the file when opening a file with the affected product.	6.1	More Details
CVE-2022-38628	Nortek Linear eMerge E3-Series 0.32-08f, 0.32-07p, 0.32-07e, 0.32-09c, 0.32-09b, 0.32-09a, and 0.32-08e were discovered to contain a cross-site scripting (XSS) vulnerability which is chained with a local session fixation. This vulnerability allows attackers to escalate privileges via unspecified vectors.	6.1	More Details
CVE-2022-44153	Rapid Software LLC Rapid SCADA 5.8.4 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2022-45917	ILIAS before 7.16 has an Open Redirect.	6.1	More Details
CVE-2022-46381	Certain Linear eMerge E3-Series devices are vulnerable to XSS via the type parameter (e.g., to the badging/badge_template_v0.php component). This affects 0.32-08f, 0.32-07p, 0.32-07e, 0.32-09c, 0.32-09b, 0.32-09a, and 0.32-08e.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44303	Resque Scheduler version 1.27.4 is vulnerable to Cross-site scripting (XSS). A remote attacker could inject javascript code to the "{schedule_job}" or "args" parameter in /resque/delayed/jobs/{schedule_job}?args={args_id} to execute javascript at client side.	6.1	More Details
CVE-2022-4407	Cross-site Scripting (XSS) - Reflected in GitHub repository thorsten/phpmyfaq prior to 3.1.9.	6.1	More Details
CVE-2022-44575	A vulnerability has been identified in PLM Help Server V4.2 (All versions). A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected application that could allow an attacker to execute malicious javascript code by tricking users into accessing a malicious link.	6.1	More Details
CVE-2022-44637	Redmine before 4.2.9 and 5.0.x before 5.0.4 allows persistent XSS in its Textile formatter due to improper sanitization in Redcloth3 Textile-formatted fields. Depending on the configuration, this may require login as a registered user.	6.1	More Details
CVE-2022-46350	A vulnerability has been identified in SCALANCE X204RNA (HSR) (All versions < V3.2.7), SCALANCE X204RNA (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (HSR) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP/HSR) (All versions < V3.2.7). The integrated web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. This can be used by an attacker to trigger a malicious request on the affected device.	6.1	More Details
CVE-2022-4413	Cross-site Scripting (XSS) - Reflected in GitHub repository nuxt/framework prior to v3.0.0-rc.13.	6.1	More Details
CVE-2022-4414	Cross-site Scripting (XSS) - DOM in GitHub repository nuxt/framework prior to v3.0.0-rc.13.	6.1	More Details
CVE-2022-45028	A cross-site scripting (XSS) vulnerability in Arris NVG443B 9.3.0h3d36 allows attackers to execute arbitrary web scripts or HTML via a crafted POST request sent to /cgi-bin/logs.ha.	6.1	More Details
CVE-2022-44031	Redmine before 4.2.9 and 5.0.x before 5.0.4 allows persistent XSS in its Textile formatter due to improper sanitization of the blockquote syntax in Textile-formatted fields.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46905	Insufficient processing of user input in WebSoft HCM 2021.2.3.327 allows an unauthenticated attacker to inject arbitrary HTML tags into the page processed by the user's browser, including scripts in the JavaScript programming language, which leads to Reflected XSS.	6.1	More Details
CVE-2022-46683	Jenkins Google Login Plugin 1.4 through 1.6 (both inclusive) improperly determines that a redirect URL after login is legitimately pointing to Jenkins.	6.1	More Details
CVE-2022-45756	SENS v1.0 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2022-41262	Due to insufficient input validation, SAP NetWeaver AS Java (HTTP Provider Service) - version 7.50, allows an unauthenticated attacker to inject a script into a web request header. On successful exploitation, an attacker can view or modify information causing a limited impact on the confidentiality and integrity of the application.	6.1	More Details
CVE-2022-31596	Under certain conditions, an attacker authenticated as a CMS administrator and with high privileges access to the Network in SAP BusinessObjects Business Intelligence Platform (Monitoring DB) - version 430, can access BOE Monitoring database to retrieve and modify (non-personal) system data which would otherwise be restricted. Also, a potential attack could be used to leave the CMS's scope and impact the database. A successful attack could have a low impact on confidentiality, a high impact on integrity, and a low impact on availability.	6.0	More Details
CVE-2022-41261	SAP Solution Manager (Diagnostic Agent) - version 7.20, allows an authenticated attacker on Windows system to access a file containing sensitive data which can be used to access a configuration file which contains credentials to access other system files. Successful exploitation can make the attacker access files and systems for which he/she is not authorized.	6.0	More Details
CVE-2022-37907	A vulnerability exists in the ArubaOS bootloader on 7xxx series controllers which can result in a denial of service (DoS) condition on an impacted system. A successful attacker can cause a system hang which can only be resolved via a power cycle of the impacted controller.	5.8	More Details
CVE-2022-37908	An authenticated attacker can impact the integrity of the ArubaOS bootloader on 7xxx series controllers. Successful exploitation can compromise the hardware chain of trust on the impacted controller.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3881	The WP Tools Increase Maximum Limits, Repair, Server PHP Info, Javascript errors, File Permissions, Transients, Error Log WordPress plugin before 3.43 does not have proper authorisation and CSRF in an AJAX action, allowing any authenticated users, such as subscriber to call it and install and activate arbitrary plugins from wordpress.org	5.7	More Details
CVE-2022-46142	Affected devices store the CLI user passwords encrypted in flash memory. Attackers with physical access to the device could retrieve the file and decrypt the CLI user passwords.	5.7	More Details
CVE-2022-23471	containerd is an open source container runtime. A bug was found in containerd's CRI implementation where a user can exhaust memory on the host. In the CRI stream server, a goroutine is launched to handle terminal resize events if a TTY is requested. If the user's process fails to launch due to, for example, a faulty command, the goroutine will be stuck waiting to send without a receiver, resulting in a memory leak. Kubernetes and crictl can both be configured to use containerd's CRI implementation and the stream server is used for handling container IO. This bug has been fixed in containerd 1.6.12 and 1.5.16. Users should update to these versions to resolve the issue. Users unable to upgrade should ensure that only trusted images and commands are used and that only trusted users have permissions to execute commands in running containers.	5.7	More Details
CVE-2022-39899	Improper authentication vulnerability in Samsung WindowManagerService prior to SMR Dec-2022 Release 1 allows attacker to send the input event using S Pen gesture.	5.7	More Details
CVE-2022-38124	Debug tool in Secomea SiteManager allows logged-in administrator to modify system state in an unintended manner.	5.7	More Details
CVE-2022-46824	In JetBrains IntelliJ IDEA before 2022.2.4 a buffer overflow in the fsnotifier daemon on macOS was possible.	5.6	More Details
CVE-2022-20471	In SendIncDecRestoreCmdPart2 of NxpMfcReader.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-238177877	5.5	More Details
CVE-2022-44699	Azure Network Watcher Agent Security Feature Bypass Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20502	In GetResolvedMethod of entrypoint_utils-inl.h, there is a possible use after free due to a stale cache. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-222166527	5.5	More Details
