

WHITE where information can be shared or published on any public forums.

مي ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء national interests, NCA provides the weekly summary of published السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة 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 Vulnerability.

- 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

severity:

- عالي جدًا: النتيجة الأساسية لـCVSS 9.0-10.0
 - · عالي: النتيجة الأساسية ل-8.9 CVSS
 - متوسط: النتيجة الأساسية لـCVSS 4.0-6.9
 - 🔹 منخفض: النتيجة الأساسية لـ CVSS 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
<u>CVE-2023-29130</u>	simatic_cn_4100	A vulnerability has been identified in SIMATIC CN 4100 (All	2023-07-11	10	Critical
<u>CVE-2023-29131</u>	siemens - simatic_cn_4100	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
<u>CVE-2023-24489</u>	citrix - sharefile_storage_z ones_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
	fortinet - multiple	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			
<u>CVE-2023-28001</u>	products		2023-07-11	9.8	Critical
	microsoft - multiple	Windows Server Update Service (WSUS) Elevation of Privilege	2022 07 11	0.0	Critical
<u>CVE-2023-32056</u>	products microsoft - multiple	Vulnerability	2023-07-11	9.8	Critical
CVE-2023-32057	products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-07-11	9.8	Critical
012 2020 02007	microsoft - multiple	Windows Partition Management Driver Elevation of Privilege	2020 07 22	5.0	entitedi
CVE-2023-33154	products	Vulnerability	2023-07-11	9.8	Critical
	microsoft - multiple	Windows Routing and Remote Access Service (RRAS) Remote Code			
CVE-2023-35365	products	Execution Vulnerability	2023-07-11	9.8	Critical
	microsoft - multiple	Windows Routing and Remote Access Service (RRAS) Remote Code			
<u>CVE-2023-35366</u>	products	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
<u>CVL-2023-33307</u>	products	The RocketMQ NameServer component still has a remote	2023-07-11	9.8	Critical
		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.			
<u>CVE-2023-37582</u>	apache - multiple products	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
	1.00000		***		

		The authentication mechanism in SonicWall GMS and Analytics			
		Web Services had insufficient checks, allowing authentication			
	sonicwall - multiple	bypass. This issue affects GMS: 9.3.2-SP1 and earlier versions;			
CVE-2023-34124	products	Analytics: 2.5.0.4-R7 and earlier versions.	2023-07-13	9.8	Critical
		Tomcat application credentials are hardcoded in SonicWall GMS			
CVE-2023-34128	sonicwall - multiple products	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
<u>CVL-2023-34128</u>	products	SonicWall GMS and Analytics use outdated Tiny Encryption	2023-07-13	9.8	Critical
		Algorithm (TEA) with a hardcoded key to encrypt sensitive data.			
	sonicwall - multiple	This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics:			
CVE-2023-34130	products	2.5.0.4-R7 and earlier versions.	2023-07-13	9.8	Critical
CVE 2022 221E0	microsoft - multiple	Microsoft Office Security Feature Dynacs Vulnershility	2023-07-11	0.6	Critical
<u>CVE-2023-33150</u>	products	Microsoft Office Security Feature Bypass Vulnerability An unauthenticated attacker in SAP Web Dispatcher - versions	2023-07-11	9.6	Critical
		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			
	sap - multiple	the back-end server executing a malicious payload which can be used to read or modify information on the server or make it			
CVE-2023-33987	products	temporarily unavailable.	2023-07-11	9.4	Critical
		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			
CVE-2023-35871	sap - multiple products	low impact on confidentiality and high impact on the integrity and availability of the system.	2023-07-11	9.4	Critical
<u>CVE-2023-53871</u>	products	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5,	2023-07-11	9.4	Cilicai
		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			
	ibm - multiple	clientRerouteServerListJNDIName, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force			
CVE-2023-27867	products	ID: 249514.	2023-07-10	8.8	High
		IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5,			0
		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,			
	ibm - multiple	an attacker could exploit this vulnerability to execute arbitrary			
CVE-2023-27868	products	code on the system. IBM X-Force ID: 249516.	2023-07-10	8.8	High
		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			
	ibm - multiple	vulnerability to execute arbitrary code on the system. IBM X-Force			
CVE-2023-27869	products	ID: 249517.	2023-07-10	8.8	High
		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)			
	sap - multiple	extension. On successful exploitation, the attacker can read or			
CVE-2023-36922	products	modify the system data as well as shut down the system.	2023-07-11	8.8	High
		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			
	siemens -	(All versions < V2.16.0). The web interface of the affected devices			
	ruggedcom_rox_m	are vulnerable to Cross-Site Request Forgery attacks. By tricking an			
CVE-2022-29561	x5000_firmware	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.			
		Improper input validation in the Zoom Desktop Client for Windows before version 5.15.0 may allow an unauthorized user to enable an			
CVE-2023-34116	zoom - zoom	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
	microsoft - multiple				
<u>CVE-2023-32049</u>	products microsoft - multiple	Windows SmartScreen Security Feature Bypass Vulnerability	2023-07-11	8.8	High
<u>CVE-2023-33134</u>	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
	microsoft - multiple				
<u>CVE-2023-33157</u>	products microsoft - multiple	Microsoft SharePoint Remote Code Execution Vulnerability	2023-07-11	8.8	High
CVE-2023-33159	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
	microsoft - multiple	Remote Procedure Call Runtime Remote Code Execution			
CVE-2023-35300	products microsoft - multiple	Vulnerability Microsoft PostScript and PCL6 Class Printer Driver Remote Code	2023-07-11	8.8	High
CVE-2023-35302	products	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
	microsoft - multiple				
<u>CVE-2023-35311</u>	products microsoft - multiple	Microsoft Outlook Security Feature Bypass Vulnerability Windows Layer-2 Bridge Network Driver Remote Code Execution	2023-07-11	8.8	High
<u>CVE-2023-35315</u>	products	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
	microsoft - multiple				
CVE-2023-35364	products	Windows Kernel Elevation of Privilege Vulnerability Microsoft is investigating reports of a series of remote code	2023-07-11	8.8	High
		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.			
	microsoft - multiple	This CVE will be updated with new information and links to			
<u>CVE-2023-36884</u>	products	security updates when they become available.	2023-07-11	8.8	High
		A vulnerability has been discovered in the Citrix Secure Access			
	citrix -	client for Ubuntu which, if exploited, could allow an attacker to			
CVE-2023-24492	secure_access_clie nt	remotely execute code if a victim user opens an attacker-crafted link and accepts further prompts.	2023-07-11	8.8	High
<u>CVL 2023 24452</u>			2023 07 11	0.0	111811
		A CWE-89: Improper Neutralization of Special Elements vulnerability used in an SQL Command			
		('SQL Injection') vulnerability exists that could allow a user already			
	schnolder electric	authenticated on DCE to			
	schneider-electric - struxureware_data	access unauthorized content, change, or delete content, or perform unauthorized actions when			
<u>CVE-2023-37196</u>	_center_expert	tampering with the alert settings of endpoints on DCE.	2023-07-12	8.8	High
		A CWE-89: Improper Neutralization of Special Elements vulnerability used in an SQL Command			
		('SQL Injection') vulnerability exists that could allow a user already			
	oobaalaa ahaa t	authenticated on DCE to			
	schneider-electric - struxureware_data	access unauthorized content, change, or delete content, or perform unauthorized actions when			
CVE-2023-37197	_center_expert	tampering with the mass configuration settings of endpoints on	2023-07-12	8.8	High

		DCE.			
		There is insufficient restrictions of called script functions in Apache			
		Jena			
		versions 4.8.0 and earlier. It allows a			
CVE-2023-32200	apache - jena	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
<u>CVE-2023-32200</u>	apache - Jena	SpringEL injection in the server agent in Apache Ambari version	2023-07-12	0.0	півн
		2.7.0 to 2.7.6 allows a malicious authenticated user to execute			
		arbitrary code remotely. Users are recommended to upgrade to			
<u>CVE-2022-42009</u>	apache - ambari	2.7.7. SpringEL injection in the metrics source in Apache Ambari version	2023-07-12	8.8	High
		2.7.0 to 2.7.6 allows a malicious authenticated user to execute			
		arbitrary code remotely. Users are recommended to upgrade to			
CVE-2022-45855	apache - ambari	2.7.7.	2023-07-12	8.8	High
		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.			
	apache - multiple	Any users running the Pulsar Function Worker for 2.9.* and earlier			
CVE-2023-30429	products	should upgrade to one of the above patched versions.	2023-07-12	8.8	High
		During the worker lifecycle, a use-after-free condition could have			
	mozilla - multiple	occured, which could have led to a potentially exploitable crash. This vulnerability affects Firefox < 115.0.2 and Firefox ESR <			
CVE-2023-3600	products	115.0.2.	2023-07-12	8.8	High
	jenkins -	A cross-site request forgery (CSRF) vulnerability in Jenkins Pipeline			
CVE-2023-37957	pipeline_restful_ap i	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
<u>CVL 2023 37337</u>	jenkins -	A cross-site request forgery (CSRF) vulnerability in Jenkins	2023 07 12	0.0	
	sumologic_publishe	Sumologic Publisher Plugin 2.2.1 and earlier allows attackers to			
CVE-2023-37958	r	connect to an attacker-specified URL.	2023-07-12	8.8	High
		A cross-site request forgery (CSRF) vulnerability in Jenkins Assembla Auth Plugin 1.14 and earlier allows attackers to trick			
CVE-2023-37961	jenkins - assembla	users into logging in to the attacker's account.	2023-07-12	8.8	High
		A cross-site request forgery (CSRF) vulnerability in Jenkins			
	1	Benchmark Evaluator Plugin 1.0.1 and earlier allows attackers to			
	jenkins - benchmark_evaluat	connect to an attacker-specified URL and to check for the existence of directories, `.csv`, and `.ycsb` files on the Jenkins			
CVE-2023-37962	or	controller file system.	2023-07-12	8.8	High
		A cross-site request forgery (CSRF) vulnerability in Jenkins			<u> </u>
		ElasticBox CI Plugin 5.0.1 and earlier allows attackers to connect to			
	jenkins -	an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in			
CVE-2023-37964	elasticbox_ci	Jenkins.	2023-07-12	8.8	High
		Vulnerability in SonicWall GMS and Analytics allows an			0
		authenticated attacker to upload files on the underlying filesystem			
CVE-2023-34126	sonicwall - multiple products	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
<u>CVE-2025-54120</u>	products	Improper Neutralization of Special Elements used in an OS	2023-07-13	0.0	High
		Command ('OS Command Injection') vulnerability in SonicWall			
		GMS, SonicWall Analytics enables an authenticated attacker to			
	conjourall multiple	execute arbitrary code with root privileges. This issue affects GMS:			
CVE-2023-34127	sonicwall - multiple products	9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions.	2023-07-13	8.8	High
<u> 2020 07127</u>	p. 044015	Improper limitation of a pathname to a restricted directory ('Path	_0_0 0, 10	0.0	
		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 privilages. This issue offects CNAS			
	sonicwall - multiple	underlying filesystem with root privileges. This issue affects GMS: 9.3.2-SP1 and earlier versions; Analytics: 2.5.0.4-R7 and earlier			

	microsoft - multiple	Microsoft Dynamics 365 (on-premises) Cross-site Scripting			
CVE-2023-35335	products	Vulnerability	2023-07-11	8.2	High
		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			
CVE-2023-32250	linux - linux_kernel	context of the kernel.	2023-07-10	8.1	High
		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			
CVE-2023-32254	linux - linux_kernel	in the context of the kernel.	2023-07-10	8.1	High
		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			
CVF 2022 22000	sap - multiple	from confidential files cannot be read but potentially some OS files	2022 07 11	0.1	11:
<u>CVE-2023-33989</u>	products microsoft - multiple	can be over-written leading to system compromise.	2023-07-11	8.1	High
CVE-2023-33127	products	.NET and Visual Studio Elevation of Privilege Vulnerability	2023-07-11	8.1	High
<u></u>	microsoft - multiple		2023 07 11	0.1	
CVE-2023-33170	products	ASP.NET and Visual Studio Security Feature Bypass Vulnerability	2023-07-11	8.1	High
		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.			
		1011 2.10.0 Defore 2.10.7, 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.			
	apache - multiple	2.11 Pulsar Broker users should upgrade to at least 2.11.1.			
CVE-2023-30428	products	3.0 Pulsar Broker users are unaffected.	2023-07-12	8.1	High
		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			
CVE 2022 27559	ibm - multiple	an unquoted service path. A local attacker could exploit this vulnerability to gain elevated privileges by inserting an executable	2022 07 10	7 9	High
<u>CVE-2023-27558</u>	products	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
<u>CVE-2023-27558</u>	products ibm -	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. IBM Watson Knowledge Catalog on Cloud Pak for Data 4.0 is	2023-07-10	7.8	High
<u>CVE-2023-27558</u>	products	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
<u>CVE-2023-27558</u> <u>CVE-2023-28958</u>	products ibm - watson_knowledge	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. IBM Watson Knowledge Catalog on Cloud Pak for Data 4.0 is potentially vulnerable to CSV Injection. A remote attacker could	2023-07-10 2023-07-10	7.8	High High
	products ibm - watson_knowledge _catalog_on_cloud	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. 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. IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect			
	products ibm - watson_knowledge _catalog_on_cloud	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. 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. IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 db2set is vulnerable to a buffer			
	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data	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. 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. 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			
<u>CVE-2023-28958</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple	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. 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. 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:	2023-07-10	7.8	High
	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data	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. 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. 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.			-
<u>CVE-2023-28958</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple	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. 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. 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:	2023-07-10	7.8	High
<u>CVE-2023-28958</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple	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. 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. 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. A vulnerability has been identified in Tecnomatix Plant Simulation	2023-07-10	7.8	High
<u>CVE-2023-28958</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple products	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. 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. 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. 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	2023-07-10	7.8	High
<u>CVE-2023-28958</u> <u>CVE-2023-30431</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple products siemens - multiple	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. 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. 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. 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	2023-07-10 2023-07-10	7.8	High High
<u>CVE-2023-28958</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple products	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. 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. 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. 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)	2023-07-10	7.8	High
<u>CVE-2023-28958</u> <u>CVE-2023-30431</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple products siemens - multiple	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. 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. 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. 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) A vulnerability has been identified in Tecnomatix Plant Simulation	2023-07-10 2023-07-10	7.8	High
<u>CVE-2023-28958</u> <u>CVE-2023-30431</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple products siemens - multiple	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. 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. 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. 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) A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation	2023-07-10 2023-07-10	7.8	High
<u>CVE-2023-28958</u> <u>CVE-2023-30431</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple products siemens - multiple	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. 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. 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. 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) A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application is	2023-07-10 2023-07-10	7.8	High
<u>CVE-2023-28958</u> <u>CVE-2023-30431</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple products siemens - multiple products	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. 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. 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. 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) A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (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) A vulnerability has been identified in 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)	2023-07-10 2023-07-10	7.8	High
<u>CVE-2023-28958</u> <u>CVE-2023-30431</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple products siemens - multiple	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. 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. 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. 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) A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2201.0008), Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), 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	2023-07-10 2023-07-10	7.8	High
<u>CVE-2023-28958</u> <u>CVE-2023-30431</u> <u>CVE-2023-37246</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple products siemens - multiple products	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. 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. 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. 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) A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (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) A vulnerability has been identified in 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)	2023-07-10 2023-07-10 2023-07-11	7.8 7.8 7.8	High High High
<u>CVE-2023-28958</u> <u>CVE-2023-30431</u> <u>CVE-2023-37246</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple products siemens - multiple products	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. 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. 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. 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) A vulnerability has been identified in 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) A vulnerability has been identified in 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) A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation	2023-07-10 2023-07-10 2023-07-11	7.8 7.8 7.8	High High High
<u>CVE-2023-28958</u> <u>CVE-2023-30431</u> <u>CVE-2023-37246</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple products siemens - multiple products siemens - multiple	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. 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. 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. 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) A vulnerability has been identified in Tecnomatix Plant Simulation V2302 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2201.0008), Tecnomatix Plant Simulation V2201 (All versions < V2302.0002). The affected application is	2023-07-10 2023-07-10 2023-07-11	7.8 7.8 7.8	High High High
<u>CVE-2023-28958</u> <u>CVE-2023-30431</u> <u>CVE-2023-37246</u>	products ibm - watson_knowledge _catalog_on_cloud _pak_for_data ibm - multiple products siemens - multiple products	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. 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. 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. 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) A vulnerability has been identified in 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) A vulnerability has been identified in 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) A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation	2023-07-10 2023-07-10 2023-07-11	7.8 7.8 7.8	High High High

