تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٩ يوليو إلى ١٥ يوليو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- عالي جدًا: النتيجة الأساسية لـCVSS 9.0-10.0
- عالي: النتيجة الأساسية لـCVSS 7.0-8.9
- متوسط: النتيجة الأساسية لـCVSS 4.0-6.9
- منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 9th of July to 15th of July. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- Critical: CVSS base score of 9.0-10.0
- High: CVSS base score of 7.0-8.9
- Medium: CVSS base score 4.0-6.9
- Low: CVSS base score 0.0-3.9

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-29130	siemens - simatic_cn_4100	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.5). Affected device consists of improper access controls in the configuration files that leads to privilege escalation. An attacker could gain admin access with this vulnerability leading to complete device control.	2023-07-11	10	Critical
CVE-2023-29131	siemens - simatic_cn_4100	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.5). Affected device consists of an incorrect default value in the SSH configuration. This could allow an attacker to bypass network isolation.	2023-07-11	10	Critical
CVE-2023-24489	citrix - sharefile_storage_zones_controller	A vulnerability has been discovered in the customer-managed ShareFile storage zones controller which, if exploited, could allow an unauthenticated attacker to remotely compromise the customer-managed ShareFile storage zones controller.	2023-07-10	9.8	Critical
CVE-2023-28001	fortinet - multiple products	An insufficient session expiration in Fortinet FortiOS 7.0.0 - 7.0.12 and 7.2.0 - 7.2.4 allows an attacker to execute unauthorized code or commands via reusing the session of a deleted user in the REST API.	2023-07-11	9.8	Critical
CVE-2023-32056	microsoft - multiple products	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability	2023-07-11	9.8	Critical
CVE-2023-32057	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-07-11	9.8	Critical
CVE-2023-33154	microsoft - multiple products	Windows Partition Management Driver Elevation of Privilege Vulnerability	2023-07-11	9.8	Critical
CVE-2023-35365	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2023-07-11	9.8	Critical
CVE-2023-35366	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2023-07-11	9.8	Critical
CVE-2023-35367	microsoft - multiple products	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	2023-07-11	9.8	Critical
CVE-2023-37582	apache - multiple products	The RocketMQ NameServer component still has a remote command execution vulnerability as the CVE-2023-33246 issue was not completely fixed in version 5.1.1. When NameServer address are leaked on the extranet and lack permission verification, an attacker can exploit this vulnerability by using the update configuration function on the NameServer component to execute commands as the system users that RocketMQ is running as. It is recommended for users to upgrade their NameServer version to 5.1.2 or above for RocketMQ 5.x or 4.9.7 or above for RocketMQ 4.x to prevent these attacks.	2023-07-12	9.8	Critical
CVE-2023-29300	adobe - multiple products	Adobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction.	2023-07-12	9.8	Critical

CVE-2023-34124	sonicwall - multiple products	The authentication mechanism in SonicWall GMS and Analytics Web Services had insufficient checks, allowing authentication bypass. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	2023-07-13	9.8	Critical
CVE-2023-34128	sonicwall - multiple products	Tomcat application credentials are hardcoded in SonicWall GMS and Analytics configuration file. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	2023-07-13	9.8	Critical
CVE-2023-34130	sonicwall - multiple products	SonicWall GMS and Analytics use outdated Tiny Encryption Algorithm (TEA) with a hardcoded key to encrypt sensitive data. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	2023-07-13	9.8	Critical
CVE-2023-33150	microsoft - multiple products	Microsoft Office Security Feature Bypass Vulnerability	2023-07-11	9.6	Critical
CVE-2023-33987	sap - multiple products	An unauthenticated attacker in SAP Web Dispatcher - versions WEBDISP 7.49, WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.81, WEBDISP 7.85, WEBDISP 7.88, WEBDISP 7.89, WEBDISP 7.90, KERNEL 7.49, KERNEL 7.53, KERNEL 7.54 KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL 7.88, KERNEL 7.89, KERNEL 7.90, KRNL64NUC 7.49, KRNL64UC 7.49, KRNL64UC 7.53, HDB 2.00, XS_ADVANCED_RUNTIME 1.00, SAP_EXTENDED_APP_SERVICES 1, can submit a malicious crafted request over a network to a front-end server which may, over several attempts, result in a back-end server confusing the boundaries of malicious and legitimate messages. This can result in the back-end server executing a malicious payload which can be used to read or modify information on the server or make it temporarily unavailable.	2023-07-11	9.4	Critical
CVE-2023-35871	sap - multiple products	The SAP Web Dispatcher - versions WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.85, WEBDISP 7.89, WEBDISP 7.91, WEBDISP 7.92, WEBDISP 7.93, KERNEL 7.53, KERNEL 7.54 KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.91, KERNEL 7.92, KERNEL 7.93, KRNL64UC 7.53, HDB 2.00, XS_ADVANCED_RUNTIME 1.00, SAP_EXTENDED_APP_SERVICES 1, has a vulnerability that can be exploited by an unauthenticated attacker to cause memory corruption through logical errors in memory management this may leads to information disclosure or system crashes, which can have low impact on confidentiality and high impact on the integrity and availability of the system.	2023-07-11	9.4	Critical
CVE-2023-27867	ibm - multiple products	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code via JNDI Injection. By sending a specially crafted request using the property clientRerouteServerListJNDIName, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249514.	2023-07-10	8.8	High
CVE-2023-27868	ibm - multiple products	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked class instantiation when providing plugin classes. By sending a specially crafted request using the named pluginClassName class, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249516.	2023-07-10	8.8	High
CVE-2023-27869	ibm - multiple products	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked logger injection. By sending a specially crafted request using the named traceFile property, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249517.	2023-07-10	8.8	High
CVE-2023-36922	sap - multiple products	Due to programming error in function module or report, SAP NetWeaver ABAP (IS-OIL) - versions 600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807, allows an authenticated attacker to inject an arbitrary operating system command into an unprotected parameter in a common (default) extension. On successful exploitation, the attacker can read or modify the system data as well as shut down the system.	2023-07-11	8.8	High
CVE-2022-29561	siemens - ruggedcom_rox_mx5000_firmware	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The web interface of the affected devices are vulnerable to Cross-Site Request Forgery attacks. By tricking an authenticated victim user to click a malicious link, an attacker	2023-07-11	8.8	High