CVE-2022-46351	A vulnerability has been identified in SCALANCE X204RNA (HSR) (All versions < V3.2.7), SCALANCE X204RNA (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (HSR) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP/HSR) (All versions < V3.2.7). Specially crafted PROFINET DCP packets could cause a denial of service condition of affected products on a local Ethernet segment (Layer 2).	5.5	More Details
CVE-2022-20500	In loadFromXml of ShortcutPackage.java, there is a possible crash on boot due to an uncaught exception. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-246540168	5.5	More Details
CVE-2022-20476	In setEnabledSetting of PackageManager.java, there is a possible way to get the device into an infinite reboot loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-240936919	5.5	More Details
CVE-2022-20496	In setDataSource of initMediaExtractor.cpp, there is a possibility of arbitrary code execution due to a use after free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-245242273	5.5	More Details
CVE-2022-4454	A vulnerability, which was classified as critical, has been found in m0ver bible-online. Affected by this issue is the function query of the file src/main/java/custom/application/search.java of the component Search Handler. The manipulation leads to sql injection. The name of the patch is 6ef0aabfb2d4ccd53fcaa9707781303af357410e. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-215444.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4207	The Image Hover Effects Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several values that can be added to an Image Hover in versions 9.8.1 to 9.8.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, the plugin only allows administrators access to edit Image Hovers, however, if a site admin makes the plugin's features available to lower privileged users through the 'Who Can Edit?' setting then this can be exploited by those users.	5.5	More Details
CVE-2022-25675	Denial of service due to reachable assertion in modem while processing filter rule from application client in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Mobile	5.5	More Details
CVE-2022-31697	The vCenter Server contains an information disclosure vulnerability due to the logging of credentials in plaintext. A malicious actor with access to a workstation that invoked a vCenter Server Appliance ISO operation (Install/Upgrade/Migrate/Restore) can access plaintext passwords used during that operation.	5.5	More Details
CVE-2022-44674	Windows Bluetooth Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2022-20482	In createNotificationChannel of NotificationManager.java, there is a possible way to make the device unusable and require factory reset due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-240422263	5.5	More Details
CVE-2022-20466	In applyKeyguardFlags of NotificationShadeWindowControllerImpl.java, there is a possible way to observe the user's password on a secondary display due to an insecure default value. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-179725730	5.5	More Details
CVE-2022-41074	Windows Graphics Component Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44647	An Out-of-bounds read vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to disclose sensitive information on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is similar to, but not the same as CVE-2022-44648.	5.5	More Details
CVE-2022-44874	wasm3 commit 7890a2097569fde845881e0b352d813573e371f9 was discovered to contain a segmentation fault via the component op_CallIndirect at /m3_exec.h.	5.5	More Details
CVE-2021-0934	In findAllDeAccounts of AccountsDb.java, there is a possible denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-169762606	5.5	More Details
CVE-2022-4312	A cleartext storage of sensitive information vulnerability exists in PcVue versions 8.10 through 15.2.3. This could allow an unauthorized user with access the email and short messaging service (SMS) accounts configuration files to discover the associated simple mail transfer protocol (SMTP) account credentials and the SIM card PIN code. Successful exploitation of this vulnerability could allow an unauthorized user access to the underlying email account and SIM card.	5.5	More Details
CVE-2022-2752	A vulnerability in the web server of Secomea GateManager allows a local user to impersonate as the previous user under some failed login conditions. This issue affects: Secomea GateManager versions from 9.4 through 9.7.	5.5	More Details
CVE-2022-33187	Brocade SANnav before v2.2.1 logs usernames and encoded passwords in debug-enabled logs. The vulnerability could allow an attacker with admin privilege to read sensitive information.	5.5	More Details
CVE-2022-37926	A vulnerability within the web-based management interface of EdgeConnect Enterprise could allow a remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface by uploading a specially crafted file. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42328	Guests can trigger deadlock in Linux netback driver T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] The patch for XSA-392 introduced another issue which might result in a deadlock when trying to free the SKB of a packet dropped due to the XSA-392 handling (CVE-2022-42328). Additionally when dropping packages for other reasons the same deadlock could occur in case of netpoll being active for the interface the xen-netback driver is connected to (CVE-2022-42329).	5.5	More Details
CVE-2022-4399	A vulnerability was found in TicklishHoneyBee nodau. It has been rated as critical. Affected by this issue is some unknown functionality of the file src/db.c. The manipulation of the argument value/name leads to sql injection. The name of the patch is 7a7d737a3929f335b9717ddbd31db91151b69ad2. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-215252.	5.5	More Details
CVE-2022-41783	tdpServer of TP-Link RE300 V1 improperly processes its input, which may allow an attacker to cause a denial-of-service (DoS) condition of the product's OneMesh function.	5.5	More Details
CVE-2022-44648	An Out-of-bounds read vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to disclose sensitive information on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is similar to, but not the same as CVE-2022-44647.	5.5	More Details
CVE-2022-42329	Guests can trigger deadlock in Linux netback driver T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] The patch for XSA-392 introduced another issue which might result in a deadlock when trying to free the SKB of a packet dropped due to the XSA-392 handling (CVE-2022-42328). Additionally when dropping packages for other reasons the same deadlock could occur in case of netpoll being active for the interface the xen-netback driver is connected to (CVE-2022-42329).	5.5	More Details
CVE-2021-44694	Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial of service in the device.	5.5	More Details
CVE-2022-4408	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.9.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46687	Jenkins Spring Config Plugin 2.0.0 and earlier does not escape build display names shown on the Spring Config view, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to change build display names.	5.4	More Details
CVE-2022-46686	Jenkins Custom Build Properties Plugin 2.79.vc095ccc85094 and earlier does not escape property values and build display names on the Custom Build Properties and Build Summary pages, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to set or change these values.	5.4	More Details