		attacker to execute code in the context of the current process. (ZDI-CAN-21155)			
		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			
	siemens - multiple	vulnerable to stack-based buffer overflow while parsing specially crafted STP files. This could allow an attacker to execute code in			
CVE-2023-37374	products	the context of the current process. (ZDI-CAN-21054) A vulnerability has been identified in Tecnomatix Plant Simulation	2023-07-11	7.8	High
		V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application is			
<u>CVE-2023-37375</u>	siemens - multiple products	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
		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			
CVE-2023-37376	siemens - multiple products	could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21051)	2023-07-11	7.8	High
		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			
<u>CVE-2023-3269</u>	linux - linux_kernel	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 2022 21750	microsoft - multiple		2022 07 14	70	
<u>CVE-2023-21756</u>	products microsoft - multiple	Windows Win32k Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-32046</u>	products microsoft -	Windows MSHTML Platform Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-32047</u>	paint_3d microsoft -	Paint 3D Remote Code Execution Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-32051</u>	raw_image_extensi on microsoft - multiple	Raw Image Extension Remote Code Execution Vulnerability	2023-07-11	7.8	High
CVE-2023-32053	products	Windows Installer Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-33148</u>	microsoft - multiple products microsoft - multiple	Microsoft Office Elevation of Privilege Vulnerability	2023-07-11	7.8	High
CVE-2023-33149	products	Microsoft Office Graphics Remote Code Execution Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-33152</u>	microsoft - multiple products microsoft - multiple	Microsoft ActiveX Remote Code Execution Vulnerability Windows Cloud Files Mini Filter Driver Elevation of Privilege	2023-07-11	7.8	High
<u>CVE-2023-33155</u>	products	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
<u>CVE-2023-33161</u>	microsoft - multiple products	Microsoft Excel Remote Code Execution Vulnerability Improper privilege management in Zoom Rooms for Windows	2023-07-11	7.8	High
<u>CVE-2023-34118</u>	zoom - rooms	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
<u>CVE-2023-34119</u>	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
<u>CVE-2023-35304</u>	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-35305</u>	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-35312</u>	microsoft - multiple products	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-35313</u>	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
<u>CVE-2023-35320</u>	microsoft - multiple products	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-35323</u>	microsoft - multiple products	Windows OLE Remote Code Execution Vulnerability	2023-07-11	7.8	High
CVE-2023-35328	microsoft - multiple products microsoft - multiple	Windows Transaction Manager Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-35337</u>	products	Win32k Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-35340</u>	microsoft - multiple products	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability	2023-07-11	7.8	High
	microsoft - multiple	Windows Image Acquisition Elevation of Privilege Vulnerability	2023-07-11	7.8	High

	microsoft multiple	Windows Geolocation Service Remote Code Execution			
<u>CVE-2023-35343</u>	microsoft - multiple products	Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-35353</u>	microsoft - multiple products	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-35356</u>	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-35357</u>	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-35358</u>	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-35362</u>	microsoft - multiple products	Windows Clip Service Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-35363</u>	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-35374</u>	microsoft - paint_3d	Paint 3D Remote Code Execution Vulnerability	2023-07-11	7.8	High
<u>CVE-2023-36536</u>	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
<u>CVE-2023-36537</u>	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
		Improper access control in Zoom Rooms for Windows before version 5.15.0 may allow an authenticated user to enable an			
<u>CVE-2023-36538</u>	zoom - rooms microsoft - multiple	escalation of privilege via local access. Windows Error Reporting Service Elevation of Privilege	2023-07-11	7.8	High
<u>CVE-2023-36874</u>	products	Vulnerability	2023-07-11	7.8	High
		A vulnerability has been discovered in the Citrix Secure Access client for Windows			
<u>CVE-2023-24491</u>	citrix - secure_access_clie nt	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
	google - multiple	In DMService, there is a possible missing permission check. This could lead to local escalation of privilege with no additional	2022.07.12	7.0	
<u>CVE-2023-30916</u>	products	execution privileges. In DMService, there is a possible missing permission check. This	2023-07-12	7.8	High
<u>CVE-2023-30917</u>	google - multiple products	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
	google - multiple	In telephony service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional			
<u>CVE-2023-30929</u>	products	execution privileges. 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	2023-07-12	7.8	High
CVE-2023-3106	linux - multiple products	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
	adobe - multiple	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			0.,
<u>CVE-2021-43757</u>	products adobe - multiple	malicious 3GP ?file 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	2023-07-12	7.8	High
<u>CVE-2023-29308</u>	products	that a victim must open a malicious file. 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	2023-07-12	7.8	High
CVE-2023-21257	google - android	interaction is not needed for exploitation.	2023-07-13	7.8	High

		there is a possible way to bypass cryptographic assurances due to			
CVE-2023-21399	google - android	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
		IBM Watson CP4D Data Stores 4.6.0 does not properly allocate resources without limits or throttling which could allow a remote			
<u>CVE-2023-27540</u>	ibm - multiple products	attacker with information specific to the system to cause a denial of service. IBM X-Force ID: 248924.	2023-07-10	7.5	High
	ibm - multiple	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			
<u>CVE-2023-30442</u>	products	wrapper using certain options. IBM X-Force ID: 253202.	2023-07-10	7.5	High
<u>CVE-2023-30445</u>	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. 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	2023-07-10	7.5	High
		specially crafted query on certain tables. IBM X-Force ID:			
<u>CVE-2023-30446</u>	ibm - multiple products	253361	2023-07-10	7.5	High
<u>CVE-2023-30447</u>	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
<u>CVE-2023-30448</u>	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
	ibm - multiple	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			
CVE-2023-30449	products citrix - multiple	specially crafted query. IBM X-Force ID: 253439.	2023-07-10	7.5	High
<u>CVE-2023-24487</u>	products	Arbitrary file read in Citrix ADC and Citrix Gateway? 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	2023-07-10	7.5	High
CVE-2023-36917	sap - multiple products	or system availability, this could lead to an attacker to completely takeover a victim's account.	2023-07-11	7.5	High
		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.			
<u>CVE-2022-31810</u>	siemens - sipass_integrated	This could allow an unauthenticated remote attacker to crash the server application, creating a denial of service condition.	2023-07-11	7.5	High
	siemens - simatic_mv540_h_f	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			
<u>CVE-2023-35920</u>	irmware siemens - simatic_mv540_h_f	manually. 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	2023-07-11	7.5	High
<u>CVE-2023-35921</u>	irmware	restarted manually. 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	2023-07-11	7.5	High
	siemens -	synchronization server of the affected products contains a			
<u>CVE-2023-36521</u>	simatic_mv540_h_f irmware	vulnerability that may lead to a denial of service condition. An attacker may	2023-07-11	7.5	High