		could perform arbitrary actions on the device on behalf of the victim user.			
CVE-2023-34116	zoom - zoom	Improper input validation in the Zoom Desktop Client for Windows before version 5.15.0 may allow an unauthorized user to enable an escalation of privilege via network access.	2023-07-11	8.8	High
CVE-2023-32038	microsoft - multiple products	Microsoft ODBC Driver Remote Code Execution Vulnerability	2023-07-11	8.8	High
CVE-2023-32049	microsoft - multiple products	Windows SmartScreen Security Feature Bypass Vulnerability	2023-07-11	8.8	High
CVE-2023-33134	microsoft - multiple products	Microsoft SharePoint Server Remote Code Execution Vulnerability	2023-07-11	8.8	High
CVE-2023-33153	microsoft - multiple products	Microsoft Outlook Remote Code Execution Vulnerability	2023-07-11	8.8	High
CVE-2023-33157	microsoft - multiple products	Microsoft SharePoint Remote Code Execution Vulnerability	2023-07-11	8.8	High
CVE-2023-33159	microsoft - multiple products	Microsoft SharePoint Server Spoofing Vulnerability	2023-07-11	8.8	High
CVE-2023-33160	microsoft - multiple products	Microsoft SharePoint Server Remote Code Execution Vulnerability	2023-07-11	8.8	High
CVE-2023-35300	microsoft - multiple products	Remote Procedure Call Runtime Remote Code Execution Vulnerability	2023-07-11	8.8	High
CVE-2023-35302	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	2023-07-11	8.8	High
CVE-2023-35303	microsoft - multiple products	USB Audio Class System Driver Remote Code Execution Vulnerability	2023-07-11	8.8	High
CVE-2023-35311	microsoft - multiple products	Microsoft Outlook Security Feature Bypass Vulnerability	2023-07-11	8.8	High
CVE-2023-35315	microsoft - multiple products	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability	2023-07-11	8.8	High
CVE-2023-35322	microsoft - multiple products	Windows Deployment Services Remote Code Execution Vulnerability	2023-07-11	8.8	High
CVE-2023-35364	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	8.8	High
CVE-2023-36884	microsoft - multiple products	Microsoft is investigating reports of a series of remote code execution vulnerabilities impacting Windows and Office products. Microsoft is aware of targeted attacks that attempt to exploit these vulnerabilities by using specially-crafted Microsoft Office documents. An attacker could create a specially crafted Microsoft Office document that enables them to perform remote code execution in the context of the victim. However, an attacker would have to convince the victim to open the malicious file. Upon completion of this investigation, Microsoft will take the appropriate action to help protect our customers. This might include providing a security update through our monthly release process or providing an out-of-cycle security update, depending on customer needs. Please see the Microsoft Threat Intelligence Blog https://aka.ms/Storm-0978 Entry for important information about steps you can take to protect your system from this vulnerability. This CVE will be updated with new information and links to security updates when they become available.	2023-07-11	8.8	High
CVE-2023-24492	citrix - secure_access_client	A vulnerability has been discovered in the Citrix Secure Access client for Ubuntu which, if exploited, could allow an attacker to remotely execute code if a victim user opens an attacker-crafted link and accepts further prompts.	2023-07-11	8.8	High
CVE-2023-37196	schneider-electric - struxureware_data_center_expert	A CWE-89: Improper Neutralization of Special Elements vulnerability used in an SQL Command ('SQL Injection') vulnerability exists that could allow a user already authenticated on DCE to access unauthorized content, change, or delete content, or perform unauthorized actions when tampering with the alert settings of endpoints on DCE.	2023-07-12	8.8	High
CVE-2023-37197	schneider-electric - struxureware_data_center_expert	A CWE-89: Improper Neutralization of Special Elements vulnerability used in an SQL Command ('SQL Injection') vulnerability exists that could allow a user already authenticated on DCE to access unauthorized content, change, or delete content, or perform unauthorized actions when tampering with the mass configuration settings of endpoints on	2023-07-12	8.8	High

		DCE.			
CVE-2023-32200	apache - jena	There is insufficient restrictions of called script functions in Apache Jena versions 4.8.0 and earlier. It allows a remote user to execute javascript via a SPARQL query. This issue affects Apache Jena: from 3.7.0 through 4.8.0.	2023-07-12	8.8	High
CVE-2022-42009	apache - ambari	SpringEL injection in the server agent in Apache Ambari version 2.7.0 to 2.7.6 allows a malicious authenticated user to execute arbitrary code remotely. Users are recommended to upgrade to 2.7.7.	2023-07-12	8.8	High
CVE-2022-45855	apache - ambari	SpringEL injection in the metrics source in Apache Ambari version 2.7.0 to 2.7.6 allows a malicious authenticated user to execute arbitrary code remotely. Users are recommended to upgrade to 2.7.7.	2023-07-12	8.8	High
CVE-2023-30429	apache - multiple products	Incorrect Authorization vulnerability in Apache Software Foundation Apache Pulsar. This issue affects Apache Pulsar: before 2.10.4, and 2.11.0. When a client connects to the Pulsar Function Worker via the Pulsar Proxy where the Pulsar Proxy uses mTLS authentication to authenticate with the Pulsar Function Worker, the Pulsar Function Worker incorrectly performs authorization by using the Proxy's role for authorization instead of the client's role, which can lead to privilege escalation, especially if the proxy is configured with a superuser role. The recommended mitigation for impacted users is to upgrade the Pulsar Function Worker to a patched version. 2.10 Pulsar Function Worker users should upgrade to at least 2.10.4. 2.11 Pulsar Function Worker users should upgrade to at least 2.11.1. 3.0 Pulsar Function Worker users are unaffected. Any users running the Pulsar Function Worker for 2.9.* and earlier should upgrade to one of the above patched versions.	2023-07-12	8.8	High
CVE-2023-3600	mozilla - multiple products	During the worker lifecycle, a use-after-free condition could have occured, which could have led to a potentially exploitable crash. This vulnerability affects Firefox < 115.0.2 and Firefox ESR < 115.0.2.	2023-07-12	8.8	High
CVE-2023-37957	jenkins - pipeline_restful_api	A cross-site request forgery (CSRF) vulnerability in Jenkins Pipeline restFul API Plugin 0.11 and earlier allows attackers to connect to an attacker-specified URL, capturing a newly generated JCLI token.	2023-07-12	8.8	High
CVE-2023-37958	jenkins - sumologic_publisher	A cross-site request forgery (CSRF) vulnerability in Jenkins Sumologic Publisher Plugin 2.2.1 and earlier allows attackers to connect to an attacker-specified URL.	2023-07-12	8.8	High
CVE-2023-37961	jenkins - assembla	A cross-site request forgery (CSRF) vulnerability in Jenkins Assembla Auth Plugin 1.14 and earlier allows attackers to trick users into logging in to the attacker's account.	2023-07-12	8.8	High
CVE-2023-37962	jenkins - benchmark_evaluator	A cross-site request forgery (CSRF) vulnerability in Jenkins Benchmark Evaluator Plugin 1.0.1 and earlier allows attackers to connect to an attacker-specified URL and to check for the existence of directories, `.csv`, and `.ycsb` files on the Jenkins controller file system.	2023-07-12	8.8	High
CVE-2023-37964	jenkins - elasticbox_ci	A cross-site request forgery (CSRF) vulnerability in Jenkins ElasticBox CI Plugin 5.0.1 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2023-07-12	8.8	High
CVE-2023-34126	sonicwall - multiple products	Vulnerability in SonicWall GMS and Analytics allows an authenticated attacker to upload files on the underlying filesystem with root privileges. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	2023-07-13	8.8	High
CVE-2023-34127	sonicwall - multiple products	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in SonicWall GMS, SonicWall Analytics enables an authenticated attacker to execute arbitrary code with root privileges. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	2023-07-13	8.8	High
CVE-2023-34129	sonicwall - multiple products	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in SonicWall GMS and Analytics allows an authenticated remote attacker to traverse the directory and extract arbitrary files using Zip Slip method to any location on the underlying filesystem with root privileges. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	2023-07-13	8.8	High