CVE-2022-46684	Jenkins Checkmarx Plugin 2022.3.3 and earlier does not escape values returned from the Checkmarx service API before inserting them into HTML reports, resulting in a stored cross-site scripting (XSS) vulnerability.	5.4	More Details
CVE-2022-45970	Alist v3.5.1 is vulnerable to Cross Site Scripting (XSS) via the bulletin board.	5.4	More Details
CVE-2022-44731	A vulnerability has been identified in SIMATIC WinCC OA V3.15 (All versions < V3.15 P038), SIMATIC WinCC OA V3.16 (All versions < V3.16 P035), SIMATIC WinCC OA V3.17 (All versions < V3.17 P024), SIMATIC WinCC OA V3.18 (All versions < V3.18 P014). The affected component allows to inject custom arguments to the Ultralight Client backend application under certain circumstances. This could allow an authenticated remote attacker to inject arbitrary parameters when starting the client via the web interface (e.g., open attacker chosen panels with the attacker's credentials or start a Ctrl script).	5.4	More Details
CVE-2022-46265	A vulnerability has been identified in Polarion ALM (All versions < V2304.0). The affected application contains a Host header injection vulnerability that could allow an attacker to spoof a Host header information and redirect users to malicious websites.	5.4	More Details
CVE-2022-45758	SENS v1.0 is vulnerable to Cross Site Scripting (XSS) via com.liuyanzhao.sens.web.controller.admin, getRegister.	5.4	More Details
CVE-2022-34318	IBM CICS TX 11.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 229461.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25630	An authenticated user can embed malicious content with XSS into the admin group policy page.	5.4	More Details
CVE-2022-34297	Yii Yii2 Gii through 2.2.4 allows stored XSS by injecting a payload into any field.	5.4	More Details
CVE-2022-4336	In BAOTA linux panel there exists a stored xss vulnerability attackers can use to obtain sensitive information via the log analysis feature.	5.4	More Details
CVE-2022-3933	The Essential Real Estate WordPress plugin before 3.9.6 does not sanitize and escapes some parameters, which could allow users with a role as low as Admin to perform Cross-Site Scripting attacks.	5.4	More Details
CVE-2022-25629	An authenticated user who has the privilege to add/edit annotations on the Content tab, can craft a malicious annotation that can be executed on the annotations page (Annotation Text Column).	5.4	More Details
CVE-2022-41947	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. Through various features of DHIS2, an authenticated user may be able to upload a file which includes embedded javascript. The user could then potentially trick another authenticated user to open the malicious file in a browser which would trigger the javascript code, resulting in a cross-site scripting (XSS) attack. DHIS2 administrators should upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. Users unable to upgrade may add the following simple CSP rule in your web proxy to the vulnerable endpoints: `script-src 'none'`. This workaround will prevent all javascript from running on those endpoints.	5.4	More Details
CVE-2022-23494	tinymce is an open source rich text editor. A cross-site scripting (XSS) vulnerability was discovered in the alert and confirm dialogs when these dialogs were provided with malicious HTML content. This can occur in plugins that use the alert or confirm dialogs, such as in the `image` plugin, which presents these dialogs when certain errors occur. The vulnerability allowed arbitrary JavaScript execution when an alert presented in the TinyMCE UI for the current user. This vulnerability has been patched in TinyMCE 5.10.7 and TinyMCE 6.3.1 by ensuring HTML sanitization was still performed after unwrapping invalid elements. Users are advised to upgrade to either 5.10.7 or 6.3.1. Users unable to upgrade may ensure the the `images_upload_handler` returns a valid value as per the images_upload_handler documentation.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44698	Windows SmartScreen Security Feature Bypass Vulnerability	5.4	More Details
CVE-2022-44361	An issue was discovered in ZZCMS 2022. There is a cross-site scripting (XSS) vulnerability in admin/ad_list.php.	5.4	More Details
CVE-2022-41735	IBM Business Process Manager 21.0.1 through 21.0.3.1, 20.0.0.1 through 20.0.0.2 19.0.0.1 through 19.0.0.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 65687.	5.4	More Details
CVE-2022-45217	A cross-site scripting (XSS) vulnerability in Book Store Management System v1.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Level parameter under the Add New System User module.	5.4	More Details
CVE-2022-45916	ILIAS before 7.16 allows XSS.	5.4	More Details
CVE-2022-43996	The csaf_provider package before 0.8.2 allows XSS via a crafted CSAF document uploaded as text/html. The endpoint upload allows valid CSAF advisories (JSON format) to be uploaded with Content-Type text/html and filenames ending in .html. When subsequently accessed via web browser, these advisories are served and interpreted as HTML pages. Such uploaded advisories can contain JavaScript code that will execute within the browser context of users inspecting the advisory.	5.4	More Details
CVE-2022-3853	Cross-site Scripting (XSS) is a client-side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application.	5.4	More Details
CVE-2021-38997	IBM API Connect V10.0.0.0 through V10.0.5.0, V10.0.1.0 through V10.0.1.7, and V2018.4.1.0 through 2018.4.1.19 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 213212.	5.4	More Details
CVE-2022-3934	The FlatPM WordPress plugin before 3.0.13 does not sanitise and escape some parameters before outputting them back in pages, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3935	The Welcart e-Commerce WordPress plugin before 2.8.4 does not sanitise and escape some parameters, which could allow any authenticated users, such as subscriber to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-4005	The Donation Button WordPress plugin through 4.0.0 does not sanitize and escapes some parameters, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks.	5.4	More Details
CVE-2022-46903	Insufficient processing of user input in WebSoft HCM 2021.2.3.327 allows an authenticated attacker to inject arbitrary HTML tags into the page processed by the user's browser, including scripts in the JavaScript programming language, which leads to Stored XSS.	5.4	More Details
CVE-2022-46904	Insufficient processing of user input in WebSoft HCM 2021.2.3.327 allows an authenticated attacker to inject arbitrary HTML tags into the page processed by the user's browser, including scripts in the JavaScript programming language, which leads to Self-XSS.	5.4	More Details
CVE-2022-46906	Insufficient processing of user input in WebSoft HCM 2021.2.3.327 allows an authenticated attacker to inject arbitrary HTML tags into the page processed by the user's browser, including scripts in the JavaScript programming language, which leads to Reflected XSS.	5.4	More Details
CVE-2022-31698	The vCenter Server contains a denial-of-service vulnerability in the content library service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to trigger a denial-of-service condition by sending a specially crafted header.	5.3	More Details
CVE-2022-20691	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Adaptive Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause a DoS condition of an affected device. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol packets to an affected device. A successful exploit could allow the attacker to cause the device to exhaust available memory and cause the service to restart. Cisco has released firmware updates that address this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20690	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device.	5.3	More Details