case a entral of profess statistics of all societ-based affected products if the result server is enabled An improper limitation of all societ-based An improper limitation of all societ-based CVE 2002-2042 Profession of the societ of the result server is enabled. CVE 2002-2042 Profession of the societ of the result server is enabled. CVE 2002-2042 Profession of the societ of societ						
affected products II be result server is enabled. an improve timitation of a pathname to a misting difference in a first frager in products. an improve timitation of a pathname to a misting difference in a first frager in products. 0/530232447 First frager in the intervent in an intervent and a mission of a pathname to a mathematical difference in the intervent in a mission of a pathname to a mathematical and intervent interventinterventintervent intervent intervent intervent intervent inter						
An improper limitation of a pathname to a estricted directory (Path Trevest) whenholing (VE22) in 50% Exceeds management interface 7.0.0 through 7.0, 4.2.0 through 4.2.4, 4.1.1 through 4.8.4, 0.0 through 4.0.3, 3.0 through 4.2.4, 4.1.1 through 4.8.4, 0.0 through 4.0.3, 3.0 through 4.2.4, through 2.2, 5.3 unershow the future interface 7.0.0 through 7.0, 4.2.0 through 4.2.4, 4.1.1 through 4.8.4, 0.0 through 4.0.3, 3.0 through 4.2.4, through 2.2, 5.3 unershow the future interface 7.0.0 through 7.0, 4.2.0 through 4.2.4, 4.1.1 through 4.1.8, 4.0.0 through 4.0.3, 3.0 through 4.2.4, through 2.2, 5.3 unershow the future interface 7.0.0 through 2.2, 5.1 unershow products and the future interface 7.0.0 through 2.2, 5.1 unershow products and through 2.2, 5.3 unershow the future interface 7.0.0 through 2.2, 5.1 unershow products and through 2.2, 5.2 unershow the future interface 7.0.0 through 2.2, 5.2 unershow products and through 2.2, 5.2 unershow the future interface 7.0.0 through 2.2, 5.2 unershow products and through 2.2, 5.2 unershow through 2.2, 5.2 unershow the future products and through 2.2, 5.2 unershow through 2.2, 5.2 unershow the future intercostin - mulpite through 2.2, 5.2 unershow through 2.2, 5.2 unershow through 2.2, 5.2 unershow through 2.2, 5.2 unershow products and through 2.2, 5.2 unershow the future through 2.2, 5.2 unershow through 2.2, 5.						
Path Tracessity volmentability (CVF-22) in Fordin Lender management Interest 7: 201 Intrugh 2:3, 2:3 2:1 Path Travessity Volmentability (CVF-203-3:204 CVF-2022-23427 for literative contractive contentitity contractive contractive contractive contractive contrac						
4.1.1 through 4.18, 4.0 through 4.2, 3.5 01 through 3.2, 3.2.1 6/110 Fortile 1-multiple products 2012-022 0/12-022 products Render Autoker to retrieve arbitray files from the underlying filesystem visces in through 4.2.1 for through 4.2.1 for through 4.2.2 and through 4.2.1 for the underlying filesystem visces in through 4.2.1 for th			('Path Traversal') vulnerability [CWE-22] in FortiExtender			
orticlet - multiple (VF-2022-2342) forticlet - multiple (Figure nois specially cardied with requests. 2023-07-11 7.5 High (Figure nois specially cardied with requests. CVF-2022-2023 microsoft - multiple (Figure nois specially cardied with requests. 2023-07-11 7.5 High (Figure nois specially cardied with requests. CVF-2023-2020 microsoft - multiple (Figure nois special) CVF-2023-2021 7.5 High (Figure nois special) CVF-2023-2021 microsoft - multiple (Figure nois special) CVF-2023-2021 7.5 High (Figure nois special) CVF-2023-2021 microsoft - multiple (Figure nois special) Microsoft Message Queuing Denial of Service Vulnerability 2023-07-11 7.5 High (Figure nois special) CVF-2023-2021 microsoft - multiple (Figure nois special) Microsoft Message Queuing Denial of Service Vulnerability 2023-07-11 7.5 High (Figure nois special) CVF-2023-2021 microsoft - multiple (Figure nois special) Witcosoft Message Queuing Denial of Service Vulnerability 2023-07-11 7.5 High (Figure nois special) CVF-2023-23316 microsoft - multiple (Figure nois special) Witcosoft Message Queuing Mental of Service Vulnerability 2023-07-11 7.5 High (Figure nois special) </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						
CVE-2022-2342 mordust Intervalt 7.5 High CVE-2022-2342 mordust mordust 7.5 High CVE-2022-23702 products mordust 7.5 High CVE-2022-23703 products mordust 7.5 High CVE-2022-23704 products mordust 7.5 High CVE-2022-23704 products mordust 7.5 High CVE-2022-23704 mordust Mordust National N			through 3.2.3, 5.3 all versions may allow an unauthenticated and			
CVE.2023.2029 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023.07.11 7.5 High CVE.2023.2028 products microsoft. mittiget CVE.2023.2028 2023.07.11 7.5 High CVE.2023.2026 products microsoft. mittiget CVE.2023.2026 products T.5 High CVE.2023.2026 microsoft. mittiget CVE.2023.2026 T.5 High CVE.2023.2026 microsoft. mittiget Microsoft Message Queuing Denial of Service Vulnerability 2023.07.11 7.5 High CVE.2023.2026 microsoft. mittiget Microsoft Message Queuing Denial of Service Vulnerability 2023.07.11 7.5 High CVE.2023.2026 microsoft. mittiget Microsoft Message Queuing Denial of Service Vulnerability 2023.07.11 7.5 High CVE.2023.2027 products Microsoft SharePoint Service Scartiny Feature Bypass Vulnerability 2023.07.11 7.5 High CVE.2023.2027 products microsoft. Microsoft Message Queuing Benote Code Evice Vulnerability 2023.07.11	<u>CVE-2022-23447</u>	products		2023-07-11	7.5	High
CVF_2023.2035 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVF_2023.3042 products Uticsoft - multiple T.5 High CVF_2023.3044 products Iticsoft - multiple T.5 High CVF_2023.3045 products Iticsoft - multiple T.5 High CVF_2023.3045 products Iticsoft - multiple T.5 High CVF_2023.3046 products Iticsoft - multiple T.5 High CVF_2023.3046 products Itidsoft - multiple T.5 High CVF_2023.3046 products Itidsoft Assessed Executing Denial of Service Vulnerability 2023-07-11 7.5 High CVF_2023.3046 microsoft - multiple Microsoft SharePoint Service Security Feature Bypass Vulnerability 2023-07-11 7.5 High CVF_2023.33160 microsoft - multiple Microsoft SharePoint Service Vulnerability 2023-07-11 7.5 High CVF_2023.33161 microsoft - multiple Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 <	<u>CVE-2023-32034</u>	products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-3202 products DE Automation Information Disclosure Vulnerability 2023-07-11 7.5 High CVE-2023-3204 microsoft - multiple Microsoft Message Quaving Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3204 microsoft - multiple Microsoft Message Quaving Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3316 microsoft - multiple Windows Network Load Balancing Remote Code Execution 2023-07-11 7.5 High CVE-2023-3316 microsoft - multiple Windows Namet Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3316 microsoft - multiple Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3316 microsoft - multiple Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3316 microsoft - multiple Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3316 microsoft - multiple Remote Procedure Call Runtime Denial of Service Vulnerability 2023	<u>CVE-2023-32035</u>	products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-3204 products Microsoft Nessage Quarting Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3205 products Microsoft Nessage Quarting Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3205 products Microsoft Nessage Quarting Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3305 products Windrox Stework Load Balancing Remote Code Execution 2023-07-11 7.5 High CVE-2023-33165 products Microsoft SharePoint Server Security Feature Bypass Vulnerability 2023-07-11 7.5 High CVE-2023-33165 products Microsoft SharePoint Server Security Feature Bypass Vulnerability 2023-07-11 7.5 High CVE-2023-33167 products Remote Procedure Call Buntine Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-33126 products Remote Procedure Call Buntine Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-33127 products Remote Procedure Call Buntine Denial of Service Vulnerability 2023-07-11 7.5 High	<u>CVE-2023-32042</u>	products	OLE Automation Information Disclosure Vulnerability	2023-07-11	7.5	High
CVE-2023-33045 products Microsoft Message Queuing Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-33049 products Microsoft Message Queuing Bendle of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3305 microsoft - multiple Windows Network Load Balancing Remote Code Execution 2023-07-11 7.5 High CVE-2023-3305 microsoft - multiple Microsoft SharePoint Server Security Feature Bypass Vulnerability 2023-07-11 7.5 High CVE-2023-3305 microsoft - multiple Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-33168 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-33128 microsoft - multiple Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-33129 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-33202 microsoft - multiple Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 <t< td=""><td><u>CVE-2023-32044</u></td><td>products</td><td>Microsoft Message Queuing Denial of Service Vulnerability</td><td>2023-07-11</td><td>7.5</td><td>High</td></t<>	<u>CVE-2023-32044</u>	products	Microsoft Message Queuing Denial of Service Vulnerability	2023-07-11	7.5	High
CVF.2023-3284 products IHTP sys Denial of Service Vulnerability 2023-07-11 7.5 High CVF.2023-3313 products Vulnerability 2023-07-11 7.5 High CVF.2023-3315 products Microsoft-multiple Microsoft-multiple 2023-07-11 7.5 High CVF.2023-3315 products Bemote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVF.2023-3316 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVF.2023-3316 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVF-2023-3312 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVF-2023-3312 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVF-2023-3312 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVF-2023-3312 products Becurita	<u>CVE-2023-32045</u>	products	Microsoft Message Queuing Denial of Service Vulnerability	2023-07-11	7.5	High
CVE.2022-3313 products Vulnerability 2023-07-11 7.5 High CVE.2022-33155 products Microsoft SharePoint Server Security Feature Bypass Vulnerability 2023-07-11 7.5 High CVE-2022-33156 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2022-33156 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2022-33159 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2022-33172 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2022-33172 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2022-33172 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2022-3529 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2022-35329	<u>CVE-2023-32084</u>	products		2023-07-11	7.5	High
CVE-2023-33165 products Microsoft SharePoint Server Security Feature Bypass Vulnerability 2022-07-11 7.5 High CVE-2023-33166 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-33167 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-33167 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3312 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3312 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3517 products Remote Procedure Call Runtime Denial of Service Vulnerability 2023-07-11 7.5 High CVE-2023-3527 products Windows Pramatic General Multicat (FGM) Remote Code 2023-07-11 7.5 High CVE-2023-3529 products Windows Premating Remote Code Execution Vulnerability 2023-07-11 7.5 High <td< td=""><td><u>CVE-2023-33163</u></td><td>products</td><td>-</td><td>2023-07-11</td><td>7.5</td><td>High</td></td<>	<u>CVE-2023-33163</u>	products	-	2023-07-11	7.5	High
CVE-2023-33166 (VE-2023-33167)productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-33167 (VE-2023-33167)microsoft - multiple productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-33169 (VE-2023-33168)microsoft - multiple productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-33129 (VE-2023-33127)products productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-33129 (VE-2023-33127)products productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35129 (VE-2023-3528)microsoft - multiple Windows Pragmatic General Kulticat (PGM) Remote Code Execution Vulnerability2023-07-117.5HighCVE-2023-3529 (VE-2023-3529)microsoft - multiple Windows Pragmatic General Kulticat (PGM) Remote Code Evecution Vulnerability2023-07-117.5HighCVE-2023-3530 (VE-2023-35328)microsoft - multiple Windows Print Spooler Information Disclosure Vulnerability2023-07-117.5HighCVE-2023-3533 (VE-2023-3533)microsoft - multiple ProductsWindows Prev Name Resolution Protocol Denial of Service Vulnerability2023-07-117.5HighCVE-2023-3533 (VE-2023-3533)microsoft - multiple ProductsWindows Prev Name Resolution Protocol Denial of Service Vulnerability2023-07-117.5HighCVE-202	<u>CVE-2023-33165</u>	products	Microsoft SharePoint Server Security Feature Bypass Vulnerability	2023-07-11	7.5	High
CVF-2023-33167productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVF-2023-33168productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVF-2023-33169productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVF-2023-33172productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVF-2023-33172productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVF-2023-33279microsoft - multipleWindows Pragmatic General Multicast (PGM) Remote Code2023-07-117.5HighCVF-2023-35291productsEvecution Vulnerability2023-07-117.5HighCVF-2023-35292productsHITP sys Denial of Service Vulnerability2023-07-117.5HighCVF-2023-35293productsMicrosoft Message Queuing Remote Code Execution Vulnerability2023-07-117.5HighCVF-2023-35304productsMicrosoft Message Queuing Remote Code Execution Vulnerability2023-07-117.5HighCVF-2023-35330microsoft - multipleWindows Prent Spooler Information Disclosure Vulnerability2023-07-117.5HighCVF-2023-35331productsWindows Sere Name Resolution Protocol Denial of Service Vulnerability2023-07-117.5HighCVF-2023-35332productsWindows CryptoAPI Denial of Service Vulnerability2023-07-11 <td><u>CVE-2023-33166</u></td> <td>products</td> <td>Remote Procedure Call Runtime Denial of Service Vulnerability</td> <td>2023-07-11</td> <td>7.5</td> <td>High</td>	<u>CVE-2023-33166</u>	products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-33168productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-33169productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-33179productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-33179productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35291productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35292productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35292productsMicrosoft Message Queuing Remote Code Execution Vulnerability2023-07-117.5HighCVE-2023-35293productsMicrosoft Message Queuing Remote Code Execution Vulnerability2023-07-117.5HighCVE-2023-35329productsWindows Print Spooler Information Disclosure Vulnerability2023-07-117.5HighCVE-2023-35339productsWindows Extended Negotiation Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35339productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35339productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35339productsWindows CryptoAPI Denial of Service Vulnerability2023	<u>CVE-2023-33167</u>	products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-33169productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-33172productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-33172productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35292productsExecution Vulnerability2023-07-117.5HighCVE-2023-35293productsHTTP-sys Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35294productsHTTP-sys Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35300productsWindows Print Spooler Information Disclosure Vulnerability2023-07-117.5HighCVE-2023-35330productsWindows Print Spooler Information Disclosure Vulnerability2023-07-117.5HighCVE-2023-35330productsWindows Extended Negotiation Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35339productsWindows Reer Name Resolution Protocol Denial of Service2023-07-117.5HighCVE-2023-35339productsWindows Reer Name Resolution Protocol Denial of Service2023-07-117.5HighCVE-2023-35339productsWindows Reer Name Resolution Protocol Denial of Service2023-07-117.5HighCVE-2023-35339productsWindows Reer Name Resolution Protocol Denial of Service2023-07-117.5HighCVE-2023-35339 <td< td=""><td><u>CVE-2023-33168</u></td><td>products</td><td>Remote Procedure Call Runtime Denial of Service Vulnerability</td><td>2023-07-11</td><td>7.5</td><td>High</td></td<>	<u>CVE-2023-33168</u>	products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-33172productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-33173productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35297productsExecution Vulnerability2023-07-117.5HighCVE-2023-35298productsExecution Vulnerability2023-07-117.5HighCVE-2023-35298productsMicrosoft - Multiple2023-07-117.5HighCVE-2023-35309productsMicrosoft Message Queuing Remote Code Execution Vulnerability2023-07-117.5HighCVE-2023-35320productsWindows Print Spooler Information Disclosure Vulnerability2023-07-117.5HighCVE-2023-35330productsWindows Stended Negotiation Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35330productsWindows Stended Negotiation Protocol Denial of Service2023-07-117.5HighCVE-2023-35330productsWindows Stended Negotiation Protocol Denial of Service2023-07-117.5HighCVE-2023-35331pandocuploadVulnerability2023-07-117.5HighCVE-2023-35332productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35339productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35339productsWindows CryptoAPI Denial of Service Vulnerability2023-07-11 <t< td=""><td><u>CVE-2023-33169</u></td><td>products</td><td>Remote Procedure Call Runtime Denial of Service Vulnerability</td><td>2023-07-11</td><td>7.5</td><td>High</td></t<>	<u>CVE-2023-33169</u>	products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-33173productsRemote Procedure Call Runtime Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35292microsoft - multipleKindows Pragmatic General Multicast (PGM) Remote Code2023-07-117.5HighCVE-2023-35298microsoft - multipleNicrosoft - Multiple2023-07-117.5HighCVE-2023-35309productsMicrosoft Message Queuing Remote Code Execution Vulnerability2023-07-117.5HighCVE-2023-35325productsMicrosoft Message Queuing Remote Code Execution Vulnerability2023-07-117.5HighCVE-2023-35330productsWindows Print Spooler Information Disclosure Vulnerability2023-07-117.5HighCVE-2023-35330productsWindows Perint Spooler Information Disclosure Vulnerability2023-07-117.5HighCVE-2023-35331pandocuploadWindows Peer Name Resolution Protocol Denial of Service2023-07-117.5HighCVE-2023-35332productsWindows Peer Name Resolution Protocol Denial of Service2023-07-117.5HighCVE-2023-35332productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35332productsWindows Remote Desktop Security Feature Bypass Vulnerability2023-07-117.5HighCVE-2023-25352productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5HighCVE-2023-25352productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5High <td><u>CVE-2023-33172</u></td> <td>products</td> <td>Remote Procedure Call Runtime Denial of Service Vulnerability</td> <td>2023-07-11</td> <td>7.5</td> <td>High</td>	<u>CVE-2023-33172</u>	products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-35297productsExecution Vulnerability2023-07-117.5HighVE-2023-35298productsHTTP.sys Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35290productsMicrosoft Message Queuing Remote Code Execution Vulnerability2023-07-117.5HighCVE-2023-35309productsWindows Print Spooler Information Disclosure Vulnerability2023-07-117.5HighCVE-2023-35330productsWindows Extended Negotiation Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35339pandocupleadVulnerability2023-07-117.5HighCVE-2023-35339productsWindows Extended Negotiation Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35339productsVulnerability2023-07-117.5HighMicrosoft - multipleWindows Peer Name Resolution Protocol Denial of Service2023-07-117.5HighCVE-2023-35339productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35329productsWindows Remote Desktop Security Feature Bypass Vulnerability2023-07-117.5HighCVE-2023-25329productsWindows Remote Desktop Security Feature Bypass Vulnerability2023-07-117.5HighAn Issue discovered in MikroTik Router v6.46.3 and earlier allows attacker to cause denial of service valamisconfiguration in the SSH2023-07-127.5HighCVE-2023-202021mikrotik - routerosAdobe ColdF	<u>CVE-2023-33173</u>	products		2023-07-11	7.5	High
CVE-2023-35292productsHTTP.sys Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35302productsMicrosoft Message Queuing Remote Code Execution Vulnerability2023-07-117.5HighCVE-2023-35325productsWindows Print Spooler Information Disclosure Vulnerability2023-07-117.5HighCVE-2023-35333pandocuploadWindows Extended Negotiation Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35333pandocuploadWindows Extended Negotiation Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35333pandocuploadVulnerability2023-07-117.5HighCVE-2023-35338productsWindows Pere Name Resolution Protocol Denial of Service2023-07-117.5HighCVE-2023-35339microsoft - multipleWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35352productsWindows Remote Desktop Security Feature Bypass Vulnerability2023-07-117.5HighCVE-2023-25352productsWindows Remote Desktop Security Feature Bypass Vulnerability2023-07-127.5HighCVE-2023-25352productsAnissue discovered in Mikro Tik Router v6.46.3 and earlier and earlier2023-07-127.5HighCVE-2023-29298productsAdobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.330468 (and earlier), and earlier and and earlier2023-07-127.5HighCVE-2023-29298productsExploitation of this i	<u>CVE-2023-35297</u>	products		2023-07-11	7.5	High
CVE-2023-35309productsMicrosoft Message Queuing Remote Code Execution Vulnerability2023-07-117.5HighCVE-2023-35320microsoft - multiple productsWindows Print Spooler Information Disclosure Vulnerability2023-07-117.5HighCVE-2023-35330productsWindows Extended Negotiation Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35333pandocuploadWeindows Extended Negotiation Remote Code Execution2023-07-117.5Highmicrosoft - multipleWindows Peer Name Resolution Protocol Denial of Service2023-07-117.5HighCVE-2023-35339productsVulnerability2023-07-117.5HighCVE-2023-35339productsVulnerability2023-07-117.5HighCVE-2023-35359productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35352productsWindows Remote Desktop Security Feature Bypass Vulnerability2023-07-117.5HighCVE-2020-20021mikrotik - routerosdaemon.2023-07-127.5HighAn issue discovered in MikroTik Router v6.46.3 and earlier allows attacker to cause denial of service via misconfiguration in the SH2023-07-127.5HighCVE-2023-29298productsproductsExploitation of this issue does not require user interaction.2023-07-127.5HighCVE-2023-29298productsproductsExploitation of this issue does not require user interaction.2023-07-127.5High	<u>CVE-2023-35298</u>	products	HTTP.sys Denial of Service Vulnerability	2023-07-11	7.5	High
CVE-2023-35325productsWindows Print Spooler Information Disclosure Vulnerability2023-07-117.5Highmicrosoft - multipleWindows Extended Negotiation Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35330microsoft - productsMediaWiki PandocUpload Extension Remote Code Execution2023-07-117.5HighCVE-2023-35333microsoft - productsWindows Peer Name Resolution Protocol Denial of Service2023-07-117.5HighCVE-2023-35339productsWindows Peer Name Resolution Protocol Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35339productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35352productsWindows Remote Desktop Security Feature Bypass Vulnerability2023-07-117.5HighCVE-2023-35352productsMindows Remote Desktop Security Router v6 46.3 and earlier allows attacker to cause denial of service via misconfiguration in the SSH attacker to cause denial of service via misconfiguration in the SSH2023-07-127.5HighCVE-2023-29298mikrotik - routerosdaemon.2023-03.030468 (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 acces the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction.2023-07-127.5HighCVE-2023-29298productsAdobe ColdFusion versions 2018u16 (and earlier) action Attempts vulnerability to acces the adminis	<u>CVE-2023-35309</u>	products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-07-11	7.5	High
CVE-2023-35330productsWindows Extended Negotiation Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35333pandocuploadWindews Peer Name Resolution Protocol Denial of Service2023-07-117.5HighCVE-2023-35338pandocuploadVulnerability2023-07-117.5HighCVE-2023-35338productsVulnerability2023-07-117.5HighCVE-2023-35339productsWindows Peer Name Resolution Protocol Denial of Service2023-07-117.5HighCVE-2023-35339productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35352productsWindows Remote Desktop Security Feature Bypass Vulnerability2023-07-117.5HighCVE-2020-20021mikrotik - routerosAn issue discovered in MikroTik Router v6.46.3 and earlier allows attacker to cause denial of service via misconfiguration in the SSH daemon.2023-07-127.5HighCVE-2020-20021mikrotik - routerosAdobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier) are affected by an Improper Access Control vulnerability to access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction.2023-07-127.5HighCVE-2023-29298productsproductsearlier) and 2023.0.0.330468 (and earlier), 2021u6 (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 <br< td=""><td><u>CVE-2023-35325</u></td><td>products</td><td>Windows Print Spooler Information Disclosure Vulnerability</td><td>2023-07-11</td><td>7.5</td><td>High</td></br<>	<u>CVE-2023-35325</u>	products	Windows Print Spooler Information Disclosure Vulnerability	2023-07-11	7.5	High
CVE-2023-35333pandocuploadVulnerability2023-07-117.5Highmicrosoft - multiple CVE-2023-35338productsVulnerability2023-07-117.5Highmicrosoft - multiple CVE-2023-35339productsWindows Rever Name Resolution Protocol Denial of Service2023-07-117.5HighCVE-2023-35339productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35352productsWindows Remote Desktop Security Feature Bypass Vulnerability2023-07-117.5HighCVE-2020-20021mikrotik - routerosAn issue discovered in MikroTik Router v6.46.3 and earlier allows attacker to cause denial of service via misconfiguration in the SSH daemon.2023-07-127.5HighCVE-2020-20021mikrotik - routerosAdobe 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 leverage this sunnerability to access the administration CFM and CFC endpoints.2023-07-127.5HighCVE-2023-29298productsAdobe 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 to access the administration CFM and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier) are affected by an Improper Restriction of Excessive Authentication Attempts vulnerability to access the administration of this issue does not require user interaction.2023-07-127.5High	<u>CVE-2023-35330</u>	products		2023-07-11	7.5	High
CVE-2023-35338productsVulnerability2023-07-117.5Highmicrosoft - multiple CVE-2023-35339productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5Highmicrosoft - multiple CVE-2023-35352productsWindows Remote Desktop Security Feature Bypass Vulnerability2023-07-117.5HighCVE-2023-35352productsWindows Remote Desktop Security Feature Bypass Vulnerability2023-07-117.5HighCVE-2020-20021mikrotik - routerosdaemon.2023-07-127.5HighAdobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330458 (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.2023-07-127.5HighCVE-2023-29298productsExploitation of this issue does not require user interaction.2023-07-127.5HighAdobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier), 2021u6 (and earlier), 2023.0.0.330458 (and earlier), 2023-07-127.5HighCVE-2023-29298productsExploitation of this issue does not require user interaction.2023-07-127.5HighCVE-2023-29298productsconfidentiality of the user. Exploitation of this issue does not require user interaction of Excessive Authentication Attempts vulnerability that could result in a Security feature bypass. An attacker could leverage this in	<u>CVE-2023-35333</u>	pandocupload	Vulnerability	2023-07-11	7.5	High
CVE-2023-35339microsoft - multiple productsWindows CryptoAPI Denial of Service Vulnerability2023-07-117.5HighCVE-2023-35352productsWindows Remote Desktop Security Feature Bypass Vulnerability2023-07-117.5HighCVE-2023-35352productsMindows Remote Desktop Security Feature Bypass Vulnerability2023-07-117.5HighAn issue discovered in MikroTik Router v6.46.3 and earlier allows attacker to cause denial of service via misconfiguration in the SSH daemon.2023-07-127.5HighCVE-2020-20021mikrotik - routerosAdobe 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.2023-07-127.5HighCVE-2023-29298productsAdobe 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.2023-07-127.5HighCVE-2023-29301adobe - multiple productsImproper 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 t	<u>CVE-2023-35338</u>	•		2023-07-11	7.5	High
microsoft - multiple products Windows Remote Desktop Security Feature Bypass Vulnerability 2023-07-11 7.5 High 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 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 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 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 In DMPixelLogger_ProcessDmCommand of DMPixelLogger.cpp, there is a possible out of bounds read due to a mi		microsoft - multiple				
CVE-2020-20021An issue discovered in MikroTik Router v6.46.3 and earlier allows attacker to cause denial of service via misconfiguration in the SSH daemon.2023-07-127.5HighAdobe 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.2023-07-127.5HighCVE-2023-29298adobe - multiple productsAdobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier), and CFC endpoints. Exploitation of this issue does not require user interaction.2023-07-127.5HighAdobe 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.2023-07-127.5HighIm 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 not2023-07-127.5High		microsoft - multiple				
CVE-2020-20021mikrotik - routerosdaemon.2023-07-127.5HighAdobe 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.2023-07-127.5HighCVE-2023-29298productsAdobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier) are affected by an Improper Restriction of this issue does not require user interaction.2023-07-127.5HighCVE-2023-29298Adobe 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.2023-07-127.5HighCVE-2023-29301productsrequire user interaction.2023-07-127.5HighIn DMPRixelLogger_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 not4			An issue discovered in MikroTik Router v6.46.3 and earlier allows		-	<u> </u>
Adobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.330468 (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.2023-07-127.5HighCVE-2023-29298productsAdobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0330468 (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.2023-07-127.5HighCVE-2023-29301productsIn 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 not2023-07-127.5High	<u>CVE-2020-20021</u>	mikrotik - routeros	-	2023-07-12	7.5	High
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.2023-07-127.5HighCVE-2023-29298Adobe 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.2023-07-127.5HighCVE-2023-29301adobe - multiple productsImproper Restriction of Excessive Authentication of this issue does not require user interaction.2023-07-127.5HighIn 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 not2023-07-127.5High						-
adobe - multiple productsvulnerability to access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction.2023-07-127.5HighAdobe 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.2023-07-127.5HighCVE-2023-29301productsrequire user interaction.2023-07-127.5HighIn 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 not44			Improper Access Control vulnerability that could result in a			
CVE-2023-29298productsExploitation of this issue does not require user interaction.2023-07-127.5HighAdobe 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.2023-07-127.5HighCVE-2023-29301productsrequire user interaction.2023-07-127.5HighIn 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 not11		adobe - multiple				
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.2023-07-127.5HighCVE-2023-29301In 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 not2023-07-127.5High	<u>CVE-2023-29298</u>	•	Exploitation of this issue does not require user interaction.	2023-07-12	7.5	High
CVE-2023-29301vulnerability 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.2023-07-127.5HighIn 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 not2023-07-127.5High			earlier) and 2023.0.0.330468 (and earlier) are affected by an			
CVE-2023-29301attacker could leverage this vulnerability to impact the confidentiality of the user. Exploitation of this issue does not require user interaction.2023-07-127.5HighIn 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 notIn the private of the user interaction is notIn the private of the user interaction is not						
CVE-2023-29301productsrequire user interaction.2023-07-127.5HighIn 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 not444		adaba madaba	attacker could leverage this vulnerability to impact the			
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	<u>CVE-2023-29301</u>		require user interaction.	2023-07-12	7.5	High
check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not						
			check. This could lead to remote information disclosure with no			
	<u>CVE-2023-35694</u>	google - android	additional execution privileges needed. User interaction is not needed for exploitation.	2023-07-13	7.5	High
			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			