CVE-2023-35335	microsoft - multiple products	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2023-07-11	8.2	High
CVE-2023-32250	linux - linux_kernel	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_SESSION_SETUP commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel.	2023-07-10	8.1	High
CVE-2023-32254	linux - linux_kernel	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_TREE_DISCONNECT commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel.	2023-07-10	8.1	High
CVE-2023-33989	sap - multiple products	An attacker with non-administrative authorizations in SAP NetWeaver (BI CONT ADD ON) - versions 707, 737, 747, 757, can exploit a directory traversal flaw to over-write system files. Data from confidential files cannot be read but potentially some OS files can be over-written leading to system compromise.	2023-07-11	8.1	High
CVE-2023-33127	microsoft - multiple products	.NET and Visual Studio Elevation of Privilege Vulnerability	2023-07-11	8.1	High
CVE-2023-33170	microsoft - multiple products	ASP.NET and Visual Studio Security Feature Bypass Vulnerability	2023-07-11	8.1	High
CVE-2023-30428	apache - multiple products	Incorrect Authorization vulnerability in Apache Software Foundation Apache Pulsar Broker's Rest Producer allows authenticated user with a custom HTTP header to produce a message to any topic using the broker's admin role. This issue affects Apache Pulsar Brokers: from 2.9.0 through 2.9.5, from 2.10.0 before 2.10.4, 2.11.0. The vulnerability is exploitable when an attacker can connect directly to the Pulsar Broker. If an attacker is connecting through the Pulsar Proxy, there is no known way to exploit this authorization vulnerability. There are two known risks for affected users. First, an attacker could produce garbage messages to any topic in the cluster. Second, an attacker could produce messages to the topic level policies topic for other tenants and influence topic settings that could lead to exfiltration and/or deletion of messages for other tenants. 2.8 Pulsar Broker users and earlier are unaffected. 2.9 Pulsar Broker users should upgrade to one of the patched versions. 2.10 Pulsar Broker users should upgrade to at least 2.10.4. 2.11 Pulsar Broker users should upgrade to at least 2.11.1. 3.0 Pulsar Broker users are unaffected.	2023-07-12	8.1	High
CVE-2023-27558	ibm - multiple products	IBM Db2 on Windows 10.5, 11.1, and 11.5 may be vulnerable to a privilege escalation caused by at least one installed service using an unquoted service path. A local attacker could exploit this vulnerability to gain elevated privileges by inserting an executable file in the path of the affected service. IBM X-Force ID: 249194.	2023-07-10	7.8	High
CVE-2023-28958	ibm - watson_knowledge_catalog_on_cloud_pak_for_data	IBM Watson Knowledge Catalog on Cloud Pak for Data 4.0 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 251782.	2023-07-10	7.8	High
CVE-2023-30431	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 db2set is vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow the buffer and execute arbitrary code. IBM X-Force ID: 252184.	2023-07-10	7.8	High
CVE-2023-37246	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PRT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21109)	2023-07-11	7.8	High
CVE-2023-37247	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21138)	2023-07-11	7.8	High
CVE-2023-37248	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an	2023-07-11	7.8	High

		attacker to execute code in the context of the current process. (ZDI-CAN-21155)			
CVE-2023-37374	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application is vulnerable to stack-based buffer overflow while parsing specially crafted STP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21054)	2023-07-11	7.8	High
CVE-2023-37375	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application is vulnerable to stack-based buffer overflow while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21060)	2023-07-11	7.8	High
CVE-2023-37376	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains a type confusion vulnerability while parsing STP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21051)	2023-07-11	7.8	High
CVE-2023-3269	linux - linux_kernel	A vulnerability exists in the memory management subsystem of the Linux kernel. The lock handling for accessing and updating virtual memory areas (VMAs) is incorrect, leading to use-after-free problems. This issue can be successfully exploited to execute arbitrary kernel code, escalate containers, and gain root privileges.	2023-07-11	7.8	High
CVE-2023-21756	microsoft - multiple products	Windows Win32k Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-32046	microsoft - multiple products	Windows MSHTML Platform Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-32047	microsoft - paint_3d	Paint 3D Remote Code Execution Vulnerability	2023-07-11	7.8	High
CVE-2023-32051	microsoft - raw_image_extension	Raw Image Extension Remote Code Execution Vulnerability	2023-07-11	7.8	High
CVE-2023-32053	microsoft - multiple products	Windows Installer Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-33148	microsoft - multiple products	Microsoft Office Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-33149	microsoft - multiple products	Microsoft Office Graphics Remote Code Execution Vulnerability	2023-07-11	7.8	High
CVE-2023-33152	microsoft - multiple products	Microsoft ActiveX Remote Code Execution Vulnerability	2023-07-11	7.8	High
CVE-2023-33155	microsoft - multiple products	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-33158	microsoft - multiple products	Microsoft Excel Remote Code Execution Vulnerability	2023-07-11	7.8	High
CVE-2023-33161	microsoft - multiple products	Microsoft Excel Remote Code Execution Vulnerability	2023-07-11	7.8	High
CVE-2023-34118	zoom - rooms	Improper privilege management in Zoom Rooms for Windows before version 5.14.5 may allow an authenticated user to enable an escalation of privilege via local access.	2023-07-11	7.8	High
CVE-2023-34119	zoom - rooms	Insecure temporary file in the installer for Zoom Rooms for Windows before version 5.15.0 may allow an authenticated user to enable an escalation of privilege via local access.	2023-07-11	7.8	High
CVE-2023-35299	microsoft - multiple products	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35304	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35305	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35312	microsoft - multiple products	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35313	microsoft - multiple products	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability	2023-07-11	7.8	High
CVE-2023-35317	microsoft - multiple products	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35320	microsoft - multiple products	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35323	microsoft - multiple products	Windows OLE Remote Code Execution Vulnerability	2023-07-11	7.8	High
CVE-2023-35328	microsoft - multiple products	Windows Transaction Manager Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35337	microsoft - multiple products	Win32k Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35340	microsoft - multiple products	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35342	microsoft - multiple products	Windows Image Acquisition Elevation of Privilege Vulnerability	2023-07-11	7.8	High

CVE-2023-35343	microsoft - multiple products	Windows Geolocation Service Remote Code Execution Vulnerability	2023-07-11	7.8	High
CVE-2023-35353	microsoft - multiple products	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35356	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35357	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35358	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35362	microsoft - multiple products	Windows Clip Service Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35363	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-35374	microsoft - paint_3d	Paint 3D Remote Code Execution Vulnerability	2023-07-11	7.8	High
CVE-2023-36536	zoom - rooms	Untrusted search path in the installer for Zoom Rooms for Windows before version 5.15.0 may allow an authenticated user to enable an escalation of privilege via local access.	2023-07-11	7.8	High
CVE-2023-36537	zoom - rooms	Improper privilege management in Zoom Rooms for Windows before version 5.14.5 may allow an authenticated user to enable an escalation of privilege via local access.	2023-07-11	7.8	High
CVE-2023-36538	zoom - rooms	Improper access control in Zoom Rooms for Windows before version 5.15.0 may allow an authenticated user to enable an escalation of privilege via local access.	2023-07-11	7.8	High
CVE-2023-36874	microsoft - multiple products	Windows Error Reporting Service Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-24491	citrix - secure_access_client	A vulnerability has been discovered in the Citrix Secure Access client for Windows which, if exploited, could allow an attacker with access to an endpoint with Standard User Account that has the vulnerable client installed to escalate their local privileges to that of NT AUTHORITY\SYSTEM.	2023-07-11	7.8	High
CVE-2023-29414	schneider-electric - accutech_manager	A CWE-120: Buffer Copy without Checking Size of Input (Classic Buffer Overflow) vulnerability exists that could cause user privilege escalation if a local user sends specific string input to a local function call.	2023-07-12	7.8	High
CVE-2023-30916	google - multiple products	In DMService, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-07-12	7.8	High
CVE-2023-30917	google - multiple products	In DMService, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-07-12	7.8	High
CVE-2023-30928	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-07-12	7.8	High
CVE-2023-30929	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-07-12	7.8	High
CVE-2023-3106	linux - multiple products	A NULL pointer dereference vulnerability was found in netlink_dump. This issue can occur when the Netlink socket receives the message(sendmsg) for the XFRM_MSG_GETSA, XFRM_MSG_GETPOLICY type message, and the DUMP flag is set and can cause a denial of service or possibly another unspecified impact. Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although it is unlikely.	2023-07-12	7.8	High
CVE-2021-43757	adobe - multiple products	Adobe Media Encoder versions 22.0, 15.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious 3GP ?file	2023-07-12	7.8	High
CVE-2023-29308	adobe - multiple products	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	7.8	High
CVE-2023-21257	google - android	In updateSettingsInternalLI of InstallPackageHelper.java, there is a possible way to sideload an app in the work profile due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-07-13	7.8	High