CVE-2022-37909	Aruba has identified certain configurations of ArubaOS that can lead to sensitive information disclosure from the configured ESSIDs. The scenarios in which disclosure of potentially sensitive information can occur are complex, and depend on factors beyond the control of attackers.	5.3	More Details
CVE-2022-20689	Multiple vulnerabilities in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, adjacent attacker to cause Cisco Discovery Protocol memory corruption on an affected device. These vulnerabilities are due to missing length validation checks when processing Cisco Discovery Protocol messages. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read of the valid Cisco Discovery Protocol packet data, which could allow the attacker to cause corruption in the internal Cisco Discovery Protocol database of the affected device.	5.3	More Details
CVE-2022-20688	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause Cisco Discovery Protocol service to restart. This vulnerability is due to missing length validation of certain Cisco Discovery Protocol packet header fields. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause Cisco Discovery Protocol to restart unexpectedly, resulting in a DoS condition.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20687	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition.	5.3	More Details
CVE-2022-20686	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) functionality of Cisco ATA 190 Series Analog Telephone Adapter firmware could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device and cause the LLDP service to restart. These vulnerabilities are due to missing length validation of certain LLDP packet header fields. An attacker could exploit these vulnerabilities by sending a malicious LLDP packet to an affected device. A successful exploit could allow the attacker to execute code on the affected device and cause LLDP to restart unexpectedly, resulting in a denial of service (DoS) condition.	5.3	More Details
CVE-2020-36565	Due to improper sanitization of user input on Windows, the static file handler allows for directory traversal, allowing an attacker to read files outside of the target directory that the server has permission to read.	5.3	More Details
CVE-2022-45910	Improper neutralization of special elements used in an LDAP query ('LDAP Injection') vulnerability in ActiveDirectory and Sharepoint ActiveDirectory authority connectors of Apache ManifoldCF allows an attacker to manipulate the LDAP search queries (DoS, additional queries, filter manipulation) during user lookup, if the username or the domain string are passed to the UserACLs servlet without validation. This issue affects Apache ManifoldCF version 2.23 and prior versions.	5.3	More Details
CVE-2022-4097	The All-In-One Security (AIOS) WordPress plugin before 5.0.8 is susceptible to IP Spoofing attacks, which can lead to bypassed security features (like IP blocks, rate limiting, brute force protection, and more).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46354	A vulnerability has been identified in SCALANCE X204RNA (HSR) (All versions < V3.2.7), SCALANCE X204RNA (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (HSR) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP/HSR) (All versions < V3.2.7). The webserver of an affected device is missing specific security headers. This could allow an remote attacker to extract confidential session information under certain circumstances.	5.3	More Details
CVE-2022-4122	A vulnerability was found in buildah. Incorrect following of symlinks while reading .containerignore and .dockerignore results in information disclosure.	5.3	More Details
CVE-2022-41881	Netty project is an event-driven asynchronous network application framework. In versions prior to 4.1.86.Final, a StackOverflowError can be raised when parsing a malformed crafted message due to an infinite recursion. This issue is patched in version 4.1.86.Final. There is no workaround, except using a custom HaProxyMessageDecoder.	5.3	More Details
CVE-2022-45292	User invites for Funkwhale v1.2.8 do not permanently expire after being used for signup and can be used again after an account has been deleted.	5.3	More Details
CVE-2022-45956	Boa Web Server versions 0.94.13 through 0.94.14 fail to validate the correct security constraint on the HEAD HTTP method allowing everyone to bypass the Basic Authorization mechanism.	5.3	More Details
CVE-2022-41717	An attacker can cause excessive memory growth in a Go server accepting HTTP/2 requests. HTTP/2 server connections contain a cache of HTTP header keys sent by the client. While the total number of entries in this cache is capped, an attacker sending very large keys can cause the server to allocate approximately 64 MiB per open connection.	5.3	More Details
CVE-2019-25078	A vulnerability classified as problematic was found in pacparser up to 1.3.x. Affected by this vulnerability is the function pacparser_find_proxy of the file src/pacparser.c. The manipulation of the argument url leads to buffer overflow. Attacking locally is a requirement. Upgrading to version 1.4.0 is able to address this issue. The name of the patch is 853e8f45607cb07b877ffd270c63dbcdd5201ad9. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-215443.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46158	PrestaShop is an open-source e-commerce solution. Versions prior to 1.7.8.8 did not properly restrict host filesystem access for users. Users may have been able to view the contents of the upload directory without appropriate permissions. This issue has been addressed and users are advised to upgrade to version 1.7.8.8. There are no known workarounds for this issue.	5.3	More Details
CVE-2022-23505	Passport-wsfed-saml2 is a ws-federation protocol and SAML2 tokens authentication provider for Passport. In versions prior to 4.6.3, a remote attacker may be able to bypass WSFed authentication on a website using passport-wsfed-saml2. A successful attack requires that the attacker is in possession of an arbitrary IDP signed assertion. Depending on the IDP used, fully unauthenticated attacks (e.g without access to a valid user) might also be feasible if generation of a signed message can be triggered. This issue is patched in version 4.6.3. Use of SAML2 authentication instead of WSFed is a workaround.	5.3	More Details
	A vulnerability has been identified in SIPROTEC 5 6MD84 (CP300) (All versions < V9.50), SIPROTEC 5 6MD85 (CP200) (All versions), SIPROTEC 5 6MD85 (CP300) (All versions < V9.50), SIPROTEC 5 6MD86 (CP200) (All versions), SIPROTEC 5 6MD86 (CP300) (All versions < V9.50), SIPROTEC 5 6MD89 (CP300) (All versions < V9.64), SIPROTEC 5 6MU85 (CP300) (All versions < V9.50), SIPROTEC 5 7KE85 (CP200) (All versions), SIPROTEC 5 7KE85 (CP300) (All versions < V9.64), SIPROTEC 5 7SA82 (CP100) (All versions), SIPROTEC 5 7SA82 (CP150) (All versions < V9.50), SIPROTEC 5 7SA84 (CP200) (All versions), SIPROTEC 5 7SA86 (CP200) (All versions), SIPROTEC 5 7SA86 (CP300) (All versions < V9.50), SIPROTEC 5 7SA87 (CP200) (All versions), SIPROTEC 5 7SA87 (CP300) (All versions < V9.50), SIPROTEC 5 7SD82 (CP100) (All versions), SIPROTEC 5 7SD82 (CP150) (All versions < V9.50), SIPROTEC 5 7SD84 (CP200) (All versions), SIPROTEC 5 7SD86 (CP200) (All versions), SIPROTEC 5 7SD86 (CP300) (All versions < V9.50), SIPROTEC 5 7SD87 (CP200) (All versions), SIPROTEC 5 7SD87 (CP300) (All versions < V9.50), SIPROTEC 5 7SJ81 (CP100) (All versions < V8.89), SIPROTEC 5 7SJ81 (CP150) (All versions < V9.50), SIPROTEC 5 7SJ82 (CP100) (All versions < V8.89), SIPROTEC 5 7SJ82 (CP150) (All versions < V9.50), SIPROTEC 5 7SJ85 (CP200) (All versions), SIPROTEC 5 7SJ85 (CP300) (All versions < V9.50), SIPROTEC 5 7SJ86 (CP200) (All versions), SIPROTEC 5 7SJ86 (CP300) (All versions < V9.50), SIPROTEC 5 7SK82 (CP100) (All versions < V8.89), SIPROTEC 5 7SK82 (CP150) (All versions < V9.50), SIPROTEC 5 7SK85 (CP200) (All versions), SIPROTEC 5 7SK85 (CP300) (All versions < V9.50), SIPROTEC 5 7SL82 (CP100) (All versions), SIPROTEC 5 7SL82 (CP150) (All versions < V9.50), SIPROTEC 5 7SL86 (CP200) (All versions), SIPROTEC 5 7SL86		