		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			
	sap - multiple	network, extending the scope of impact, causing a limited impact			
<u>CVE-2023-35874</u>	products	on confidentiality, integrity and availability.	2023-07-11	7.4	High
		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 RX1511 (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			
	siemens -	support insecure TLS 1.0 protocol. An attacker could achieve a			
	ruggedcom_rox_m	man-in-the-middle attack and compromise confidentiality and			
CVE-2023-36749	x5000_firmware	integrity of data.	2023-07-11	7.4	High
	microsoft - multiple				
CVE-2023-21526	products	Windows Netlogon Information Disclosure Vulnerability	2023-07-11	7.4	High
		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 - multiple	Cisco has not released and will not release software updates that			
CVE-2023-20185	products	address this vulnerability.	2023-07-12	7.4	High
		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			
	sap - multiple	the resource. Furthermore, a standard template could be deleted,			
CVE-2023-35870	products	hence making the resource temporarily unavailable.	2023-07-11	7.3	High
	microsoft - multiple				
CVE-2023-32054	· · · - In . · · ·	Volume Shadow Copy Elevation of Privilege Vulnerability			Liah
	products		2023-07-11	7.3	High
	products	SAP Solution Manager (Diagnostics agent) - version 7.20, allows an	2023-07-11	7.3	підії
	products	SAP Solution Manager (Diagnostics agent) - version 7.20, allows an attacker to tamper with headers in a client request. This misleads	2023-07-11	7.3	підп
		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	2023-07-11	7.3	підн
	sap -	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			
<u>CVE-2023-36921</u>		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 2023-07-11	7.3	High
<u>CVE-2023-36921</u>	sap -	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. SAP Solution Manager (Diagnostics agent) - version 7.20, allows an			
<u>CVE-2023-36921</u>	sap -	 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. SAP Solution Manager (Diagnostics agent) - version 7.20, allows an unauthenticated attacker to blindly execute HTTP requests. On 			
<u>CVE-2023-36921</u>	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. 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 			
	sap - solution_manager sap -	 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. 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 			High
<u>CVE-2023-36921</u> <u>CVE-2023-36925</u>	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. 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 	2023-07-11	7.2	
<u>CVE-2023-36921</u> <u>CVE-2023-36925</u>	sap - solution_manager sap -	 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. 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
	sap - solution_manager sap -	 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. 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. An improper neutralization of special elements used in an OS 	2023-07-11	7.2	High
<u>CVE-2023-36925</u>	sap - solution_manager sap - solution_manager fortinet - multiple	 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. 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. 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 	2023-07-11 2023-07-11	7.2	High High
<u>CVE-2023-36925</u>	sap - solution_manager 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. 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. 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
<u>CVE-2023-36925</u>	sap - solution_manager sap - solution_manager fortinet - multiple	 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. 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. 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. A vulnerability has been identified in RUGGEDCOM ROX MX5000 	2023-07-11 2023-07-11	7.2	High High
<u>CVE-2023-36925</u>	sap - solution_manager sap - solution_manager fortinet - multiple	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. 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. 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. A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions	2023-07-11 2023-07-11	7.2	High High
	sap - solution_manager sap - solution_manager fortinet - multiple	 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. 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. 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. A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), 	2023-07-11 2023-07-11	7.2	High High
<u>CVE-2023-36925</u>	sap - solution_manager sap - solution_manager fortinet - multiple	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. 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. 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. 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	2023-07-11 2023-07-11	7.2	High High
<u>CVE-2023-36925</u>	sap - solution_manager sap - solution_manager fortinet - multiple	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. 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. 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. 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	2023-07-11 2023-07-11	7.2	High High
<u>CVE-2023-36925</u>	sap - solution_manager sap - solution_manager fortinet - multiple	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. 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. 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. 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 <	2023-07-11 2023-07-11	7.2	High High
<u>CVE-2023-36925</u>	sap - solution_manager sap - solution_manager fortinet - multiple	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. 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. 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. 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 RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0),	2023-07-11 2023-07-11	7.2	High High
<u>CVE-2023-36925</u>	sap - solution_manager sap - solution_manager fortinet - multiple	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. 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. 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. A vulnerability has been identified in RUGGEDCOM ROX MX50000 (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	2023-07-11 2023-07-11	7.2	High High
<u>CVE-2023-36925</u>	sap - solution_manager sap - solution_manager fortinet - multiple	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. 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. 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. A vulnerability has been identified in RUGGEDCOM ROX MX50000 (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	2023-07-11 2023-07-11	7.2	High High
<u>CVE-2023-36925</u>	sap - solution_manager sap - solution_manager fortinet - multiple	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. 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. 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. A vulnerability has been identified in RUGGEDCOM ROX MX50000 (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	2023-07-11 2023-07-11	7.2	High High
<u>CVE-2023-36925</u>	sap - solution_manager sap - solution_manager fortinet - multiple	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. 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. 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. 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), RUGGEDCOM ROX RX5000 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (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	2023-07-11 2023-07-11	7.2	High High
<u>CVE-2023-36925</u>	sap - solution_manager sap - solution_manager fortinet - multiple products	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. 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. 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. 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	2023-07-11 2023-07-11	7.2	High High

		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 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			
	siemens -	due to missing server side input sanitation. This could allow an			
	ruggedcom_rox_m	authenticated privileged remote attacker to execute arbitrary			
CVE-2023-36751	x5000 firmware	code with root privileges.	2023-07-11	7.2	High
		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			
	siemens -	injection due to missing server side input sanitation. This could			
	ruggedcom_rox_m	allow an authenticated privileged remote attacker to execute			
<u>CVE-2023-36752</u>	x5000_firmware	arbitrary code with root privileges.	2023-07-11	7.2	High
		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			
	siemens -	injection due to missing server side input sanitation. This could			
	ruggedcom_rox_m	allow an authenticated privileged remote attacker to execute			
CVE-2023-36753	x5000_firmware	arbitrary code with root privileges.	2023-07-11	7.2	High
		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			
	siemens -	command injection due to missing server side input sanitation.			
	ruggedcom_rox_m	This could allow an authenticated privileged remote attacker to		_	
<u>CVE-2023-36754</u>	x5000_firmware	execute arbitrary code with root privileges.	2023-07-11	7.2	High
	1	A vulnerability has been identified in RUGGEDCOM ROX MX5000			
		,			
		(All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions			
		(All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0),			
		(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			
		(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 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 <			
		(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),			
		(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			
		(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), 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			
		(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			
	siemens -	(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			
	ruggedcom_rox_m	(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			
<u>CVE-2023-36755</u>	ruggedcom_rox_m x5000_firmware	(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	2023-07-11	7.2	High
<u>CVE-2023-36755</u> <u>CVE-2023-32033</u>	ruggedcom_rox_m x5000_firmware microsoft - multiple products	(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 2023-07-11	7.2	High
	ruggedcom_rox_m x5000_firmware microsoft - multiple	(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.			
<u>CVE-2023-32033</u>	ruggedcom_rox_m x5000_firmware microsoft - multiple products microsoft - multiple	(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. <u>Microsoft Failover Cluster Remote Code Execution Vulnerability</u> Windows Active Directory Certificate Services (AD CS) Remote	2023-07-11	7.2	High
<u>CVE-2023-32033</u>	ruggedcom_rox_m x5000_firmware microsoft - multiple products microsoft - multiple	(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. <u>Microsoft Failover Cluster Remote Code Execution Vulnerability</u> Windows Active Directory Certificate Services (AD CS) Remote	2023-07-11	7.2	High
<u>CVE-2023-32033</u>	ruggedcom_rox_m x5000_firmware microsoft - multiple products microsoft - multiple products	(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. <u>Microsoft Failover Cluster Remote Code Execution Vulnerability</u> Windows Active Directory Certificate Services (AD CS) Remote	2023-07-11	7.2	High
<u>CVE-2023-32033</u>	ruggedcom_rox_m x5000_firmware microsoft - multiple products microsoft - multiple	(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. <u>Microsoft Failover Cluster Remote Code Execution Vulnerability</u> Windows Active Directory Certificate Services (AD CS) Remote	2023-07-11	7.2	High