CVE-2023-21399	google - android	there is a possible way to bypass cryptographic assurances 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.	2023-07-13	7.8	High
CVE-2023-27540	ibm - multiple products	IBM Watson CP4D Data Stores 4.6.0 does not properly allocate resources without limits or throttling which could allow a remote attacker with information specific to the system to cause a denial of service. IBM X-Force ID: 248924.	2023-07-10	7.5	High
CVE-2023-30442	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 federated server is vulnerable to a denial of service as the server may crash when using a specially crafted wrapper using certain options. IBM X-Force ID: 253202.	2023-07-10	7.5	High
CVE-2023-30445	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253357.	2023-07-10	7.5	High
CVE-2023-30446	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253361 .	2023-07-10	7.5	High
CVE-2023-30447	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253436.	2023-07-10	7.5	High
CVE-2023-30448	ibm - multiple products	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253437.	2023-07-10	7.5	High
CVE-2023-30449	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 253439.	2023-07-10	7.5	High
CVE-2023-24487	citrix - multiple products	Arbitrary file read in Citrix ADC and Citrix Gateway?	2023-07-10	7.5	High
CVE-2023-36917	sap - multiple products	SAP BusinessObjects Business Intelligence Platform - version 420, 430, allows an unauthorized attacker who had hijacked a user session, to be able to bypass the victim's old password via brute force, due to unrestricted rate limit for password change functionality. Although the attack has no impact on integrity loss or system availability, this could lead to an attacker to completely takeover a victim's account.	2023-07-11	7.5	High
CVE-2022-31810	siemens - sipass_integrated	A vulnerability has been identified in SiPass integrated (All versions < V2.90.3.8). Affected server applications improperly check the size of data packets received for the configuration client login, causing a stack-based buffer overflow. This could allow an unauthenticated remote attacker to crash the server application, creating a denial of service condition.	2023-07-11	7.5	High
CVE-2023-35920	siemens - simatic_mv540_h_firmware	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3.4), SIMATIC MV540 S (All versions < V3.3.4), SIMATIC MV550 H (All versions < V3.3.4), SIMATIC MV550 S (All versions < V3.3.4), SIMATIC MV560 U (All versions < V3.3.4), SIMATIC MV560 X (All versions < V3.3.4). Affected devices cannot properly process specially crafted IP packets sent to the devices. This could allow an unauthenticated remote attacker to cause a denial of service condition. The affected devices must be restarted manually.	2023-07-11	7.5	High
CVE-2023-35921	siemens - simatic_mv540_h_firmware	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3.4), SIMATIC MV540 S (All versions < V3.3.4), SIMATIC MV550 H (All versions < V3.3.4), SIMATIC MV550 S (All versions < V3.3.4), SIMATIC MV560 U (All versions < V3.3.4), SIMATIC MV560 X (All versions < V3.3.4). Affected devices cannot properly process specially crafted Ethernet frames sent to the devices. This could allow an unauthenticated remote attacker to cause a denial of service condition. The affected devices must be restarted manually.	2023-07-11	7.5	High
CVE-2023-36521	siemens - simatic_mv540_h_firmware	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3.4), SIMATIC MV540 S (All versions < V3.3.4), SIMATIC MV550 H (All versions < V3.3.4), SIMATIC MV550 S (All versions < V3.3.4), SIMATIC MV560 U (All versions < V3.3.4), SIMATIC MV560 X (All versions < V3.3.4). The result synchronization server of the affected products contains a vulnerability that may lead to a denial of service condition. An attacker may	2023-07-11	7.5	High

		cause a denial of service situation of all socket-based communication of the affected products if the result server is enabled.			
CVE-2022-23447	fortinet - multiple products	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability [CWE-22] in FortiExtender management interface 7.0.0 through 7.0.3, 4.2.0 through 4.2.4, 4.1.1 through 4.1.8, 4.0.0 through 4.0.2, 3.3.0 through 3.3.2, 3.2.1 through 3.2.3, 5.3 all versions may allow an unauthenticated and remote attacker to retrieve arbitrary files from the underlying filesystem via specially crafted web requests.	2023-07-11	7.5	High
CVE-2023-32034	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-32035	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-32042	microsoft - multiple products	OLE Automation Information Disclosure Vulnerability	2023-07-11	7.5	High
CVE-2023-32044	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-32045	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-32084	microsoft - multiple products	HTTP.sys Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-33163	microsoft - multiple products	Windows Network Load Balancing Remote Code Execution Vulnerability	2023-07-11	7.5	High
CVE-2023-33165	microsoft - multiple products	Microsoft SharePoint Server Security Feature Bypass Vulnerability	2023-07-11	7.5	High
CVE-2023-33166	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-33167	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-33168	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-33169	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-33172	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-33173	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-35297	microsoft - multiple products	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	2023-07-11	7.5	High
CVE-2023-35298	microsoft - multiple products	HTTP.sys Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-35309	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-07-11	7.5	High
CVE-2023-35325	microsoft - multiple products	Windows Print Spooler Information Disclosure Vulnerability	2023-07-11	7.5	High
CVE-2023-35330	microsoft - multiple products	Windows Extended Negotiation Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-35333	microsoft - pandocupload	MediaWiki PandocUpload Extension Remote Code Execution Vulnerability	2023-07-11	7.5	High
CVE-2023-35338	microsoft - multiple products	Windows Peer Name Resolution Protocol Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-35339	microsoft - multiple products	Windows CryptoAPI Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-35352	microsoft - multiple products	Windows Remote Desktop Security Feature Bypass Vulnerability	2023-07-11	7.5	High
CVE-2020-20021	mikrotik - routeros	An issue discovered in MikroTik Router v6.46.3 and earlier allows attacker to cause denial of service via misconfiguration in the SSH daemon.	2023-07-12	7.5	High
CVE-2023-29298	adobe - multiple products	Adobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction.	2023-07-12	7.5	High
CVE-2023-29301	adobe - multiple products	Adobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier) are affected by an Improper Restriction of Excessive Authentication Attempts vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to impact the confidentiality of the user. Exploitation of this issue does not require user interaction.	2023-07-12	7.5	High
CVE-2023-35694	google - android	In DMPixelLogger_ProcessDmCommand of DMPixelLogger.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-07-13	7.5	High

CVE-2023-35874	sap - multiple products	SAP NetWeaver Application Server ABAP and ABAP Platform - version KRNL64NUC, 7.22, KRNL64NUC 7.22EXT, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53, KERNEL 7.22, KERNEL, 7.53, KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.92, KERNEL 7.93, under some conditions, performs improper authentication checks for functionalities that require user identity. An attacker can perform malicious actions over the network, extending the scope of impact, causing a limited impact on confidentiality, integrity and availability.	2023-07-11	7.4	High
CVE-2023-36749	siemens - ruggedcom_rox_mx5000_firmware	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The webserver of the affected devices support insecure TLS 1.0 protocol. An attacker could achieve a man-in-the-middle attack and compromise confidentiality and integrity of data.	2023-07-11	7.4	High
CVE-2023-21526	microsoft - multiple products	Windows Netlogon Information Disclosure Vulnerability	2023-07-11	7.4	High
CVE-2023-20185	cisco - multiple products	A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify intersite encrypted traffic. This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting intersite encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites. Cisco has not released and will not release software updates that address this vulnerability.	2023-07-12	7.4	High
CVE-2023-35870	sap - multiple products	When creating a journal entry template in SAP S/4HANA (Manage Journal Entry Template) - versions S4CORE 104, 105, 106, 107, an attacker could intercept the save request and change the template, leading to an impact on confidentiality and integrity of the resource. Furthermore, a standard template could be deleted, hence making the resource temporarily unavailable.	2023-07-11	7.3	High
CVE-2023-32054	microsoft - multiple products	Volume Shadow Copy Elevation of Privilege Vulnerability	2023-07-11	7.3	High
CVE-2023-36921	sap - solution_manager	SAP Solution Manager (Diagnostics agent) - version 7.20, allows an attacker to tamper with headers in a client request. This misleads SAP Diagnostics Agent to serve poisoned content to the server. On successful exploitation, the attacker can cause a limited impact on confidentiality and availability of the application.	2023-07-11	7.2	High
CVE-2023-36925	sap - solution_manager	SAP Solution Manager (Diagnostics agent) - version 7.20, allows an unauthenticated attacker to blindly execute HTTP requests. On successful exploitation, the attacker can cause a limited impact on confidentiality and availability of the application and other applications the Diagnostics Agent can reach.	2023-07-11	7.2	High
CVE-2023-23777	fortinet - multiple products	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.18 and below may allow a privileged attacker to execute arbitrary bash commands via crafted cli backup parameters.	2023-07-11	7.2	High
CVE-2023-36750	siemens - ruggedcom_rox_mx5000_firmware	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The software-upgrade Url parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	2023-07-11	7.2	High