CVE Number	Description	Base Score	Reference
CVE-2022-45044	(CP300) (All versions < V9.50), SIPROTEC 5 7SL87 (CP200) (All versions), SIPROTEC 5 7SL87 (CP300) (All versions < V9.50), SIPROTEC 5 7SS85 (CP200) (All versions), SIPROTEC 5 7SS85 (CP300) (All versions < V9.50), SIPROTEC 5 7ST85 (CP200) (All versions), SIPROTEC 5 7ST85 (CP300) (All versions < V9.64), SIPROTEC 5 7ST86 (CP300) (All versions < V9.64), SIPROTEC 5 7SX82 (CP150) (All versions < V9.50), SIPROTEC 5 7SX85 (CP300) (All versions < V9.50), SIPROTEC 5 7UM85 (CP300) (All versions < V9.50), SIPROTEC 5 7UT82 (CP100) (All versions), SIPROTEC 5 7UT82 (CP150) (All versions < V9.50), SIPROTEC 5 7UT85 (CP200) (All versions), SIPROTEC 5 7UT85 (CP300) (All versions < V9.50), SIPROTEC 5 7UT86 (CP200) (All versions), SIPROTEC 5 7UT86 (CP300) (All versions < V9.50), SIPROTEC 5 7UT87 (CP200) (All versions), SIPROTEC 5 7UT87 (CP300) (All versions < V9.50), SIPROTEC 5 7VE85 (CP300) (All versions < V9.50), SIPROTEC 5 7VK87 (CP200) (All versions), SIPROTEC 5 7VK87 (CP300) (All versions < V9.50), SIPROTEC 5 7VU85 (CP300) (All versions < V9.50), SIPROTEC 5 Communication Module ETH-BA-2EL (All versions < V8.89 installed on CP100 devices), SIPROTEC 5 Communication Module ETH-BA-2EL (All versions < V9.50 installed on CP150 and CP300 devices), SIPROTEC 5 Communication Module ETH-BA-2EL (All versions installed on CP200 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (All versions < V8.89 installed on CP100 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (All versions < V9.50 installed on CP150 and CP300 devices), SIPROTEC 5 Communication Module ETH-BB-2FO (All versions installed on CP200 devices), SIPROTEC 5 Communication Module ETH-BD-2FO (All versions < V9.50), SIPROTEC 5 Compact 7SX800 (CP050) (All versions < V9.50). Affected devices do not properly restrict secure client-initiated renegotiations within the SSL and TLS protocols. This could allow an attacker to create a denial of service condition on the ports 443/tcp and 4443/tcp for the duration of the attack.	5.3	More Details
CVE-2022-46828	In JetBrains IntelliJ IDEA before 2022.3 a DYLIB injection on macOS was possible.	5.2	More Details
CVE-2022-41949	DHIS 2 is an open source information system for data capture, management, validation, analytics and visualization. In affected versions an authenticated DHIS2 user can craft a request to DHIS2 to instruct the server to make requests to external resources (like third party servers). This could allow an attacker, for example, to identify vulnerable services which might not be otherwise exposed to the public internet or to determine whether a specific file is present on the DHIS2 server. DHIS2 administrators should upgrade to the following hotfix releases: 2.36.12.1, 2.37.8.1, 2.38.2.1, 2.39.0.1. At this time, there is no known workaround or mitigation for this vulnerability.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44695	Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial of service in the device.	4.9	More Details
CVE-2022-40939	In certain Secustation products the administrator account password can be read. This affects V2.5.5.3116-S50-SMA-B20171107A, V2.3.4.1301-M20-TSA-B20150617A, V2.5.5.3116-S50-RXA-B20180502A, V2.5.5.3116-S50-SMA-B20190723A, V2.5.5.3116-S50-SMB-B20161012A, V2.3.4.2103-S50-NTD-B20170508B, V2.5.5.3116-S50-SMB-B20160601A, V2.5.5.2601-S50-TSA-B20151229A, and V2.5.5.3116-S50-SMA-B20170217.	4.9	More Details
CVE-2022-46047	AeroCMS v0.0.1 is vulnerable to SQL Injection via the delete parameter.	4.9	More Details
CVE-2022-43518	An authenticated path traversal vulnerability exists in the Aruba EdgeConnect Enterprise web interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below.	4.9	More Details
CVE-2022-22488	IBM OpenBMC OP910 and OP940 could allow a privileged user to cause a denial of service by uploading or deleting too many CA certificates in a short period of time. IBM X-Force ID: 2226337.	4.9	More Details
CVE-2022-44532	An authenticated path traversal vulnerability exists in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files in Aruba EdgeConnect Enterprise Software version(s): ECOS 9.2.1.0 and below; ECOS 9.1.3.0 and below; ECOS 9.0.7.0 and below; ECOS 8.3.7.1 and below.	4.9	More Details
CVE-2021-44693	Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial of service in the device.	4.9	More Details
CVE-2022-42445	HCL Launch could allow a user with administrative privileges, including "Manage Security" permissions, the ability to recover a credential previously saved for performing authenticated LDAP searches.	4.9	More Details
CVE-2022-37406	Cross-site scripting vulnerability in Aficio SP 4210N firmware versions prior to Web Support 1.05 allows a remote authenticated attacker with an administrative privilege to inject an arbitrary script.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42486	Stored cross-site scripting vulnerability in User group management of baserCMS versions prior to 4.7.2 allows a remote authenticated attacker with an administrative privilege to inject an arbitrary script.	4.8	More Details
CVE-2022-4000	The WooCommerce Shipping WordPress plugin through 1.2.11 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-3260	The response header has not enabled X-FRAME-OPTIONS, Which helps prevents against Clickjacking attack.. Some browsers would interpret these results incorrectly, allowing clickjacking attacks.	4.8	More Details
CVE-2022-39911	Improper check or handling of exceptional conditions vulnerability in Samsung Pass prior to version 4.0.06.1 allows attacker to access Samsung Pass.	4.8	More Details
CVE-2022-3919	The Jetpack CRM WordPress plugin before 5.4.3 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-45008	Online Leave Management System v1.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the component /leave_system/admin/?page=maintenance/department. This vulnerability allows attackers to execute arbitrary web scripts or HTML via crafted payload injected into the Name field under the Create New module.	4.8	More Details
CVE-2022-3609	The GetYourGuide Ticketing WordPress plugin before 1.0.4 does not sanitise and escape some parameters, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-41994	Stored cross-site scripting vulnerability in Permission Settings of baserCMS versions prior to 4.7.2 allows a remote authenticated attacker with an administrative privilege to inject an arbitrary script.	4.8	More Details
CVE-2022-46058	AeroCMS v0.0.1 was discovered to contain a cross-site scripting (XSS) vulnerability via add_post.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Comments text field.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4010	The Image Hover Effects WordPress plugin before 5.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-32537	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system components while the pump is being paired with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced technical knowledge is required for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance	4.8	More Details