	1			1	1
		Injection') vulnerability exists that could cause remote code execution when an admin user on DCE			
		uploads or tampers with install			
		packages.			
		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			
	schneider-electric -	tampers with backups which			
	struxureware_data	are then manually restored.			
<u>CVE-2023-37199</u>	_center_expert	there is a possible out of bounds read due to a missing bounds	2023-07-12	7.2	High
		check. This could lead to remote denial of service with System			
		execution privileges needed. User interaction is not needed for			
CVE-2023-35691	google - android	exploitation.	2023-07-13	7.2	High
		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			
CVE-2023-33990	sap - sql_anywhere	Windows. Other platforms are not impacted.	2023-07-11	7.1	High
	microsoft - multiple				
<u>CVE-2023-35347</u>	products	Microsoft Install Service Elevation of Privilege Vulnerability	2023-07-11	7.1	High
		A missing permission check in Jenkins Orka by MacStadium Plugin			
		1.33 and earlier allows attackers with Overall/Read permission to			
	jenkins -	connect to an attacker-specified URL using attacker-specified			
CVE 2022 27040	orka_by_macstadiu	credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2022 07 12	7 1	Lliab
<u>CVE-2023-37949</u>	m	A missing permission check in Jenkins ElasticBox Cl Plugin 5.0.1	2023-07-12	7.1	High
		and earlier allows attackers with Overall/Read permission to			
		connect to an attacker-specified URL using attacker-specified			
	jenkins -	credentials IDs obtained through another method, capturing			
CVE-2023-37965	elasticbox_ci	credentials stored in Jenkins.	2023-07-12	7.1	High
	microsoft - multiple			_	
<u>CVE-2023-32050</u>	products	Windows Installer Elevation of Privilege Vulnerability	2023-07-11	7	High
	microsoft - malware_protectio				
CVE-2023-33156	n_engine	Microsoft Defender Elevation of Privilege Vulnerability	2023-07-11	7	High
	microsoft - multiple			-	
CVE-2023-35360	products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7	High
	microsoft - multiple				
CVE-2023-35361	products	Windows Kernel Elevation of Privilege Vulnerability	2023-07-11	7	High
		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 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			
	siemens -	attacker in a man-in-the-middle position to read and modify any data			
	ruggedcom_rox_m				
<u>CVE-2023-36748</u>	x5000_firmware	passed over to and from the affected device.	2023-07-11	6.8	Medium
	microsoft -				
	windows_admin_ce				
<u>CVE-2023-29347</u>	nter	Windows Admin Center Spoofing Vulnerability	2023-07-11	6.8	Medium
0.00	microsoft - multiple				
<u>CVE-2023-32043</u>	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
<u>UVE-2023-35332</u>	products microsoft - multiple	windows Remote Desktop Protocol Security Feature Bypass	2023-07-11	0.ð	iviedium
CVE-2023-32055	products	Active Template Library Elevation of Privilege Vulnerability	2023-07-11	6.7	Medium
<u></u>		In multiple functions of io uring.c, there is a possible kernel	11	0.7	
		memory corruption due to improper locking. This could lead to			
		local escalation of privilege in the kernel with System execution			
CVE-2023-21400	google - android	privileges needed. User interaction is not needed for exploitation.	2023-07-13	6.7	Medium
0.00		In incfs_kill_sb of fs/incfs/vfs.c, there is a possible memory			
CVE-2023-35693	google - android	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.			
	microsoft - multiple	User interaction is not needed for exploitation.			
<u>CVE-2023-35310</u>	products	Windows DNS Server Remote Code Execution Vulnerability	2023-07-11	6.6	Medium
<u>CVE-2023-35344</u>	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	2023-07-11	6.6	Medium
<u>CVE-2023-35345</u>	microsoft - multiple products microsoft - multiple	Windows DNS Server Remote Code Execution Vulnerability	2023-07-11	6.6	Medium
<u>CVE-2023-35346</u>	products microsoft - multiple	Windows DNS Server Remote Code Execution Vulnerability Windows Active Directory Certificate Services (AD CS) Remote	2023-07-11	6.6	Medium
<u>CVE-2023-35351</u>	products	Code Execution Vulnerability	2023-07-11	6.6	Medium
<u>CVE-2023-28955</u>	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
	ibm - multiple	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			
<u>CVE-2023-29256</u>	products	federation features are used. IBM X-Force ID: 252046. The SAP BW BICS communication layer in SAP Business Warehouse	2023-07-10	6.5	Medium
	sap - multiple	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			
CVE-2023-33992	products	level. The missing check only affects the data level.	2023-07-11	6.5	Medium
	sap - netweaver_process	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			
<u>CVE-2023-35872</u>	_integration	limited impact on confidentiality and availability of the application. The Runtime Workbench (RWB) of SAP NetWeaver Process	2023-07-11	6.5	Medium
	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			
CVE-2023-35873 CVE-2023-24881	_integration microsoft - teams	limited impact on confidentiality and availability of the application. Microsoft Teams Information Disclosure Vulnerability	2023-07-11 2023-07-11	6.5 6.5	Medium Medium
<u> </u>	fortinet - multiple	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	2023 07 11	0.5	mediam
<u>CVE-2023-25606</u>	products microsoft - multiple	underlying filesystem via specially crafted web requests. Windows Layer-2 Bridge Network Driver Information Disclosure	2023-07-11	6.5	Medium
<u>CVE-2023-32037</u>	products microsoft - multiple	Vulnerability	2023-07-11	6.5	Medium
<u>CVE-2023-33151</u>	products microsoft - multiple	Microsoft Outlook Spoofing Vulnerability	2023-07-11	6.5	Medium
<u>CVE-2023-33164</u>	products microsoft - multiple	Remote Procedure Call Runtime Denial of Service Vulnerability Microsoft PostScript and PCL6 Class Printer Driver Information	2023-07-11	6.5	Medium
<u>CVE-2023-35296</u>	products microsoft - multiple	Disclosure Vulnerability	2023-07-11	6.5	Medium
<u>CVE-2023-35308</u>	products microsoft - multiple	Windows MSHTML Platform Security Feature Bypass Vulnerability	2023-07-11	6.5	Medium
<u>CVE-2023-35314</u>	products microsoft - multiple	Remote Procedure Call Runtime Denial of Service Vulnerability Remote Procedure Call Runtime Information Disclosure	2023-07-11	6.5	Medium
<u>CVE-2023-35316</u>	products microsoft - multiple	Vulnerability	2023-07-11	6.5	Medium
<u>CVE-2023-35318</u>	products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	6.5	Medium
<u>CVE-2023-35319</u>	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-07-11	6.5	Medium
<u>CVE-2023-35321</u>	microsoft - multiple products	Windows Deployment Services Denial of Service Vulnerability	2023-07-11	6.5	Medium
<u>CVE-2023-35329</u>	microsoft - multiple products	Windows Authentication Denial of Service Vulnerability	2023-07-11	6.5	Medium
<u>CVE-2023-35331</u>	microsoft - multiple products	Windows Local Security Authority (LSA) Denial of Service Vulnerability	2023-07-11	6.5	Medium
<u>CVE-2023-35348</u>	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

	microsoft - multiple				
CVE-2023-36871	products	Azure Active Directory Security Feature Bypass Vulnerability	2023-07-11	6.5	Medium
		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			
CVE-2022-46651	apache - airflow	removed the vulnerability.	2023-07-12	6.5	Mediur
		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			
CVE-2023-22887	apache - airflow	version that is not affected	2023-07-12	6.5	Mediun
		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.			
CVE-2023-22888	apache - airflow	It is recommended to upgrade to a version that is not affected	2023-07-12	6.5	Mediun
		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.			
	apache - multiple	3.0 Pulsar Broker users are unaffected. Any users running the Pulsar Broker for 2.8.* and earlier should			
CVE-2023-31007	products	upgrade to one of the above patched versions.	2023-07-12	6.5	Mediun
		Apache Airflow, versions before 2.6.3, is affected by a vulnerability			
		that allows unauthorized read access to a DAG through the URL. It			
CVE-2023-35908	apache - airflow	is recommended to upgrade to a version that is not affected Apache Airflow, versions before 2.6.3, has a vulnerability where an	2023-07-12	6.5	Medium
		authenticated user can use crafted input to make the current			
		request hang. It is recommended to upgrade to a version that is			
<u>CVE-2023-36543</u>	apache - airflow	not affected	2023-07-12	6.5	Mediun
		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 Pulsar Function worker users should upgrade to at least 2.11.1.			
		3.0 Pulsar Function Worker users are unaffected.			
	apache - multiple	Any users running the Pulsar Function Worker for 2.9.* and earlier		a -	
<u>CVE-2023-37579</u>	products	should upgrade to one of the above patched versions. The session restore helper crashed whenever there was no	2023-07-12	6.5	Mediun
		parameter sent to the message handler. This vulnerability affects			
CVE-2023-37456	mozilla - firefox	Firefox for iOS < 115.	2023-07-12	6.5	Mediun
	jenkins -	Jenkins External Monitor Job Type Plugin 206.v9a_94ff0b_4a_10			
CVE-2023-37942	external_monitor_j	and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2023-07-12	6.5	Mediun
<u>UVL-2023-3/342</u>	ob_type	A missing permission check in Jenkins Datadog Plugin 5.4.1 and	2023-07-12	0.5	ivieulun
		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.			
<u>CVE-2023-37951</u>	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
		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			
CVE-2023-37952	jenkins - mabl	obtained through another method, capturing credentials stored in Jenkins.	2023-07-12	6.5	Mediun
		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			
CVE-2023-37953	jenkins - mabl	IDs obtained through another method, capturing credentials stored in Jenkins.	2023-07-12	6.5	Mediun
	-	A cross-site request forgery (CSRF) vulnerability in Jenkins Test			
	jenkins - test_results_aggreg	Results Aggregator Plugin 1.2.13 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified			
<u>CVE-2023-37955</u>	ator	credentials.	2023-07-12	6.5	Mediun
	jenkins -	A missing permission check in Jenkins Test Results Aggregator Plugin 1.2.13 and earlier allows attackers with Overall/Read			
CVE-2023-37956	test_results_aggreg ator	permission to connect to an attacker-specified URL using attacker- specified credentials.	2023-07-12	6.5	Mediun
<u>CVL-2023-37930</u>	jenkins -	A missing permission check in Jenkins Sumologic Publisher Plugin	2023-07-12	0.5	weului
CVE-2023-37959	sumologic_publishe r	2.2.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL.	2023-07-12	6.5	Mediun
	jenkins -	Jenkins MathWorks Polyspace Plugin 1.0.5 and earlier allows			
<u>CVE-2023-37960</u>	mathworks_polysp ace	attackers with Item/Configure permission to send emails with arbitrary files from the Jenkins controller file systems.	2023-07-12	6.5	Mediun
		Path Traversal vulnerability in GMS and Analytics allows an			
	sonicwall - multiple	authenticated attacker to read arbitrary files from the underlying filesystem with root privileges. This issue affects GMS: 9.3.2-SP1			
<u>CVE-2023-34125</u>	products	and earlier versions; Analytics: 2.5.0.4-R7 and earlier versions. Path Traversal vulnerability in SonicWall GMS and Analytics allows	2023-07-13	6.5	Mediur
		a remote authenticated attacker to read arbitrary files from the			
	sonicwall - multiple	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			
<u>CVE-2023-34135</u>	products	versions.	2023-07-13	6.5	Mediun
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	Mediur
	p	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			
<u>CVE-2023-33988</u>	sap - enable_now	information. In SAP Enable Now - versions WPB_MANAGER 1.0,	2023-07-11	6.1	Mediur
		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			
CVE-2023-36918	sap - enable_now	Scripting, which could result in disclosure or modification of information.	2023-07-11	6.1	Mediun
		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			
	siemens -				
<u>CVE-2023-36386</u>	ruggedcom_rox_m x5000_firmware	"invalid params element name" error on the get_elements parameters.	2023-07-11	6.1	Mediur
		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),			
	siemens	RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM			
	siemens - ruggedcom_rox_m	ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions <			
CVE-2023-36389	x5000_firmware	V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0),	2023-07-11	6.1	Mediun