CVE-2023-36751	siemens - ruggedcom_rox_mx5000_firmware	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The install-app URL parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	2023-07-11	7.2	High
CVE-2023-36752	siemens - ruggedcom_rox_mx5000_firmware	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The upgrade-app URL parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	2023-07-11	7.2	High
CVE-2023-36753	siemens - ruggedcom_rox_mx5000_firmware	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The uninstall-app App-name parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	2023-07-11	7.2	High
CVE-2023-36754	siemens - ruggedcom_rox_mx5000_firmware	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The SCEP server configuration URL parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	2023-07-11	7.2	High
CVE-2023-36755	siemens - ruggedcom_rox_mx5000_firmware	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The SCEP CA Certificate Name parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	2023-07-11	7.2	High
CVE-2023-32033	microsoft - multiple products	Microsoft Failover Cluster Remote Code Execution Vulnerability	2023-07-11	7.2	High
CVE-2023-35350	microsoft - multiple products	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability	2023-07-11	7.2	High
CVE-2023-37198	schneider-electric - struxureware_data_center_expert	A CWE-94: Improper Control of Generation of Code ('Code	2023-07-12	7.2	High

		Injection') vulnerability exists that could cause remote code execution when an admin user on DCE uploads or tampers with install packages.			
CVE-2023-37199	schneider-electric - struxureware_data _center_expert	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists that could cause remote code execution when an admin user on DCE tampers with backups which are then manually restored.	2023-07-12	7.2	High
CVE-2023-35691	google - android	there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with System execution privileges needed. User interaction is not needed for exploitation.	2023-07-13	7.2	High
CVE-2023-33990	sap - sql_anywhere	SAP SQL Anywhere - version 17.0, allows an attacker to prevent legitimate users from accessing the service by crashing the service. An attacker with low privileged account and access to the local system can write into the shared memory objects. This can be leveraged by an attacker to perform a Denial of Service. Further, an attacker might be able to modify sensitive data in shared memory objects.This issue only affects SAP SQL Anywhere on Windows. Other platforms are not impacted.	2023-07-11	7.1	High
CVE-2023-35347	microsoft - multiple products	Microsoft Install Service Elevation of Privilege Vulnerability	2023-07-11	7.1	High
CVE-2023-37949	jenkins - orka_by_macstadiu m	A missing permission check in Jenkins Orka by MacStadium Plugin 1.33 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2023-07-12	7.1	High
CVE-2023-37965	jenkins - elasticbox_ci	A missing permission check in Jenkins ElasticBox CI Plugin 5.0.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2023-07-12	7.1	High
CVE-2023-32050	microsoft - multiple products	Windows Installer Elevation of Privilege Vulnerability	2023-07-11	7	High
CVE-2023-33156	microsoft - malware_protectio n_engine	Microsoft Defender Elevation of Privilege Vulnerability	2023-07-11	7	High
CVE-2023-35360	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7	High
CVE-2023-35361	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7	High
CVE-2023-36748	siemens - ruggedcom_rox_m x5000_firmware	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The affected devices are configured to offer weak ciphers by default. This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over to and from the affected device.	2023-07-11	6.8	Medium
CVE-2023-29347	microsoft - windows_admin_ce nter	Windows Admin Center Spoofing Vulnerability	2023-07-11	6.8	Medium
CVE-2023-32043	microsoft - multiple products	Windows Remote Desktop Security Feature Bypass Vulnerability	2023-07-11	6.8	Medium
CVE-2023-35332	microsoft - multiple products	Windows Remote Desktop Protocol Security Feature Bypass	2023-07-11	6.8	Medium
CVE-2023-32055	microsoft - multiple products	Active Template Library Elevation of Privilege Vulnerability	2023-07-11	6.7	Medium
CVE-2023-21400	google - android	In multiple functions of io_uring.c, there is a possible kernel memory corruption due to improper locking. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.	2023-07-13	6.7	Medium
CVE-2023-35693	google - android	In incfs_kill_sb of fs/incfs/vfs.c, there is a possible memory corruption due to a use after free. This could lead to local	2023-07-13	6.7	Medium

		escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.			
CVE-2023-35310	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	2023-07-11	6.6	Medium
CVE-2023-35344	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	2023-07-11	6.6	Medium
CVE-2023-35345	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	2023-07-11	6.6	Medium
CVE-2023-35346	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	2023-07-11	6.6	Medium
CVE-2023-35351	microsoft - multiple products	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability	2023-07-11	6.6	Medium
CVE-2023-28955	ibm - watson_knowledge_catalog_on_cloud_pak_for_data	IBM Watson Knowledge Catalog on Cloud Pak for Data 4.0 could allow an authenticated user send a specially crafted request that could cause a denial of service. IBM X-Force ID: 251704.	2023-07-10	6.5	Medium
CVE-2023-29256	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to an information disclosure due to improper privilege management when certain federation features are used. IBM X-Force ID: 252046.	2023-07-10	6.5	Medium
CVE-2023-33992	sap - multiple products	The SAP BW BICS communication layer in SAP Business Warehouse and SAP BW/4HANA - version SAP_BW 730, SAP_BW 731, SAP_BW 740, SAP_BW 730, SAP_BW 750, DW4CORE 100, DW4CORE 200, DW4CORE 300, may expose unauthorized cell values to the data response. To be able to exploit this, the user still needs authorizations on the query as well as on the keyfigure/measure level. The missing check only affects the data level.	2023-07-11	6.5	Medium
CVE-2023-35872	sap - netweaver_process_integration	The Message Display Tool (MDT) of SAP NetWeaver Process Integration - version SAP_XIAF 7.50, does not perform authentication checks for certain functionalities that require user identity. An unauthenticated user might access technical data about the product status and its configuration. The vulnerability does not allow access to sensitive information or administrative functionalities. On successful exploitation an attacker can cause limited impact on confidentiality and availability of the application.	2023-07-11	6.5	Medium
CVE-2023-35873	sap - netweaver_process_integration	The Runtime Workbench (RWB) of SAP NetWeaver Process Integration - version SAP_XITOOL 7.50, does not perform authentication checks for certain functionalities that require user identity. An unauthenticated user might access technical data about the product status and its configuration. The vulnerability does not allow access to sensitive information or administrative functionalities. On successful exploitation an attacker can cause limited impact on confidentiality and availability of the application.	2023-07-11	6.5	Medium
CVE-2023-24881	microsoft - teams	Microsoft Teams Information Disclosure Vulnerability	2023-07-11	6.5	Medium
CVE-2023-25606	fortinet - multiple products	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability [CWE-23] in FortiAnalyzer and FortiManager management interface 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4 all versions may allow a remote and authenticated attacker to retrieve arbitrary files from the underlying filesystem via specially crafted web requests.	2023-07-11	6.5	Medium
CVE-2023-32037	microsoft - multiple products	Windows Layer-2 Bridge Network Driver Information Disclosure Vulnerability	2023-07-11	6.5	Medium
CVE-2023-33151	microsoft - multiple products	Microsoft Outlook Spoofing Vulnerability	2023-07-11	6.5	Medium
CVE-2023-33164	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	6.5	Medium
CVE-2023-35296	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	2023-07-11	6.5	Medium
CVE-2023-35308	microsoft - multiple products	Windows MSHTML Platform Security Feature Bypass Vulnerability	2023-07-11	6.5	Medium
CVE-2023-35314	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	6.5	Medium
CVE-2023-35316	microsoft - multiple products	Remote Procedure Call Runtime Information Disclosure Vulnerability	2023-07-11	6.5	Medium
CVE-2023-35318	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	6.5	Medium
CVE-2023-35319	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	6.5	Medium
CVE-2023-35321	microsoft - multiple products	Windows Deployment Services Denial of Service Vulnerability	2023-07-11	6.5	Medium
CVE-2023-35329	microsoft - multiple products	Windows Authentication Denial of Service Vulnerability	2023-07-11	6.5	Medium
CVE-2023-35331	microsoft - multiple products	Windows Local Security Authority (LSA) Denial of Service Vulnerability	2023-07-11	6.5	Medium
CVE-2023-35348	microsoft - multiple products	Active Directory Federation Service Security Feature Bypass Vulnerability	2023-07-11	6.5	Medium
CVE-2023-36868	microsoft - multiple products	Azure Service Fabric on Windows Information Disclosure Vulnerability	2023-07-11	6.5	Medium