CVE-2022-3862	The Livemesh Addons for Elementor WordPress plugin before 7.2.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-3906	The Easy Form Builder WordPress plugin before 3.4.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-44213	ZKTeco Xiamen Information Technology ZKBio ECO ADMS <=3.1-164 is vulnerable to Cross Site Scripting (XSS).	4.8	More Details
CVE-2022-4402	A vulnerability classified as critical has been found in RainyGao DocSys 2.02.37. This affects an unknown part of the component ZIP File Decompression Handler. The manipulation leads to path traversal: '../filedir'. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-215271.	4.7	More Details
CVE-2022-4311	An insertion of sensitive information into log file vulnerability exists in PcVue versions 15 through 15.2.2. This could allow a user with access to the log files to discover connection strings of data sources configured for the DbConnect, which could include credentials. Successful exploitation of this vulnerability could allow other users unauthorized access to the underlying data sources.	4.7	More Details
CVE-2022-44636	The Samsung TV (2021 and 2022 model) smart remote control allows attackers to enable microphone access via Bluetooth spoofing when a user is activating remote control by pressing a button. This is fixed in xxx72510, E9172511 for 2021 models, xxxA1000, 4x2A0200 for 2022 models.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39900	Improper access control vulnerability in Nice Catch prior to SMR Dec-2022 Release 1 allows physical attackers to access contents of all toast generated in the application installed in Secure Folder through Nice Catch.	4.6	More Details
CVE-2022-20497	In updatePublicMode of NotificationLockscreenUserManagerImpl.java, there is a possible way to reveal sensitive notifications on the lockscreen due to an incorrect state transition. This could lead to local information disclosure with physical access required and an app that runs above the lockscreen, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-246301979	4.6	More Details
CVE-2022-46062	Gym Management System v0.0.1 is vulnerable to Cross Site Request Forgery (CSRF).	4.5	More Details
CVE-2022-41299	IBM Cloud Transformation Advisor 2.0.1 through 3.3.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 237214.	4.4	More Details
CVE-2022-20449	In writeApplicationRestrictionsLAr of UserManagerService.java, there is a possible overwrite of system files due to a path traversal error. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-239701237	4.4	More Details
CVE-2022-20498	In fdt_path_offset_namelen of fdt_ro.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12L Android-13Android ID: A-246465319	4.4	More Details
CVE-2022-39897	Exposure of Sensitive Information vulnerability in kernel prior to SMR Dec-2022 Release 1 allows attackers to access the kernel address information via log.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4261	Rapid7 Nexpose and InsightVM versions prior to 6.6.172 failed to reliably validate the authenticity of update contents. This failure could allow an attacker to provide a malicious update and alter the functionality of Rapid7 Nexpose. The attacker would need some pre-existing mechanism to provide a malicious update, either through a social engineering effort, privileged access to replace downloaded updates in transit, or by performing an Attacker-in-the-Middle attack on the update service itself.	4.4	More Details
CVE-2022-37910	A buffer overflow vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in a denial of service on the affected system.	4.4	More Details
CVE-2020-36610	A vulnerability was found in annyshow DuxCMS 2.1. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-215116.	4.3	More Details
CVE-2022-45871	A Denial-of-Service (DoS) vulnerability was discovered in the fsicapd component used in WithSecure products whereby the service may crash while parsing ICAP request. The exploit can be triggered remotely by an attacker.	4.3	More Details
CVE-2022-44688	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4.3	More Details
CVE-2022-4354	A vulnerability was found in LinZhaoguan pb-cms 2.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /blog/comment of the component Message Board. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-215114 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2022-4349	A vulnerability classified as problematic has been found in CTF-hacker pwn. This affects an unknown part of the file delete.html. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-215109 was assigned to this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46160	Tuleap is an Open Source Suite to improve management of software developments and collaboration. In versions prior to 14.2.99.104, project level authorizations are not properly verified when accessing the project "homepage"/dashboards. Users not authorized to access a project may still be able to get some information provided by the widgets (e.g. number of members, content of the Notes widget...). This issue has been patched in Tuleap Community Edition 14.2.99.104, Tuleap Enterprise Edition 14.2-4, and Tuleap Enterprise Edition 14.1-5.	4.3	More Details
CVE-2022-29838	Improper Authentication vulnerability in the encrypted volumes and auto mount features of Western Digital My Cloud devices allows insecure direct access to the drive information in the case of a device reset. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux.	4.3	More Details
CVE-2022-23473	Tuleap is an Open Source Suite to improve management of software developments and collaboration. In versions prior to 14.2.99.148, Authorizations are not properly verified when accessing MediaWiki standalone resources. Users with read only permissions for pages are able to also edit them. This only affects the MediaWiki standalone plugin. This issue is patched in versions Tuleap Community Edition 14.2.99.148, Tuleap Enterprise Edition 14.2-5, and Tuleap Enterprise Edition 14.1-6.	4.3	More Details
CVE-2022-41273	Due to improper input sanitization in SAP Sourcing and SAP Contract Lifecycle Management - version 1100, an attacker can redirect a user to a malicious website. In order to perform this attack, the attacker sends an email to the victim with a manipulated link that appears to be a legitimate SAP Sourcing URL, since the victim doesn’t suspect the threat, they click on the link, log in to SAP Sourcing and CLM and at this point, they get redirected to a malicious website.	4.3	More Details
CVE-2022-46685	In Jenkins Gitea Plugin 1.4.4 and earlier, the implementation of Gitea personal access tokens did not support credentials masking, potentially exposing them through the build log.	4.3	More Details
CVE-2022-4004	The Donation Button WordPress plugin through 4.0.0 does not properly check for privileges and nonce tokens in its "donation_button_twilio_send_test_sms" AJAX action, which may allow any users with an account on the affected site, like subscribers, to use the plugin's Twilio integration to send SMSes to arbitrary phone numbers.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4397	A vulnerability was found in morontt zend-blog-number-2. It has been classified as problematic. Affected is an unknown function of the file application/forms/Comment.php of the component Comment Handler. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. The name of the patch is 36b2d4abe20a6245e4f8df7a4b14e130b24d429d. It is recommended to apply a patch to fix this issue. VDB-215250 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2022-41263	Due to a missing authentication check, SAP Business Objects Business Intelligence Platform (Web Intelligence) - versions 420, 430, allows an authenticated non-administrator attacker to modify the data source information for a document that is otherwise restricted. On successful exploitation, the attacker can modify information causing a limited impact on the integrity of the application.	4.3	More Details