CVE 2023-2021 CVE 2000, Provide consists of the affect of publication that coole allow an attacker to execute malitous javariet code when emaility exists in the web interface of the affect of publication that coole allow an attacker to execute malitous javariet code when emaility exists in the web interface of the affect of publication "mouting public error. Image: CVE 2002, PUBLICATION PUBLICATION PUBLICATION PUBLICATION PUBLICATION Publication exists in the web interface of the affect of publication (VIII wearing v VIII able to exist in the value interface of the affect of publication (VIII wearing v VIIII able to exist in the value interface of the affect of publication (VIII wearing v VIIII able to exist in the value interface of the affect of publication (VIII wearing v VIIII able to exist in the value interface of the affect of publication (VIIII wearing v VIIII able to exist in the value interface of the affect of publication (VIIII wearing v VIIII able to exist in the value interface of the affect of publication (VIIIII wearing v VIIII able to exist in the value interface of the affect of publication (VIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII			RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000			
UP: 2023 2034 bit status and status			(All versions < V2.16.0). A reflected cross-site scripting (XSS)			
Value is reflected visuality and is reflected in the response without satistation while throwing an involution in BUGGEDDDM RX MODE visuality and involution in BUGGEDDDM RX MODE VEX.100.1 A vulnerability has been involution in BUGGEDDDM RX MODE visuality and involution in BUGGEDDDM RX MODE visuality and involution in BUGGEDDDM RX MODE VEX.100.1 A vulnerability has been involution in BUGGEDDDM RX MODE visuality and involution in BUGGEDDDM RX MODE visuality and involution in BUGGEDDDM RX MODE VEX.100.1 A vulnerability in BUGGEDDM RX MODE visuality and involution in BUGGEDDM RX MODE visuality and involution in BUGGEDDM RX MODE VEX.100.1 A vulnerability in BUGGEDDM RX MODE visuality and involution in BUGGEDDM RX MODE visuality and involution in BUGGEDDM RX MODE VEX.2023.0001 BUGGEDDM RX MODE visuality and involution in BUGGEDDM RX MODE visuality and involution in BUGGEDDM RX MODE VEX.2023.0001 BUGGEDDM RX MODE visuality and involution in BUGGEDDM RX MODE visuality and involution in BUGGEDDM RX MODE VEX.2023.0001 BUGGEDDM RX MODE visuality and involution in BUGGEDDM RX MODE visuality and involution in BUGGEDDM RX MODE VEX.2023.0001 BUGGEDDM RX MODE visuality and involution in BUGGEDDM RX MODE visuality and involutin And involutin And involution in PUGGEDDM RX MODE <td></td> <td></td> <td>that could allow an attacker to execute malicious javascript code</td> <td></td> <td></td> <td></td>			that could allow an attacker to execute malicious javascript code			
cviewality exists viewality has been identified in RUGGECOM NOX MOSDOD (viewality exists) viewality has been identified in RUGGECOM NOX MOSDOD (viewality exists) viewality has been identified in RUGGECOM NOX MOSDOD (viewality exists) viewality has been identified in RUGGECOM NOX MOSDOD (viewality exists) viewality is a second of the second						
cv1_2023_2010 cv1_2 6.0, NUGGEDCOM ROX NASSODIE (AI versions < V.2.6.0), RUGGEDCOM ROX NASSODIE (AI VERSIONE), RUGGEDCOM ROX NASSODIE (RUGGEDCOM ROX NASSODIE			, , ,			
ruggedom		siemens -	(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			
microsoft: multiple Microsoft Dynamics 365 (on-premises) Cross-site Scripting 2023-07-11 6.1 Medium CVE-2023-33171 inviting Junkins OpenShift Login Plugin 1.1.0227.v370808/h. Ja. 20 and earlier improperly determines that a redict UBL affe login is leptimately pointing to lenkins, allowing attackers to perform 2023-07-12 6.1 Medium CVE-2023-37947 openShift Login helicectal XSS attacks, also known as non-persistent attacks, occur when a maliclous scripts is reflected off a web application to the vicit in Storwarr. The script sci activated through a link, which sends a request to a website with a vulnerability that enables 2023-07-13 6.1 Medium CVE-2023-29455 zabbix - multiple products Reflected XSS attacks, occur when a malicious scripts. 2023-07-13 6.1 Medium CVE-2023-29457 Products Reflected XSS attacks, occur when a malicious scripts. 2023-07-13 6.1 Medium CVE-2023-29457 Products Reflected XSS attacks, occur when a malicious scripts. 2023-07-13 6.1 Medium CVE-2023-29457 Products Reflected XSS attacks, occur when a malicious scripts. 2023-07-13 6.1 Medium CVE-2023-292470 Products Reflected XSS attackere out and attacker to a						
CVF-2023-3317 products Vulnerability	<u>CVE-2023-36390</u>	—	·	2023-07-11	6.1	Medium
cvF=2023-37947 jenkins - legitimately pointing to lenkins, allowing attackers to perform phishing attacks. 2023-07-12 6.1 Medium cvF=2023-37947 openshift_login Reflected XS5 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 secution of malicious script is reflected off a web application to the victim's browser. The script is activated through a link, which secution of malicious script is reflected off a web application to the victim's browser. The script is an Berline activated through Action form fields, which can be sent as request abbix - multiple 2023-07-13 6.1 Medium cvF=2023-29457 products Reflected XS 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 abbix - multiple 5.1 Medium cvF=2023-29457 products A vulnerability in Cisco BroadWorks could allow an authenticated, device. 2023-07-13 6.1 Medium cvF=2023-29457 products The vulnerability is due to insufficient input validation by the operating system CLI. An attacker to execute commands as the root user. To exploit this vulnerability, an attacker must have valid exploit could allow the tattacker to execute commands and haves performs the connection test to Active directory unencrypted, allowing attackers able to captive metwork traffits between the lenkins controller and Active Directory servers	<u>CVE-2023-33171</u>	•	Vulnerability	2023-07-11	6.1	Medium
CVE-2023-37947 Ignitinately pointing to lenkins, allowing attackers to perform openshift login Iegitimately pointing to lenkins, allowing attackers to perform when a malicious script is reflected off a web application to the victim's torower. The script is activated through allink, which arabbix - multiple Reflected XSS attacks, also known as non-persistent attacks, occur when a malicious script is reflected off a web application to the victim's torower. The script is activated through allink, which arabbix - multiple 2023-07-12 6.1 Medium CVE-2023-29452 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 activated through Action form fields, which can be sent as request activated through action form fields, which can be sent as request activated through action form fields, which can be sent as request activated through action form fields, which can be sent as request activated through action form fields, which can be sent as request activated through action form fields, which can be sent as request activated through allow the attacker could exploit this vulnerability by using a crafted command to the affected system. Assuccessful exploit could allow the attacker rough activater must have valid activate activater must have valid approxemants as the root user. The script system CLI. An attacker must have valid approxemants able to activate active must have valid approxemants able to activate active must have valid approxemants able to activate must have valid approxemants able to activate active active active active active active directory active directory unercrypted, allowing attackers able to active directory unencrypted, allowing attackers able to active approxeman						
CVE-2023-29452 Eeffected 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 2023-07-13 6.1 Medium CVE-2023-29452 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 a attacked through Action form fields, which can be sent as request to a website with a vulnerability in Cisco BroadWorks could allow an authenticated, local attacker to elevate privileges to the root user on an affected device. 2023-07-13 6.1 Medium CVE-2023-29457 products A vulnerability in Cisco BroadWorks could allow an authenticated, local attacker to elevate privileges to the root user on an affected device. 2023-07-12 6 Medium CVE-2023-20210 products The vulnerability in Cisco BroadWorks could allow an authenticated, local attacker to execute commands to the affected system. Assucces/ful exploit could allow the attacker to execute commands as the root user. To exploit this vulnerability in Cisco BroadWorks administrative privileges on the affected device. 2023-07-12 6 Medium CVE-2023-37943 ipenkins - corepiol this vulnerability in Cisco BroadWorks administrative privileges on the affected device. 2023-07-12 5 Medium		jenkins -				
cvtr.2023-29455 when a malicious script is reflected off a web application to the victim's browser. The script is activated through a hink, which sends a request to a website with a vulnerability that enables execution of malicious scripts. 2023-07-13 6.1 Medium CVE-2023-29455 products execution of malicious scripts. 2023-07-13 6.1 Medium CVE-2023-29457 products Reflected XS3 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 sen as request to a website with a vulnerability, which can be sen as request to a website with a vulnerability is cue to an affected device. 2023-07-13 6.1 Medium CVE-2023-29457 products A vulnerability is cue to insufficient input validation by the operating system CLL 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, and tacker must have valid exploit could allow the attacker to exclue device. 2023-07-12 6 Medium CVE-2023-20210 products Jenkins Active Directory Pulgin Z30 and earlier ignores the "Require TLS" and "startTIs" 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 recelentials. 2023-07-12 5	<u>CVE-2023-37947</u>	openshift_login		2023-07-12	6.1	Medium
zabbix - multiple sends a request to a website with a vulnerability that enables 2023-07-13 6.1 Medium CVE-2023-29455 products execution of malicious scripts. 2023-07-13 6.1 Medium zabbix - multiple Reflected XSS attacks, occur when a malicious scripts. 2023-07-13 6.1 Medium CVE-2023-29457 products a website with a vulnerability that enables execution of 2023-07-13 6.1 Medium CVE-2023-29457 products malenticitation to the victim's browser. The script can be as requested to a website with a vulnerability to Cisco BroadWorks could allow an authenticated, locid attacker to elevate privileges to the root user on an affected device. 6.1 Medium CVE-2023-20210 The vulnerability is due to insufficient input validation by the operating system CLL An attacker could exploit this vulnerability by issuing a crafted command to the affected system. A successful 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 on a affected device. 2023-07-12 6 Medium CVE-2023-20210 products BroadWorks administrative privileges on the affected device. 2023-07-12 5.9 Medium CVE-2023-20210 products BroadWorks admi						
CVE-2023-29455 products execution of malicious scripts. 2023-07-13 6.1 Medium 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 website with a vulnerability that enables execution of malicious scripts. 2023-07-13 6.1 Medium CVE-2023-29457 products a vebsite with a vulnerability that enables execution of malicious scripts. 2023-07-13 6.1 Medium CVE-2023-29457 products A vulnerability in Cisco BroadWorks could allow an authenticated, local attacker to elevate privileges to the root user on an affected device. 2023-07-13 6.1 Medium CVE-2023-20210 The vulnerability is due to insufficient input validation by the operating system CLL An attacker could exploit this vulnerability. By issing 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 mus have valid graduers TS' and StartTS' options and always performs the connection test to Active Directory Pungin 2.30 and earlier ignores the "Require TS' and Active Directory servers to obtain Active Directory controller and Active Directory revers to obtain Active Directory controller and Active Directory revers to fotain Active Director						
CVE-2023-29457 Reflected XSS attack, 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 products 2023-07-13 6.1 Medium CVE-2023-29457 Products A vulnerability in Cisco BroadWorks could allow an authenticated, local attacker to elevate privileges to the root user on an affected device. 2023-07-13 6.1 Medium CVE-2023-20210 The vulnerability is due to insufficient input validation by the operating system CLL 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 users. To exploit this vulnerability, an attacker must have valid BroadWorks administrative privileges on the affected device. 2023-07-12 6 Medium CVE-2023-20210 Frequire TLS' and "StarTIIs" options and always performs the connection test to Active directory unencrypted, allowing attackers able to capture network traffic between the lenkins controller and Active Directory servers to obtain Active Directory creentials. 2023-07-12 5.9 Medium CVE-2023-20426 microsoft - multiple products Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability 2023-07-11 5.5 Medium CVE-2023-32039 microsoft - multiple products Microsoft PostScript a	CVE-2023-29455			2023-07-13	6.1	Medium
cvt-2023-29457zabbix - multiple productsactivated through Action form fields, which can be sent as request to a website with a vulnerability that enables execution of malicious scripts.2023-07-136.1MediumCvt-2023-29457productsA vulnerability in Cisco Broad/Works could allow an authenticated, local attacker to elevate privileges to the root user on an affected device.2023-07-136.1MediumCvt-2023-20210The 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.2023-07-126MediumCvtE-2023-20210productsBroadWorks administrative privileges on the affected device.2023-07-125.9MediumCvtE-2023-30943active_directoryactive_directory Pugnica.3.0 and earline inforems the controller and Active Directory servers to obtain Active Directory unerry tervers to obtain Active Directory products5.9MediumCvtE-2023-37943active_directoryNulnerability has been identified in Citrix Workspace app for Linux that, if exploited, may result in a malicious local user borg abie to gain access to the Citrix Virtual Apps and Desktops session of another user who is using the same computer from which the products2023-07-105.5MediumCvtE-2023-32040microsoft - multiple productsMicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerabili			Reflected XSS attacks, occur when a malicious script is reflected off			
CVE-2023-29457zabbix - multiple productsto a website with a vulnerability that enables execution of malicious scripts.2023-07-136.1MediumA vulnerability in Cisco BroadWorks could allow an authenticated, local attacker to elevate privileges to the root user on an affected device.2023-07-136.1MediumCVE-2023-20420The vulnerability in Cisco BroadWorks could allow an authenticated, local attacker to elevate privileges to the root user on an affected device.5.5MediumCVE-2023-20210productsThe vulnerability is due to insufficient input validation by the operating system CLI. An attacker to execute commands as the root user. To exploit this vulnerability, an attacker must have valid user. To exploit this vulnerability, an attacker must have valid exploit could allow the attacker to execute commands as the root user. To exploit this vulnerability. an attacker and havas performs the "Require TLS" and "StartTIS" options and always performs the connection test to Active directory unencrypted, allowing attackers able to capture network traffic between the lenkins controller and Active Directory Plugin 2.30 and beating sports attackers able to capture network traffic between the lenkins controller and Active Directory errest to adlows performs the controller and Active Directory errest to ablain Active Directory2023-07-125.9MediumCVE-2023-20406A vulnerability has been identified in Citrix Workspace app for Linux that, if exploited, may result in a malicous local user being able to gain access to the Citrix Virtual Apps and Desktops session of another user who is using the same computer information2023-07-115.5MediumCVE-2023-32049productsDisclosu						
CVE-2023-20210 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-2023-20210 products BroadWorks administrative privileges on the affected device. 2023-07-12 6 Medium "Require TLS" and "StartTIS" options and always performs the connection test to Active directory unencrypted, allowing attackers able to capture network traffic between the lenkins controller and Active Directory servers to obtain Active Directory credentials. 2023-07-12 5.9 Medium CVE-2023-37943 active_directory redentials. 2023-07-10 5.5 Medium CVE-2023-24486 citrix - workspace incrosoft - multiple Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability 2023-07-11 5.5 Medium microsoft - multiple Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability 2023-07-11 5.5 Medium cvE-2023-32040 <td< td=""><td></td><td>zabbix - multiple</td><td></td><td></td><td></td><td></td></td<>		zabbix - multiple				
CVE-2023-2020 Iocal attacker to elevate privileges to the root user on an affected device. Intervalue and the privileges to the root user on an affected device. Intervalue and the privileges to the root user on an affected device. Intervalue and the privileges to the root user on an affected operating system CLI. An attacker could exploit this vulnerability by issuing a crafted command to the affected system. Asuccessful exploit could allow the attacker to execute commands as the root user. To exploit this vulnerability, an attacker must have valid 2023-07-12 6 Medium CVE-2023-20210 products BraadWorks administrative privileges on the affected device. 2023-07-12 6 Medium CVE-2023-20210 products BraadWorks administrative privileges on the affected device. 2023-07-12 6 Medium CVE-2023-20210 products Inkins Active Directory Pluging. 3.3 and aderalier ignores 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 2023-07-12 5.9 Medium CVE-2023-37943 active_directory 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 device. S.9 Medium CVE-2023-3	<u>CVE-2023-29457</u>	products		2023-07-13	6.1	Medium
cvE-2023-20210operating 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.2023-07-126MediumCVE-2023-20210productsJenkins Active Directory Plugin 2.30 and earlier ignores the "Require TLS" and "StartTIs" options and always performs the connection test to Active Directory unencrypted, allowing attacker able to capture network traffic between the Jenkins attacker able to capture network traffic between the Jenkins attacker able to capture network traffic between the Jenkins controller and Active Directory servers to obtain Active Directory controller and Active Directory servers to obtain Active Directory atticker sable to gain access to the 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 Disclosure Vulnerability and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-105.5MediumCVE-2023-32040microsoft - multiple Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-32041microsoft - multiple Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-32041microsoft - multiple Microsoft PostScript and PCL6 Class Printer Driver Information Uvlnerability2023-07-115.5MediumCVE			local attacker to elevate privileges to the root user on an affected			
CVE-2023-24486A 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.2023-07-105.5MediumCVE-2023-24486citrix - workspaceMicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-32039productsMicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-32040productsMicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-32041microsoft - multiple productsMicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure2023-07-115.5MediumCVE-2023-32041productsWindows Update Orchestrator Service Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-32045productsMicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-32085productsMicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-33162productsMicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-33174productsMicrosoft Excel Information Disclo		products jenkins -	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. Jenkins Active Directory Plugin 2.30 and earlier ignores the "Require TLS" and "StartTIs" 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			
cVE-2023-24486able 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.2023-07-105.5MediumcVE-2023-24486citrix - workspaceICA session is launched.2023-07-105.5MediumcVE-2023-32039productsDisclosure Vulnerability2023-07-115.5MediumcVE-2023-32040productsDisclosure Vulnerability2023-07-115.5MediumcVE-2023-32041productsDisclosure Vulnerability2023-07-115.5MediumcVE-2023-32042productsDisclosure Vulnerability2023-07-115.5MediumcVE-2023-32041productsVindows Update Orchestrator Service Information Disclosure	<u>CVL 2020 07010</u>	uncetory		2023 07 12	5.5	Wealdin
CVE-2023-24486of another user who is using the same computer from which the ICA session is launched.2023-07-105.5Mediummicrosoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver Information2023-07-115.5MediumCVE-2023-32039productsDisclosure Vulnerability2023-07-115.5MediumCVE-2023-32040productsDisclosure Vulnerability2023-07-115.5MediumCVE-2023-32041productsDisclosure Vulnerability2023-07-115.5MediumCVE-2023-32041productsVulnerability2023-07-115.5MediumCVE-2023-32041productsVulnerability2023-07-115.5MediumCVE-2023-32041productsVulnerability2023-07-115.5MediumCVE-2023-32045productsVulnerability2023-07-115.5MediumCVE-2023-32045productsDisclosure Vulnerability2023-07-115.5MediumCVE-2023-32055productsDisclosure Vulnerability2023-07-115.5MediumCVE-2023-32056productsMicrosoft Excel Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-33162productsMicrosoft Excel Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-33174productsWindows Cryptographic Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver Information5.5Medi						
microsoft - multiple CVE-2023-32039Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-32040microsoft - multiple productsMicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-32040productsDisclosure Vulnerability2023-07-115.5Mediummicrosoft - multiple vulnerabilityWindows Update Orchestrator Service Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multiple vulnerabilityMicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-32085 productsmicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-32085 productsmicrosoft - multiple Disclosure Vulnerability2023-07-115.5MediumcVE-2023-33162 CVE-2023-33162Microsoft Excel Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multiple microsoft - multiple microsoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver Information5.5Mediummicrosoft - multiple microsoft - multipleMicrosoft Excel Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multiple microsoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver Information5.5Medium			- · · ·			
CVE-2023-32039productsDisclosure Vulnerability2023-07-115.5MediumMicrosoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver Information2023-07-115.5MediumCVE-2023-32040productsDisclosure Vulnerability2023-07-115.5Mediummicrosoft - multipleWindows Update Orchestrator Service Information Disclosure2023-07-115.5MediumCVE-2023-32041productsVulnerability2023-07-115.5Mediummicrosoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver InformationCVE-2023-32085productsDisclosure Vulnerability2023-07-115.5MediumCVE-2023-32085productsDisclosure Vulnerability2023-07-115.5MediumMicrosoft - multipleMicrosoft Excel Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-33162productsMicrosoft Excel Information Disclosure Vulnerability2023-07-115.5MediumMicrosoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver InformationCVE-2023-33162productsWindows Cryptographic Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-33174productsWindows Cryptographic Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver Informationmicrosoft - multipleMicrosoft PostScript and	<u>CVE-2023-24486</u>		ICA session is launched.	2023-07-10	5.5	Medium
microsoft - multiple productsMicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multiple productsWindows Update Orchestrator Service Information Disclosure Vulnerability2023-07-115.5MediumcVE-2023-32041productsVulnerability2023-07-115.5Mediummicrosoft - multiple productsMicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumcVE-2023-32085productsDisclosure Vulnerability2023-07-115.5MediumcVE-2023-33162productsMicrosoft Excel Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multiple productsMicrosoft Excel Information Disclosure Vulnerability2023-07-115.5MediumcVE-2023-33162productsMicrosoft Excel Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multiple microsoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver Information5.5Mediummicrosoft - multiple microsoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver Information5.5Mediummicrosoft - multiple microsoft - multipleWindows Cryptographic Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver Information5.5Medium	<u>CVE-20</u> 23-32039	•		2023-07-11	5.5	Medium
microsoft - multiple productsWindows Update Orchestrator Service Information Disclosure 2023-07-112023-07-115.5Mediummicrosoft - multiple productsMicrosoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-32085productsDisclosure Vulnerability2023-07-115.5Mediummicrosoft - multiple productsMicrosoft Excel Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-33162productsMicrosoft Excel Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multiple productsMicrosoft Excel Information Disclosure Vulnerability2023-07-115.5MediumCVE-2023-33174productsWindows Cryptographic Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multiple productsWindows Cryptographic Information Disclosure Vulnerability2023-07-115.5Medium		microsoft - multiple	Microsoft PostScript and PCL6 Class Printer Driver Information			
CVE-2023-32041productsVulnerability2023-07-115.5Mediummicrosoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver Information </td <td><u>CVE-2023-32040</u></td> <td></td> <td></td> <td>2023-07-11</td> <td>5.5</td> <td>Medium</td>	<u>CVE-2023-32040</u>			2023-07-11	5.5	Medium
CVE-2023-32085productsDisclosure Vulnerability2023-07-115.5Mediummicrosoft - multiplemicrosoft - multiple2023-07-115.5MediumCVE-2023-33162productsMicrosoft Excel Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multiplemicrosoft - multiple5.5MediumCVE-2023-33174productsWindows Cryptographic Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver Information5.5Medium	<u>CVE-2023-32041</u>	products	Vulnerability	2023-07-11	5.5	Medium
CVE-2023-33162productsMicrosoft Excel Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multipleproductsWindows Cryptographic Information Disclosure Vulnerability2023-07-115.5Mediummicrosoft - multipleMicrosoft PostScript and PCL6 Class Printer Driver InformationLossLossLoss	<u>CVE-2023-32085</u>	products		2023-07-11	5.5	Medium
CVE-2023-33174 microsoft - multiple Windows Cryptographic Information Disclosure Vulnerability 2023-07-11 5.5 Medium microsoft - multiple Microsoft PostScript and PCL6 Class Printer Driver Information Microsoft - multiple Microsoft PostScript and PCL6 Class Printer Driver Information	<u>CVE-2023-331</u> 62		Microsoft Excel Information Disclosure Vulnerability	2023-07-11	5.5	Medium
		microsoft - multiple products	Windows Cryptographic Information Disclosure Vulnerability			
	CVE-2023-35306	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	2023-07-11	5.5	Medium