CVE-2023-36871	microsoft - multiple products	Azure Active Directory Security Feature Bypass Vulnerability	2023-07-11	6.5	Medium
CVE-2022-46651	apache - airflow	Apache Airflow, versions before 2.6.3, is affected by a vulnerability that allows an unauthorized actor to gain access to sensitive information in Connection edit view. This vulnerability is considered low since it requires someone with access to Connection resources specifically updating the connection to exploit it. Users should upgrade to version 2.6.3 or later which has removed the vulnerability.	2023-07-12	6.5	Medium
CVE-2023-22887	apache - airflow	Apache Airflow, versions before 2.6.3, is affected by a vulnerability that allows an attacker to perform unauthorized file access outside the intended directory structure by manipulating the run_id parameter. This vulnerability is considered low since it requires an authenticated user to exploit it. It is recommended to upgrade to a version that is not affected	2023-07-12	6.5	Medium
CVE-2023-22888	apache - airflow	Apache Airflow, versions before 2.6.3, is affected by a vulnerability that allows an attacker to cause a service disruption by manipulating the run_id parameter. This vulnerability is considered low since it requires an authenticated user to exploit it. It is recommended to upgrade to a version that is not affected	2023-07-12	6.5	Medium
CVE-2023-31007	apache - multiple products	Improper Authentication vulnerability in Apache Software Foundation Apache Pulsar Broker allows a client to stay connected to a broker after authentication data expires if the client connected through the Pulsar Proxy when the broker is configured with authenticateOriginalAuthData=false or if a client connects directly to a broker with a specially crafted connect command when the broker is configured with authenticateOriginalAuthData=false. This issue affects Apache Pulsar: through 2.9.4, from 2.10.0 through 2.10.3, 2.11.0. 2.9 Pulsar Broker users should upgrade to at least 2.9.5. 2.10 Pulsar Broker users should upgrade to at least 2.10.4. 2.11 Pulsar Broker users should upgrade to at least 2.11.1. 3.0 Pulsar Broker users are unaffected. Any users running the Pulsar Broker for 2.8.* and earlier should upgrade to one of the above patched versions.	2023-07-12	6.5	Medium
CVE-2023-35908	apache - airflow	Apache Airflow, versions before 2.6.3, is affected by a vulnerability that allows unauthorized read access to a DAG through the URL. It is recommended to upgrade to a version that is not affected	2023-07-12	6.5	Medium
CVE-2023-36543	apache - airflow	Apache Airflow, versions before 2.6.3, has a vulnerability where an authenticated user can use crafted input to make the current request hang. It is recommended to upgrade to a version that is not affected	2023-07-12	6.5	Medium
CVE-2023-37579	apache - multiple products	Incorrect Authorization vulnerability in Apache Software Foundation Apache Pulsar Function Worker. This issue affects Apache Pulsar: before 2.10.4, and 2.11.0. Any authenticated user can retrieve a source's configuration or a sink's configuration without authorization. Many sources and sinks contain credentials in the configuration, which could lead to leaked credentials. This vulnerability is mitigated by the fact that there is not a known way for an authenticated user to enumerate another tenant's sources or sinks, meaning the source or sink name would need to be guessed in order to exploit this vulnerability. The recommended mitigation for impacted users is to upgrade the Pulsar Function Worker to a patched version. 2.10 Pulsar Function Worker users should upgrade to at least 2.10.4. 2.11 Pulsar Function Worker users should upgrade to at least 2.11.1. 3.0 Pulsar Function Worker users are unaffected. Any users running the Pulsar Function Worker for 2.9.* and earlier should upgrade to one of the above patched versions.	2023-07-12	6.5	Medium
CVE-2023-37456	mozilla - firefox	The session restore helper crashed whenever there was no parameter sent to the message handler. This vulnerability affects Firefox for iOS < 115.	2023-07-12	6.5	Medium
CVE-2023-37942	jenkins - external_monitor_job_type	Jenkins External Monitor Job Type Plugin 206.v9a_94ff0b_4a_10 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2023-07-12	6.5	Medium
CVE-2023-37944	jenkins - datadog	A missing permission check in Jenkins Datadog Plugin 5.4.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials	2023-07-12	6.5	Medium

		IDs obtained through another method, capturing credentials stored in Jenkins.			
CVE-2023-37951	jenkins - mabl	Jenkins mabl Plugin 0.0.46 and earlier does not set the appropriate context for credentials lookup, allowing attackers with Item/Configure permission to access and capture credentials they are not entitled to.	2023-07-12	6.5	Medium
CVE-2023-37952	jenkins - mabl	A cross-site request forgery (CSRF) vulnerability in Jenkins mabl Plugin 0.0.46 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2023-07-12	6.5	Medium
CVE-2023-37953	jenkins - mabl	A missing permission check in Jenkins mabl Plugin 0.0.46 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2023-07-12	6.5	Medium
CVE-2023-37955	jenkins - test_results_aggregator	A cross-site request forgery (CSRF) vulnerability in Jenkins Test Results Aggregator Plugin 1.2.13 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials.	2023-07-12	6.5	Medium
CVE-2023-37956	jenkins - test_results_aggregator	A missing permission check in Jenkins Test Results Aggregator Plugin 1.2.13 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials.	2023-07-12	6.5	Medium
CVE-2023-37959	jenkins - sumologic_publisher	A missing permission check in Jenkins Sumologic Publisher Plugin 2.2.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL.	2023-07-12	6.5	Medium
CVE-2023-37960	jenkins - mathworks_polyspace	Jenkins MathWorks Polyspace Plugin 1.0.5 and earlier allows attackers with Item/Configure permission to send emails with arbitrary files from the Jenkins controller file systems.	2023-07-12	6.5	Medium
CVE-2023-34125	sonicwall - multiple products	Path Traversal vulnerability in GMS and Analytics allows an authenticated attacker to read arbitrary files from the underlying filesystem with root privileges. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	2023-07-13	6.5	Medium
CVE-2023-34135	sonicwall - multiple products	Path Traversal vulnerability in SonicWall GMS and Analytics allows a remote authenticated attacker to read arbitrary files from the underlying file system via web service. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	2023-07-13	6.5	Medium
CVE-2023-24488	citrix - multiple products	Cross site scripting vulnerability in Citrix ADC and Citrix Gateway? in allows and attacker to perform cross site scripting	2023-07-10	6.1	Medium
CVE-2023-33988	sap - enable_now	In SAP Enable Now - versions WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704, the Content-Security-Policy and X-XSS-Protection response headers are not implemented, allowing an unauthenticated attacker to attempt reflected cross-site scripting, which could result in disclosure or modification of information.	2023-07-11	6.1	Medium
CVE-2023-36918	sap - enable_now	In SAP Enable Now - versions WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704, the X-Content-Type-Options response header is not implemented, allowing an unauthenticated attacker to trigger MIME type sniffing, which leads to Cross-Site Scripting, which could result in disclosure or modification of information.	2023-07-11	6.1	Medium
CVE-2023-36386	siemens - ruggedcom_rox_mx5000_firmware	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). 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. The value is reflected in the response without sanitization while throwing an “invalid params element name” error on the get_elements parameters.	2023-07-11	6.1	Medium
CVE-2023-36389	siemens - ruggedcom_rox_mx5000_firmware	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0),	2023-07-11	6.1	Medium

		RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). 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. The malformed value is reflected directly in the response without sanitization while throwing an “invalid path” error.			
CVE-2023-36390	siemens - ruggedcom_rox_mx5000_firmware	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). 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. The value is reflected in the response without sanitization while throwing an “invalid params element name” error on the action parameters.	2023-07-11	6.1	Medium
CVE-2023-33171	microsoft - multiple products	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2023-07-11	6.1	Medium
CVE-2023-37947	jenkins - openshift_login	Jenkins OpenShift Login Plugin 1.1.0.227.v27e08dfb_1a_20 and earlier improperly determines that a redirect URL after login is legitimately pointing to Jenkins, allowing attackers to perform phishing attacks.	2023-07-12	6.1	Medium
CVE-2023-29455	zabbix - multiple products	Reflected XSS attacks, also known as non-persistent attacks, occur when a malicious script is reflected off a web application to the victim's browser. The script is activated through a link, which sends a request to a website with a vulnerability that enables execution of malicious scripts.	2023-07-13	6.1	Medium
CVE-2023-29457	zabbix - multiple products	Reflected XSS attacks, occur when a malicious script is reflected off a web application to the victim's browser. The script can be activated through Action form fields, which can be sent as request to a website with a vulnerability that enables execution of malicious scripts.	2023-07-13	6.1	Medium
CVE-2023-20210	cisco - multiple products	A vulnerability in Cisco BroadWorks could allow an authenticated, local attacker to elevate privileges to the root user on an affected device. The vulnerability is due to insufficient input validation by the operating system CLI. An attacker could exploit this vulnerability by issuing a crafted command to the affected system. A successful exploit could allow the attacker to execute commands as the root user. To exploit this vulnerability, an attacker must have valid BroadWorks administrative privileges on the affected device.	2023-07-12	6	Medium
CVE-2023-37943	jenkins - active_directory	Jenkins Active Directory Plugin 2.30 and earlier ignores the "Require TLS" and "StartTls" options and always performs the connection test to Active directory unencrypted, allowing attackers able to capture network traffic between the Jenkins controller and Active Directory servers to obtain Active Directory credentials.	2023-07-12	5.9	Medium
CVE-2023-24486	citrix - workspace	A vulnerability has been identified in Citrix Workspace app for Linux that, if exploited, may result in a malicious local user being able to gain access to the Citrix Virtual Apps and Desktops session of another user who is using the same computer from which the ICA session is launched.	2023-07-10	5.5	Medium
CVE-2023-32039	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	2023-07-11	5.5	Medium
CVE-2023-32040	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	2023-07-11	5.5	Medium
CVE-2023-32041	microsoft - multiple products	Windows Update Orchestrator Service Information Disclosure Vulnerability	2023-07-11	5.5	Medium
CVE-2023-32085	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	2023-07-11	5.5	Medium
CVE-2023-33162	microsoft - multiple products	Microsoft Excel Information Disclosure Vulnerability	2023-07-11	5.5	Medium
CVE-2023-33174	microsoft - multiple products	Windows Cryptographic Information Disclosure Vulnerability	2023-07-11	5.5	Medium
CVE-2023-35306	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	2023-07-11	5.5	Medium

CVE-2023-35324	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	2023-07-11	5.5	Medium
CVE-2023-35326	microsoft - multiple products	Windows CDP User Components Information Disclosure Vulnerability	2023-07-11	5.5	Medium
CVE-2023-35341	microsoft - multiple products	Microsoft DirectMusic Information Disclosure Vulnerability	2023-07-11	5.5	Medium
CVE-2023-36872	microsoft - vp9_video_extensions	VP9 Video Extensions Information Disclosure Vulnerability	2023-07-11	5.5	Medium
CVE-2023-30913	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30918	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30919	google - multiple products	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30920	google - multiple products	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30921	google - multiple products	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30922	google - multiple products	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30923	google - multiple products	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30924	google - multiple products	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30925	google - multiple products	In opm service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30926	google - multiple products	In opm service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30927	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30930	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30931	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30932	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30933	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30934	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30935	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30936	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30937	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30938	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30939	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30940	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-30941	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium

CVE-2023-30942	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-32788	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-32789	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33881	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33882	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33883	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33884	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33885	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33886	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33887	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33888	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33889	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33890	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33891	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33892	google - multiple products	In fastDial service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33893	google - multiple products	In fastDial service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33894	google - multiple products	In fastDial service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33895	google - multiple products	In fastDial service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33899	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33900	google - multiple products	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33901	google - multiple products	In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2023-33902	google - multiple products	In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
CVE-2021-43758	adobe - multiple products	Adobe Media Encoder versions 22.0, 15.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious MP4 file.	2023-07-12	5.5	Medium
CVE-2021-43759	adobe - multiple products	Adobe Media Encoder versions 22.0, 15.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious MP4 file.	2023-07-12	5.5	Medium

CVE-2021-43760	adobe - multiple products	Adobe Media Encoder versions 22.0, 15.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious MOV file.	2023-07-12	5.5	Medium
CVE-2021-44696	adobe - prelude	Adobe Prelude version 22.1.1 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious JPEG file.	2023-07-12	5.5	Medium
CVE-2023-29309	adobe - multiple products	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	5.5	Medium
CVE-2023-29310	adobe - multiple products	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	5.5	Medium
CVE-2023-29311	adobe - multiple products	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	5.5	Medium
CVE-2023-29312	adobe - multiple products	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	5.5	Medium
CVE-2023-29313	adobe - multiple products	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	5.5	Medium
CVE-2023-29314	adobe - multiple products	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	5.5	Medium
CVE-2023-29315	adobe - multiple products	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	5.5	Medium
CVE-2023-29316	adobe - multiple products	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	5.5	Medium
CVE-2023-29317	adobe - multiple products	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	5.5	Medium
CVE-2023-29318	adobe - multiple products	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	5.5	Medium
CVE-2023-29319	adobe - multiple products	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	5.5	Medium