CVE-2022-46830	In JetBrains TeamCity between 2022.10 and 2022.10.1 a custom STS endpoint allowed internal port scanning.	4.1	More Details
CVE-2022-29839	Insufficiently Protected Credentials vulnerability in the remote backups application on Western Digital My Cloud devices that could allow an attacker who has gained access to a relevant endpoint to use that information to access protected data. This issue affects: Western Digital My Cloud My Cloud versions prior to 5.25.124 on Linux.	4.1	More Details
CVE-2022-39898	Improper access control vulnerability in IIccPhoneBook prior to SMR Dec-2022 Release 1 allows attackers to access some information of usim.	4.0	More Details
CVE-2022-39914	Exposure of Sensitive Information from an Unauthorized Actor vulnerability in Samsung DisplayManagerService prior to Android T(13) allows local attacker to access connected DLNA device information.	4.0	More Details
CVE-2022-46825	In JetBrains IntelliJ IDEA before 2022.3 the built-in web server leaked information about open projects.	4.0	More Details
CVE-2022-39896	Improper access control vulnerabilities in Contacts prior to SMR Dec-2022 Release 1 allows to access sensitive information via implicit intent.	4.0	More Details
CVE-2022-39905	Implicit intent hijacking vulnerability in Telecom application prior to SMR Dec-2022 Release 1 allows attacker to access sensitive information via implicit intent.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39903	Improper access control vulnerability in RCS call prior to SMR Dec-2022 Release 1 allows local attackers to access RCS incoming call number.	4.0	More Details
CVE-2022-39895	Improper access control vulnerability in ContactListUtils in Phone prior to SMR Dec-2022 Release 1 allows to access contact group information via implicit intent.	4.0	More Details
CVE-2022-23523	In versions prior to 0.8.1, the linux-loader crate uses the offsets and sizes provided in the ELF headers to determine the offsets to read from. If those offsets point beyond the end of the file this could lead to Virtual Machine Monitors using the `linux-loader` crate entering an infinite loop if the ELF header of the kernel they are loading was modified in a malicious manner. This issue has been addressed in 0.8.1. The issue can be mitigated by ensuring that only trusted kernel images are loaded or by verifying that the headers do not point beyond the end of the file.	4.0	More Details
CVE-2022-39894	Improper access control vulnerability in ContactListStartActivityHelper in Phone prior to SMR Dec-2022 Release 1 allows to access sensitive information via implicit intent.	4.0	More Details
CVE-2022-41802	Kernel subsystem within OpenHarmony-v3.1.4 and prior versions in kernel_liteos_a has a kernel stack overflow vulnerability when call SysClockGetres. 4 bytes padding data from kernel stack are copied to user space incorrectly and leaked.	4.0	More Details
CVE-2022-39910	Improper access control vulnerability in Samsung Pass prior to version 4.0.06.7 allow physical attackers to access data of Samsung Pass on a certain state of an unlocked device using pop-up view.	3.9	More Details
CVE-2022-46827	In JetBrains IntelliJ IDEA before 2022.3 an XXE attack leading to SSRF via requests to custom plugin repositories was possible.	3.9	More Details
CVE-2022-37911	Due to improper restrictions on XML entities multiple vulnerabilities exist in the command line interface of ArubaOS. A successful exploit could allow an authenticated attacker to retrieve files from the local system or cause the application to consume system resources, resulting in a denial of service condition.	3.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4455	A vulnerability, which was classified as problematic, was found in sproctor php-calendar. This affects an unknown part of the file index.php. The manipulation of the argument $_SERVER['PHP_SELF'] leads to cross site scripting. It is possible to initiate the attack remotely. The name of the patch is a2941109b42201c19733127ced763e270a357809. It is recommended to apply a patch to fix this issue. The identifier VDB-215445 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4377	A vulnerability was found in S-CMS 5.0 Build 20220328. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Contact Information Page. The manipulation of the argument Make a Call leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-215197 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4353	A vulnerability has been found in LinZhaoguan pb-cms 2.0 and classified as problematic. Affected by this vulnerability is the function IpUtil.getIpAddr. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-215113 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4456	A vulnerability has been found in falling-fruit and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. The attack can be initiated remotely. The name of the patch is 15adb8e1ea1f1c3e3d152fc266071f621ef0c621. It is recommended to apply a patch to fix this issue. VDB-215446 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-4444	A vulnerability was found in ipti br.tag. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 2.13.0 is able to address this issue. The name of the patch is 7e311be22d3a0a1b53e61cb987ba13d681d85f06. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-215431.	3.5	More Details
CVE-2022-4348	A vulnerability was found in y_project RuoYi-Cloud. It has been rated as problematic. Affected by this issue is some unknown functionality of the component JSON Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-215108.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4347	A vulnerability was found in xiandafu beetl-bbs. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file WebUtils.java. The manipulation of the argument user leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-215107.	3.5	More Details
CVE-2022-45228	Dragino Lora LG01 18ed40 IoT v4.3.4 was discovered to contain a Cross-Site Request Forgery in the logout page.	3.5	More Details
CVE-2022-4401	A vulnerability was found in pallidlight online-course-selection-system. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-215268.	3.5	More Details
CVE-2022-23469	Traefik is an open source HTTP reverse proxy and load balancer. Versions prior to 2.9.6 are subject to a potential vulnerability in Traefik displaying the Authorization header in its debug logs. In certain cases, if the log level is set to DEBUG, credentials provided using the Authorization header are displayed in the debug logs. Attackers must have access to a users logging system in order for credentials to be stolen. This issue has been addressed in version 2.9.6. Users are advised to upgrade. Users unable to upgrade may set the log level to `INFO`, `WARN`, or `ERROR`.	3.5	More Details
CVE-2022-4421	A vulnerability was found in rAthena FluxCP. It has been classified as problematic. Affected is an unknown function of the file themes/default/servicedesk/view.php of the component Service Desk Image URL Handler. The manipulation of the argument sslink leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is 8a39b2b2bf28353b3503ff1421862393db15aa7e. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-215304.	3.5	More Details
CVE-2022-4341	A vulnerability has been found in csliuwy coder-chain_gdut and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /back/index.php/user/User/?1. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-215095.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4400	A vulnerability was found in zbl1996 FS-Blog and classified as problematic. This issue affects some unknown processing of the component Title Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-215267.	3.5	More Details