CVE-2023-35326 m CVE-2023-35341 v CVE-2023-36872 v CVE-2023-30913 v CVE-2023-30913 v CVE-2023-30913 v CVE-2023-30913 v CVE-2023-30918 v CVE-2023-30919 v CVE-2023-30920 v	products nicrosoft - multiple products nicrosoft - multiple products microsoft - /p9_video_extensi ons google - multiple products google - multiple products google - multiple products google - multiple products	Disclosure VulnerabilityWindows CDP User Components Information Disclosure VulnerabilityMicrosoft DirectMusic Information Disclosure VulnerabilityMicrosoft DirectMusic Information Disclosure VulnerabilityIn telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-11 2023-07-11 2023-07-11 2023-07-11 2023-07-12 2023-07-12 2023-07-12	5.5 5.5 5.5 5.5 5.5 5.5	Medium Medium Medium Medium Medium Medium
CVE-2023-35326 m CVE-2023-35341 m CVE-2023-35341 v CVE-2023-36872 v CVE-2023-30913 v CVE-2023-30913 v CVE-2023-30913 v CVE-2023-30918 v CVE-2023-30919 v CVE-2023-30920 v	products nicrosoft - multiple products microsoft - /p9_video_extensi ons google - multiple products google - multiple products google - multiple products google - multiple products google - multiple products	VulnerabilityMicrosoft DirectMusic Information Disclosure VulnerabilityVP9 Video Extensions Information Disclosure VulnerabilityIn telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-07-11 2023-07-11 2023-07-12 2023-07-12 2023-07-12	5.5 5.5 5.5 5.5 5.5	Medium Medium Medium Medium
CVE-2023-35341 V CVE-2023-36872 CVE-2023-30913 CVE-2023-30918 CVE-2023-30919 CVE-2023-30920	products microsoft - /p9_video_extensi ons google - multiple products google - multiple products google - multiple products google - multiple products google - multiple products	VP9 Video Extensions Information Disclosure Vulnerability In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional	2023-07-11 2023-07-12 2023-07-12 2023-07-12	5.5 5.5 5.5 5.5	Medium Medium Medium Medium
CVE-2023-36872 CVE-2023-30913 CVE-2023-30918 CVE-2023-30919 CVE-2023-30920	<pre>/p9_video_extensi ons google - multiple products google - multiple products google - multiple products google - multiple products google - multiple products</pre>	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. 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 2023-07-12 2023-07-12	5.5 5.5 5.5	Medium Medium Medium
<u>CVE-2023-30913</u> <u>CVE-2023-30918</u> <u>CVE-2023-30919</u> <u>CVE-2023-30920</u>	products google - multiple products google - multiple products google - multiple products google - multiple products	could lead to local information disclosure with no additional execution privileges needed. In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional	2023-07-12 2023-07-12	5.5	Medium Medium
<u>CVE-2023-30918</u> <u>CVE-2023-30919</u> <u>CVE-2023-30920</u>	google - multiple products google - multiple products google - multiple products 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. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional	2023-07-12 2023-07-12	5.5	Medium Medium
<u>CVE-2023-30919</u> <u>CVE-2023-30920</u>	google - multiple products google - multiple products 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. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional	2023-07-12	5.5	Medium
<u>CVE-2023-30919</u> <u>CVE-2023-30920</u>	products google - multiple products google - multiple products	could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional			
<u>CVE-2023-30920</u>	products google - multiple products	could lead to local information disclosure with no additional execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional	2023-07-12	5.5	Medium
	products	could lead to local information disclosure with no additional			meanum
			2023-07-12	5.5	Medium
	google - multiple	In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional			
<u>CVE-2023-30922</u>	products google - multiple	execution privileges needed. In messaging service, there is a missing permission check. This could lead to local information disclosure with no additional	2023-07-12	5.5	Medium
<u>CVE-2023-30923</u>	products	execution privileges needed. In messaging service, there is a missing permission check. This	2023-07-12	5.5	Medium
<u>CVE-2023-30924</u>	google - multiple products	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
<u>CVE-2023-30926</u>	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
<u>CVE-2023-30927</u>	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. In telephony service, there is a missing permission check. This	2023-07-12	5.5	Medium
<u>CVE-2023-30930</u>	google - multiple products	could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	Medium
<u>CVE-2023-30931</u>	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
<u>CVE-2023-30932</u>	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
<u>CVE-2023-30933</u>	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
	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
<u>CVE-2023-30936</u>	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
<u>CVE-2023-30937</u>	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
<u>CVE-2023-30938</u>	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
<u>CVE-2023-30939</u>	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
	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
	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

	ſ	1	Γ		
		In telephony service, there is a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
<u>CVE-2023-30942</u>	products	execution privileges needed.	2023-07-12	5.5	Medium
		In telephony service, there is a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
<u>CVE-2023-32788</u>	products	execution privileges needed.	2023-07-12	5.5	Medium
		In telephony service, there is a missing permission check. This			
01/5 0000 00700	google - multiple	could lead to local information disclosure with no additional	2022 07 42		
<u>CVE-2023-32789</u>	products	execution privileges needed.	2023-07-12	5.5	Medium
		In telephony service, there is a missing permission check. This			
CVE 2022 22001	google - multiple	could lead to local information disclosure with no additional	2022 07 12		N A a alterna
<u>CVE-2023-33881</u>	products	execution privileges needed.	2023-07-12	5.5	Medium
		In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional			
CVE 2022 22002	google - multiple		2022 07 12		Madium
<u>CVE-2023-33882</u>	products	execution privileges needed. In telephony service, there is a missing permission check. This	2023-07-12	5.5	Medium
	googlo multiplo	could lead to local information disclosure with no additional			
CVE 2022 22002	google - multiple		2023-07-12	5.5	Medium
<u>CVE-2023-33883</u>	products	execution privileges needed. In telephony service, there is a missing permission check. This	2023-07-12	5.5	weatum
	googlo multiplo	could lead to local information disclosure with no additional			
CVE-2023-33884	google - multiple		2023-07-12	5.5	Medium
<u>UVE-2023-33884</u>	products	execution privileges needed.	2023-07-12	5.5	weatum
	accelo multiplo	In telephony service, there is a missing permission check. This			
CVE 2022 22005	google - multiple	could lead to local information disclosure with no additional	2022 07 12		Madium
<u>CVE-2023-33885</u>	products	execution privileges needed.	2023-07-12	5.5	Medium
	and the second second	In telephony service, there is a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional	2022.07.12		N.A !!
<u>CVE-2023-33886</u>	products	execution privileges needed.	2023-07-12	5.5	Medium
		In telephony service, there is a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
<u>CVE-2023-33887</u>	products	execution privileges needed.	2023-07-12	5.5	Medium
		In telephony service, there is a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-33888	products	execution privileges needed.	2023-07-12	5.5	Medium
		In telephony service, there is a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-33889	products	execution privileges needed.	2023-07-12	5.5	Medium
		In telephony service, there is a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-33890	products	execution privileges needed.	2023-07-12	5.5	Medium
		In telephony service, there is a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-33891	products	execution privileges needed.	2023-07-12	5.5	Medium
		In fastDial service, there is a missing permission check. This could			
	google - multiple	lead to local information disclosure with no additional execution			
CVE-2023-33892	products	privileges needed.	2023-07-12	5.5	Medium
		In fastDial service, there is a missing permission check. This could			
	google - multiple	lead to local information disclosure with no additional execution			
CVE-2023-33893	products	privileges needed.	2023-07-12	5.5	Medium
		In fastDial service, there is a missing permission check. This could			
	google - multiple	lead to local information disclosure with no additional execution			
CVE-2023-33894	products	privileges needed.	2023-07-12	5.5	Medium
		In fastDial service, there is a missing permission check. This could			
	google - multiple	lead to local information disclosure with no additional execution			
CVE-2023-33895	products	privileges needed.	2023-07-12	5.5	Medium
		In telephony service, there is a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-33899	products	execution privileges needed.	2023-07-12	5.5	Medium
		In telephony service, there is a missing permission check. This			
	1				
CVE_2022_22000	google - multiple	could lead to local information disclosure with no additional	2022 07 42	5.5	Medium
CVE-2023-33900	google - multiple products	could lead to local information disclosure with no additional execution privileges needed.	2023-07-12	5.5	
<u>CVE-2023-33900</u>	google - multiple products	execution privileges needed.	2023-07-12	5.5	
<u>CVE-2023-33900</u>	products		2023-07-12	5.5	
	products google - multiple	execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional			Medium
<u>CVE-2023-33900</u> <u>CVE-2023-33901</u>	products	execution privileges needed. 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 2023-07-12	5.5	Medium
	products google - multiple products	 execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In bluetooth service, there is a missing permission check. This 			Medium
<u>CVE-2023-33901</u>	products google - multiple products google - multiple	execution privileges needed.In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional	2023-07-12	5.5	
	products google - multiple products	 execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. 			Medium Medium
<u>CVE-2023-33901</u>	products google - multiple products google - multiple	 execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. Adobe Media Encoder versions 22.0, 15.4.2 (and earlier) are 	2023-07-12	5.5	
<u>CVE-2023-33901</u>	products google - multiple products google - multiple	 execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. Adobe Media Encoder versions 22.0, 15.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to 	2023-07-12	5.5	
<u>CVE-2023-33901</u>	products google - multiple products google - multiple	 execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. 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 	2023-07-12	5.5	
<u>CVE-2023-33901</u>	products google - multiple products google - multiple products	 execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. 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 	2023-07-12	5.5	
<u>CVE-2023-33901</u> <u>CVE-2023-33902</u>	products google - multiple products google - multiple products adobe - multiple	 execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. 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 	2023-07-12 2023-07-12	5.5	Medium
<u>CVE-2023-33901</u>	products google - multiple products google - multiple products	 execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. 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	
<u>CVE-2023-33901</u> <u>CVE-2023-33902</u>	products google - multiple products google - multiple products adobe - multiple	 execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. 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. Adobe Media Encoder versions 22.0, 15.4.2 (and earlier) are 	2023-07-12 2023-07-12	5.5	Medium
<u>CVE-2023-33901</u> <u>CVE-2023-33902</u>	products google - multiple products google - multiple products adobe - multiple	 execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. 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. 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 2023-07-12	5.5	Medium
<u>CVE-2023-33901</u> <u>CVE-2023-33902</u>	products google - multiple products google - multiple products adobe - multiple	 execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. 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. 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 2023-07-12	5.5	Medium
<u>CVE-2023-33901</u> <u>CVE-2023-33902</u>	products google - multiple products google - multiple products adobe - multiple products	 execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. 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. 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. 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 	2023-07-12 2023-07-12	5.5	Medium
<u>CVE-2023-33901</u> <u>CVE-2023-33902</u>	products google - multiple products google - multiple products adobe - multiple	 execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. In bluetooth service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. 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. 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 2023-07-12	5.5	Medium