CVE-2021-0948	google - android	The PVRSRVBridgeGetMultiCoreInfo ioctl in the PowerVR kernel driver can return uninitialized kernel memory to user space. The contents of this memory could contain sensitive information.	2023-07-13	5.5	Medium
CVE-2023-21260	google - multiple products	In notification access permission dialog box, malicious application can embedded a very long service label that overflow the original user prompt and possibly contains mis-leading information to be appeared as a system message for user confirmation.	2023-07-13	5.5	Medium
CVE-2023-32052	microsoft - power_apps	Microsoft Power Apps (online) Spoofing Vulnerability	2023-07-11	5.4	Medium
CVE-2023-35336	microsoft - multiple products	Windows MSHTML Platform Security Feature Bypass Vulnerability	2023-07-11	5.4	Medium
CVE-2023-37455	mozilla - firefox	The permission request prompt from the site in the background tab was overlaid on top of the site in the foreground tab. This vulnerability affects Firefox for iOS < 115.	2023-07-12	5.4	Medium
CVE-2023-37963	jenkins - benchmark_evaluator	A missing permission check in Jenkins Benchmark Evaluator Plugin 1.0.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL and to check for the existence of directories, `.csv`, and `.ycsb` files on the Jenkins controller file system.	2023-07-12	5.4	Medium
CVE-2023-29454	zabbix - multiple products	Stored or persistent cross-site scripting (XSS) is a type of XSS where the attacker first sends the payload to the web application, then the application saves the payload (e.g., in a database or server-side text files), and finally, the application unintentionally executes the payload for every victim visiting its web pages.	2023-07-13	5.4	Medium
CVE-2023-31405	sap - netweaver_application_server_for_java	SAP NetWeaver AS for Java - versions ENGINEAPI 7.50, SERVERCORE 7.50, J2EE-APPS 7.50, allows an unauthenticated attacker to craft a request over the network which can result in unwarranted modifications to a system log without user interaction. There is no ability to view any information or any effect on availability.	2023-07-11	5.3	Medium
CVE-2023-36919	sap - enable_now	In SAP Enable Now - versions WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704, the Referrer-Policy response header is not implemented, allowing an unauthenticated attacker to obtain referrer details, resulting in information disclosure.	2023-07-11	5.3	Medium
CVE-2022-29562	siemens - ruggedcom_rox_mx5000_firmware	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). Affected devices do not properly handle malformed HTTP packets. This could allow an unauthenticated remote attacker to send a malformed HTTP packet causing certain functions to fail in a controlled manner.	2023-07-11	5.3	Medium
CVE-2023-35373	microsoft - mono	Mono Authenticode Validation Spoofing Vulnerability	2023-07-11	5.3	Medium
CVE-2023-36924	sap - multiple products	While using a specific function, SAP ERP Defense Forces and Public Security - versions 600, 603, 604, 605, 616, 617, 618, 802, 803, 804, 805, 806, 807, allows an authenticated attacker with admin privileges to write arbitrary data to the syslog file. On successful exploitation, an attacker could modify all the syslog data causing a complete compromise of integrity of the application.	2023-07-11	4.9	Medium
CVE-2023-32083	microsoft - multiple products	Microsoft Failover Cluster Information Disclosure Vulnerability	2023-07-11	4.9	Medium
CVE-2023-38046	paloaltonetworks - multiple products	A vulnerability exists in Palo Alto Networks PAN-OS software that enables an authenticated administrator with the privilege to commit a specifically created configuration to read local files and resources from the system.	2023-07-12	4.9	Medium
CVE-2023-3108	linux - linux_kernel	A flaw was found in the subsequent get_user_pages_fast in the Linux kernel's interface for symmetric key cipher algorithms in the skcipher_recvmsg of crypto/algif_skcipher.c function. This flaw allows a local user to crash the system.	2023-07-11	4.7	Medium
CVE-2022-48450	google - multiple products	In bluetooth service, there is a possible missing params check. This could lead to local denial of service with System execution privileges needed.	2023-07-12	4.4	Medium
CVE-2023-33896	google - multiple products	In libimpl-ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-07-12	4.4	Medium
CVE-2023-33897	google - multiple products	In libimpl-ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-07-12	4.4	Medium
CVE-2023-33903	google - multiple products	In FM service, there is a possible missing params check. This could lead to local denial of service with System execution privileges needed.	2023-07-12	4.4	Medium

CVE-2023-33904	google - multiple products	In hci_server, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-07-12	4.4	Medium
CVE-2023-33905	google - multiple products	In iwnpi server, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-07-12	4.4	Medium
CVE-2023-23487	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to insufficient audit logging. IBM X-Force ID: 245918.	2023-07-10	4.3	Medium
CVE-2023-28953	ibm - cognos_analytics_cartridge_for_ibm_cloud_pak_for_data	IBM Cognos Analytics on Cloud Pak for Data 4.0 could allow an attacker to make system calls that might compromise the security of the containers due to misconfigured security context. IBM X-Force ID: 251465.	2023-07-10	4.3	Medium
CVE-2023-35887	apache - mina	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Software Foundation Apache MINA. In SFTP servers implemented using Apache MINA SSHD that use a RootedFileSystem, logged users may be able to discover "exists/does not exist" information about items outside the rooted tree via paths including parent navigation ("..") beyond the root, or involving symlinks. This issue affects Apache MINA: from 1.0 before 2.10. Users are recommended to upgrade to 2.10	2023-07-10	4.3	Medium
CVE-2023-24490	citrix - multiple products	Users with only access to launch VDA applications can launch an unauthorized desktop	2023-07-10	4.3	Medium
CVE-2023-37945	jenkins - saml_single_sign_on	A missing permission check in Jenkins SAML Single Sign On(SSO) Plugin 2.1.0 through 2.3.0 (both inclusive) allows attackers with Overall/Read permission to download a string representation of the current security realm.	2023-07-12	4.3	Medium
CVE-2023-37950	jenkins - mabl	A missing permission check in Jenkins mabl Plugin 0.0.46 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	2023-07-12	4.3	Medium
CVE-2023-37954	jenkins - rebuilder	A cross-site request forgery (CSRF) vulnerability in Jenkins Rebuilder Plugin 320.v5a_0933a_e7d61 and earlier allows attackers to rebuild a previous build.	2023-07-12	4.3	Medium
CVE-2022-48451	google - multiple products	In bluetooth service, there is a possible out of bounds write due to race condition. This could lead to local denial of service with System execution privileges needed.	2023-07-12	4.1	Medium
CVE-2023-37948	jenkins - cloud_infrastructure_compute	Jenkins Oracle Cloud Infrastructure Compute Plugin 1.0.16 and earlier does not validate SSH host keys when connecting OCI clouds, enabling man-in-the-middle attacks.	2023-07-12	3.7	Low
CVE-2023-34442	apache - multiple products	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Software Foundation Apache Camel.This issue affects Apache Camel: from 3.X through <=3.14.8, from 3.18.X through <=3.18.7, from 3.20.X through <= 3.20.5, from 4.X through <= 4.0.0-M3. Users should upgrade to 3.14.9, 3.18.8, 3.20.6 or 3.21.0 and for users on Camel 4.x update to 4.0.0-M1	2023-07-10	3.3	Low
CVE-2022-22302	fortinet - multiple products	A clear text storage of sensitive information (CWE-312) vulnerability in both FortiGate version 6.4.0 through 6.4.1, 6.2.0 through 6.2.9 and 6.0.0 through 6.0.13 and FortiAuthenticator version 5.5.0 and all versions of 6.1 and 6.0 may allow a local unauthorized party to retrieve the Fortinet private keys used to establish secure communication with both Apple Push Notification and Google Cloud Messaging services, via accessing the files on the filesystem.	2023-07-11	3.3	Low
CVE-2023-34117	zoom - zoom_software_development_kit	Relative path traversal in the Zoom Client SDK before version 5.15.0 may allow an unauthorized user to enable information disclosure via local access.	2023-07-11	3.3	Low
CVE-2023-33879	google - multiple products	In music service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	3.3	Low
CVE-2023-33880	google - multiple products	In music service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	3.3	Low
CVE-2023-21262	google - multiple products	In startInput of AudioPolicyInterfaceImpl.cpp, there is a possible way of erroneously displaying the microphone privacy indicator due to a race condition. This could lead to false user expectations. User interaction is needed for exploitation.	2023-07-13	3.1	Low

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.