CVE-2022-4396	A vulnerability was found in RDFlib pyrdfa3 and classified as problematic. This issue affects the function _get_option of the file pyRdfa/__init__.py. The manipulation leads to cross site scripting. The attack may be initiated remotely. The name of the patch is ffd1d62dd50d5f4190013b39cedcdfbd81f3ce3e. It is recommended to apply a patch to fix this issue. The identifier VDB-215249 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2022-4350	A vulnerability, which was classified as problematic, was found in Mingsoft MCMS 5.2.8. Affected is an unknown function of the file search.do. The manipulation of the argument content_title leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-215112.	3.5	More Details
CVE-2022-41287	A vulnerability has been identified in JT2Go (All versions < V14.1.0.6), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.8), Teamcenter Visualization V14.0 (All versions < V14.0.0.4), Teamcenter Visualization V14.1 (All versions < V14.1.0.6). The CGM_NIST_Loader.dll contains divide by zero vulnerability when parsing a CGM file. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	3.3	More Details
CVE-2022-41288	A vulnerability has been identified in JT2Go (All versions < V14.1.0.6), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.8), Teamcenter Visualization V14.0 (All versions < V14.0.0.4), Teamcenter Visualization V14.1 (All versions < V14.1.0.6). The CGM_NIST_Loader.dll contains stack exhaustion vulnerability when parsing a CGM file. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41280	A vulnerability has been identified in JT2Go (All versions < V14.1.0.6), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.8), Teamcenter Visualization V14.0 (All versions < V14.0.0.4), Teamcenter Visualization V14.1 (All versions < V14.1.0.6). The CGM_NIST_Loader.dll contains a null pointer dereference vulnerability while parsing specially crafted CGM files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	3.3	More Details
CVE-2022-4123	A flaw was found in Buildah. The local path and the lowest subdirectory may be disclosed due to incorrect absolute path traversal, resulting in an impact to confidentiality.	3.3	More Details
CVE-2022-45484	A vulnerability has been identified in JT2Go (All versions < V14.1.0.6), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.9), Teamcenter Visualization V13.3 (All versions < V13.3.0.8), Teamcenter Visualization V14.0 (All versions < V14.0.0.5), Teamcenter Visualization V14.0 (All versions < V14.0.0.4), Teamcenter Visualization V14.1 (All versions < V14.1.0.6). The CCITT_G4Decode.dll contains an out of bounds read vulnerability when parsing a RAS file. An attacker can leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19056)	3.3	More Details
CVE-2022-31699	VMware ESXi contains a heap-overflow vulnerability. A malicious local actor with restricted privileges within a sandbox process may exploit this issue to achieve a partial information disclosure.	3.3	More Details
CVE-2022-39904	Exposure of Sensitive Information vulnerability in Samsung Settings prior to SMR Dec-2022 Release 1 allows local attackers to access the Network Access Identifier via log.	3.3	More Details
CVE-2022-41278	A vulnerability has been identified in JT2Go (All versions < V14.1.0.6), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.8), Teamcenter Visualization V14.0 (All versions < V14.0.0.4), Teamcenter Visualization V14.1 (All versions < V14.1.0.6). The CGM_NIST_Loader.dll contains a null pointer dereference vulnerability while parsing specially crafted CGM files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	3.3	More Details
CVE-2022-39915	Improper access control vulnerability in Calendar prior to versions 11.6.08.0 in Android Q(10), 12.2.11.3000 in Android R(11), 12.3.07.2000 in Android S(12), and 12.4.02.0 in Android T(13) allows attackers to access sensitive information via implicit intent.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41279	A vulnerability has been identified in JT2Go (All versions < V14.1.0.6), Teamcenter Visualization V13.2 (All versions < V13.2.0.12), Teamcenter Visualization V13.3 (All versions < V13.3.0.8), Teamcenter Visualization V14.0 (All versions < V14.0.0.4), Teamcenter Visualization V14.1 (All versions < V14.1.0.6). The CGM_NIST_Loader.dll contains a null pointer dereference vulnerability while parsing specially crafted CGM files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	3.3	More Details
CVE-2022-46143	Affected devices do not check the TFTP blocksize correctly. This could allow an authenticated attacker to read from an uninitialized buffer that potentially contains previously allocated data.	2.7	More Details
CVE-2021-4244	A vulnerability classified as problematic has been found in yikes-inc-easy-mailchimp-extender Plugin up to 6.8.5. This affects an unknown part of the file admin/partials/ajax/add_field_to_form.php. The manipulation of the argument field_name/merge_tag/field_type/list_id leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 6.8.6 is able to address this issue. The name of the patch is 3662c6593aa1bb4286781214891d26de2e947695. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-215307.	2.6	More Details
CVE-2020-36609	A vulnerability was found in annyshow DuxCMS 2.1. It has been classified as problematic. This affects an unknown part of the file admin.php&r=article/AdminContent/edit of the component Article Handler. The manipulation of the argument content leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-215115.	2.4	More Details
CVE-2022-20240	In sOpAllowSystemRestrictionBypass of AppOpsManager.java, there is a possible leak of location information due to a missing permission check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-231496105	2.3	More Details
CVE-2022-39906	Improper access control vulnerability in SecTelephonyProvider prior to SMR Dec-2022 Release 1 allows attackers to access message information.	2.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23481	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a Out of Bound Read in xrdp_caps_process_confirm_active() function. There are no known workarounds for this issue. Users are advised to upgrade.	0.0	More Details
CVE-2022-23482	xrdp is an open source project which provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP). xrdp < v0.9.21 contain a Out of Bound Read in xrdp_sec_process_mcs_data_CS_CORE() function. There are no known workarounds for this issue. Users are advised to upgrade.	0.0	More Details
CVE-2020-35588	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn. Further investigation showed that it was not a vulnerability. Notes: none.	N/A	More Details
CVE-2021-4243	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-32850. Reason: This candidate is a duplicate of CVE-2021-32850. Notes: All CVE users should reference CVE-2021-32850 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2022-0925	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2021-39617	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-3931	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-43503	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-44147	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-16891. Reason: This candidate is a reservation duplicate of CVE-2019-16891. Notes: All CVE users should reference CVE-2019-16891 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45119	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-20444	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details