		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			
	adobe - multiple	vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a			
CVE-2021-43760	products	malicious MOV file.	2023-07-12	5.5	Medium
		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	2022 07 12		Madium
<u>CVE-2021-44696</u>	adobe - prelude	interaction in that a victim must open a malicious JPEG file. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and	2023-07-12	5.5	Medium
		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.			
	adobe - multiple	Exploitation of this issue requires user interaction in that a victim			
CVE-2023-29309	products	must open a malicious file.	2023-07-12	5.5	Medium
		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.			
	adobe - multiple	Exploitation of this issue requires user interaction in that a victim			
CVE-2023-29310	products	must open a malicious file.	2023-07-12	5.5	Medium
		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.			
	adobe - multiple	Exploitation of this issue requires user interaction in that a victim			
<u>CVE-2023-29311</u>	products	must open a malicious file.	2023-07-12	5.5	Medium
		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.			
	adobe - multiple	Exploitation of this issue requires user interaction in that a victim			
CVE-2023-29312	products	must open a malicious file.	2023-07-12	5.5	Medium
	· · ·	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			
	adaha multiala	leverage this vulnerability to bypass mitigations such as ASLR.			
CVE-2023-29313	adobe - multiple products	Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	5.5	Medium
012 2023 20015	products	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and	2023 07 12	5.5	Wiedian
		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.			
CVE-2023-29314	adobe - multiple products	Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-07-12	5.5	Medium
<u>CVL-2025-25514</u>	products		2023-07-12		weulun
		Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and		5.5	
	i	Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that		5.5	
				5.5	
		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.		5.5	
CVE 2022 20245	adobe - multiple	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	2022 07 12		Madium
<u>CVE-2023-29315</u>	adobe - multiple products	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
<u>CVE-2023-29315</u>		 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and 	2023-07-12		Medium
<u>CVE-2023-29315</u>		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		Mediun
<u>CVE-2023-29315</u>	products	 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. 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. 	2023-07-12		Mediun
	products adobe - multiple	 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. 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 is provided 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 		5.5	
	products	 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. 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 2023-07-12		
<u>CVE-2023-29315</u> <u>CVE-2023-29316</u>	products adobe - multiple	 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. 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and 		5.5	
	products adobe - multiple	 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. 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that a victim must open a malicious file. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that 		5.5	
	products adobe - multiple	 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. 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and 		5.5	
	products adobe - multiple	 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. 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that a victim must open a malicious file. 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 earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could 		5.5	
<u>CVE-2023-29316</u>	products adobe - multiple products	 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. 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that a victim must open a malicious file. 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. 		5.5	Mediun
	products adobe - multiple products adobe - multiple	 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. 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. 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. 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and 	2023-07-12	5.5	Medium
<u>CVE-2023-29316</u>	products adobe - multiple products adobe - multiple	 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. 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. 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. 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that a victim must open a malicious file. 	2023-07-12	5.5	Medium
<u>CVE-2023-29316</u>	products adobe - multiple products adobe - multiple	 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. 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. 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. 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. 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 learlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could learlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could 	2023-07-12	5.5	Mediun
<u>CVE-2023-29316</u>	products adobe - multiple products adobe - multiple products	 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. 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that volter of this issue requires user interaction in that a victim must open a malicious file. 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. 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. 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. 	2023-07-12	5.5	Mediun
<u>CVE-2023-29316</u> <u>CVE-2023-29317</u>	adobe - multiple products adobe - multiple products adobe - multiple	 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. 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. 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. 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. 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. 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 miti	2023-07-12 2023-07-12	5.5	Mediun
<u>CVE-2023-29316</u> <u>CVE-2023-29317</u>	products adobe - multiple products adobe - multiple products	 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. 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that volter of this issue requires user interaction in that a victim must open a malicious file. 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. 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. 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. 	2023-07-12	5.5	Mediun
<u>CVE-2023-29316</u> <u>CVE-2023-29317</u>	adobe - multiple products adobe - multiple products adobe - multiple	 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. 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. 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that 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. 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. 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	2023-07-12 2023-07-12	5.5	Mediun
<u>CVE-2023-29316</u> <u>CVE-2023-29317</u>	adobe - multiple products adobe - multiple products adobe - multiple	 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. 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. 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. 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. 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue	2023-07-12 2023-07-12	5.5	Mediun
<u>CVE-2023-29316</u>	adobe - multiple products adobe - multiple products adobe - multiple	 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. 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. 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. 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. 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. Adobe InDesign versions ID18.3 (and earlier) and ID17.4.1 (and earlier) are affected by an out-of-bounds read vulnerability that could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue	2023-07-12 2023-07-12	5.5	Medium

		The PVRSRVBridgeGetMultiCoreInfo ioctl in the PowerVR kernel driver can return uninitialized kernel memory to user space. The			
CVE-2021-0948	google - android	contents of this memory could contain sensitive information.	2023-07-13	5.5	Mediu
	800810 0101010	In notification access permission dialog box, malicious application		0.0	
		can embedded a very long service label that overflow the original			
	google - multiple	user prompt and possibly contains mis-leading information to be			
CVE-2023-21260	products	appeared as a system message for user confirmation.	2023-07-13	5.5	Mediu
:VE-2023-32052	microsoft -	Microsoft Power Apps (online) Spoofing Vulnerability	2023-07-11	5.4	Mediu
<u>.vE-2023-32032</u>	power_apps microsoft - multiple	Microsoft Power Apps (online) spooring vulnerability	2023-07-11	5.4	Ivieului
VE-2023-35336	products	Windows MSHTML Platform Security Feature Bypass Vulnerability	2023-07-11	5.4	Mediu
		The permission request prompt from the site in the background			
		tab was overlaid on top of the site in the foreground tab. This			
VE-2023-37455	mozilla - firefox	vulnerability affects Firefox for iOS < 115.	2023-07-12	5.4	Mediu
		A missing permission check in Jenkins Benchmark Evaluator Plugin			
	ionking	1.0.1 and earlier allows attackers with Overall/Read permission to			
	jenkins - benchmark_evaluat	connect to an attacker-specified URL and to check for the existence of directories, `.csv`, and `.ycsb` files on the Jenkins			
VE-2023-37963	or	controller file system.	2023-07-12	5.4	Mediu
<u>VE 2023 37303</u>	01	Stored or persistent cross-site scripting (XSS) is a type of XSS	2023 07 12	5.1	meana
		where the attacker first sends the payload to the web application,			
		then the application saves the payload (e.g., in a database or			
	zabbix - multiple	server-side text files), and finally, the application unintentionally			
<u>:VE-2023-29454</u>	products	executes the payload for every victim visiting its web pages.	2023-07-13	5.4	Mediu
		SAP NetWeaver AS for Java - versions ENGINEAPI 7.50,			
		SERVERCORE 7.50, J2EE-APPS 7.50, allows an unauthenticated			
	sap - netweaver_applicat	attacker to craft a request over the network which can result in unwarranted modifications to a system log without user			
	ion_server_for_jav	interaction. There is no ability to view any information or any			
VE-2023-31405	a	effect on availability.	2023-07-11	5.3	Mediu
		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			
VE-2023-36919	sap - enable_now	to obtain referrer details, resulting in information disclosure.	2023-07-11	5.3	Mediu
		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 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			
	siemens -	malformed HTTP packets. This could allow an unauthenticated			
	ruggedcom_rox_m	malformed HTTP packets. This could allow an unauthenticated remote attacker to send a malformed HTTP packet causing certain			
	ruggedcom_rox_m x5000_firmware	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	
	ruggedcom_rox_m	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. Mono Authenticode Validation Spoofing Vulnerability	2023-07-11 2023-07-11	5.3 5.3	
	ruggedcom_rox_m x5000_firmware	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. Mono Authenticode Validation Spoofing Vulnerability While using a specific function, SAP ERP Defense Forces and Public			
	ruggedcom_rox_m x5000_firmware	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. Mono Authenticode Validation Spoofing Vulnerability While using a specific function, SAP ERP Defense Forces and Public Security - versions 600, 603, 604, 605, 616, 617, 618, 802, 803,			
<u>XVE-2022-29562</u> XVE-2023-35373	ruggedcom_rox_m x5000_firmware	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. Mono Authenticode Validation Spoofing Vulnerability 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			
	ruggedcom_rox_m x5000_firmware	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. Mono Authenticode Validation Spoofing Vulnerability While using a specific function, SAP ERP Defense Forces and Public Security - versions 600, 603, 604, 605, 616, 617, 618, 802, 803,			
	ruggedcom_rox_m x5000_firmware microsoft - mono	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. Mono Authenticode Validation Spoofing Vulnerability 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			Mediu
<u>VE-2023-35373</u>	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple	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. <u>Mono Authenticode Validation Spoofing Vulnerability</u> 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	5.3 4.9	Mediu Mediu
VE-2023-35373 VE-2023-36924	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability	2023-07-11	5.3	Mediu Mediu
VE-2023-35373 VE-2023-36924	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability A vulnerability exists in Palo Alto Networks PAN-OS software that	2023-07-11 2023-07-11	5.3 4.9	Mediu Mediu
VE-2023-35373 VE-2023-36924	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability A vulnerability exists in Palo Alto Networks PAN-OS software that enables an authenticated administrator with the privilege to	2023-07-11 2023-07-11	5.3 4.9	Mediu Mediu
VE-2023-35373 VE-2023-36924 VE-2023-32083	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks -	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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	2023-07-11 2023-07-11 2023-07-11	5.3 4.9 4.9	Mediu Mediu Mediu
VE-2023-35373 VE-2023-36924 VE-2023-32083	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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.	2023-07-11 2023-07-11	5.3 4.9	Mediu Mediu Mediu
VE-2023-35373 VE-2023-36924 VE-2023-32083	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks -	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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. A flaw was found in the subsequent get_user_pages_fast in the	2023-07-11 2023-07-11 2023-07-11	5.3 4.9 4.9	Mediu Mediu Mediu
VE-2023-35373 VE-2023-36924 VE-2023-32083	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks -	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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. A flaw was found in the subsequent get_user_pages_fast in the Linux kernel's interface for symmetric key cipher algorithms in the	2023-07-11 2023-07-11 2023-07-11	5.3 4.9 4.9	Mediu Mediu Mediu
<u>VE-2023-35373</u> <u>VE-2023-36924</u> <u>VE-2023-32083</u> <u>VE-2023-38046</u>	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks -	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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. 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	2023-07-11 2023-07-11 2023-07-11	5.3 4.9 4.9	Mediu Mediu Mediu
<u>VE-2023-35373</u> <u>VE-2023-36924</u> <u>VE-2023-32083</u> <u>VE-2023-38046</u>	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks - multiple products	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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. 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 2023-07-11 2023-07-11 2023-07-12	5.3 4.9 4.9 4.9	Mediu Mediu Mediu
<u>VE-2023-35373</u> <u>VE-2023-36924</u> <u>VE-2023-32083</u> <u>VE-2023-38046</u>	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks - multiple products	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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. 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	2023-07-11 2023-07-11 2023-07-11 2023-07-12	5.3 4.9 4.9 4.9	Mediu Mediu Mediu
<u>VE-2023-35373</u> <u>VE-2023-36924</u> <u>VE-2023-32083</u> <u>VE-2023-38046</u> <u>CVE-2023-3108</u>	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks - multiple products	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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. 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. In bluetooth service, there is a possible missing params check.	2023-07-11 2023-07-11 2023-07-11 2023-07-12	5.3 4.9 4.9 4.9	Mediu Mediu Mediu Mediu
<u>VE-2023-35373</u> <u>VE-2023-36924</u> <u>VE-2023-32083</u> <u>VE-2023-38046</u> <u>CVE-2023-3108</u>	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks - multiple products linux - linux_kernel google - multiple	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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. 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. In bluetooth service, there is a possible missing params check. This could lead to local denial of service with System execution	2023-07-11 2023-07-11 2023-07-11 2023-07-12 2023-07-11	5.3 4.9 4.9 4.9 4.7	Mediu Mediu Mediu Mediu
VE-2023-35373 VE-2023-36924 VE-2023-32083 VE-2023-32083 VE-2023-38046 VE-2023-3108	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks - multiple products linux - linux_kernel google - multiple products	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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. 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. In bluetooth service, there is a possible missing params check. This could lead to local denial of service with System execution privileges needed. 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	2023-07-11 2023-07-11 2023-07-11 2023-07-12 2023-07-11 2023-07-12	5.3 4.9 4.9 4.9 4.7 4.7	Mediu Mediu Mediu Mediu Mediu
<u>VE-2023-35373</u> <u>VE-2023-36924</u> <u>VE-2023-32083</u> <u>VE-2023-38046</u> <u>CVE-2023-3108</u> <u>CVE-2022-48450</u>	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks - multiple products linux - linux_kernel google - multiple products	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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. 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. In bluetooth service, there is a possible missing params check. This could lead to local denial of service with System execution privileges needed. 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.	2023-07-11 2023-07-11 2023-07-11 2023-07-12 2023-07-11	5.3 4.9 4.9 4.9 4.7	Mediu Mediu Mediu Mediu Mediu
<u>VE-2023-35373</u> <u>VE-2023-36924</u> <u>VE-2023-32083</u> <u>VE-2023-38046</u> <u>CVE-2023-3108</u> <u>CVE-2022-48450</u>	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks - multiple products linux - linux_kernel google - multiple products google - multiple	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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. 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. In bluetooth service, there is a possible missing params check. This could lead to local denial of service with System execution privileges needed. 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. In libimpl-ril, there is a possible out of bounds write due to a	2023-07-11 2023-07-11 2023-07-11 2023-07-12 2023-07-11 2023-07-12	5.3 4.9 4.9 4.9 4.7 4.7	Mediu Mediu Mediu Mediu Mediu
XVE-2023-35373 XVE-2023-36924 XVE-2023-32083 XVE-2023-32083 XVE-2023-38046 XVE-2023-3108 XVE-2023-3108 XVE-2023-33896	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks - multiple products linux - linux_kernel google - multiple products google - multiple products	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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. 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. In bluetooth service, there is a possible missing params check. This could lead to local denial of service with System execution privileges needed. 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. 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	2023-07-11 2023-07-11 2023-07-11 2023-07-12 2023-07-12 2023-07-12 2023-07-12	5.3 4.9 4.9 4.9 4.7 4.7 4.4 4.4	Mediu Mediu Mediu Mediu Mediu
<u>VE-2023-35373</u>	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks - multiple products linux - linux_kernel google - multiple products google - multiple	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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. 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. In bluetooth service, there is a possible missing params check. This could lead to local denial of service with System execution privileges needed. 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. 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.	2023-07-11 2023-07-11 2023-07-11 2023-07-12 2023-07-11 2023-07-12	5.3 4.9 4.9 4.9 4.7 4.7	Mediu Mediu Mediu Mediu Mediu
XVE-2023-35373 XVE-2023-36924 XVE-2023-32083 XVE-2023-32083 XVE-2023-38046 XVE-2023-3108 XVE-2023-3108 XVE-2023-33896	ruggedcom_rox_m x5000_firmware microsoft - mono sap - multiple products microsoft - multiple products paloaltonetworks - multiple products linux - linux_kernel google - multiple products google - multiple products	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. Mono Authenticode Validation Spoofing Vulnerability 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. Microsoft Failover Cluster Information Disclosure Vulnerability 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. 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. In bluetooth service, there is a possible missing params check. This could lead to local denial of service with System execution privileges needed. 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. 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	2023-07-11 2023-07-11 2023-07-11 2023-07-12 2023-07-12 2023-07-12 2023-07-12	5.3 4.9 4.9 4.9 4.7 4.7 4.4 4.4	Mediu Mediu Mediu Mediu Mediu Mediu Mediu

		In hci_server, there is a possible out of bounds read due to a			
	google - multiple	missing bounds check. This could lead to local denial of service			
CVE-2023-33904	products	with System execution privileges needed.	2023-07-12	4.4	Medium
		In iwnpi server, there is a possible out of bounds write due to a			
	google - multiple	missing bounds check. This could lead to local denial of service			
<u>CVE-2023-33905</u>	products	with System execution privileges needed.	2023-07-12	4.4	Medium
	ihm multiple	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect			
CVE-2023-23487	ibm - multiple products	Server) 11.1 and 11.5 is vulnerable to insufficient audit logging. IBM X-Force ID: 245918.	2023-07-10	4.3	Medium
<u>CVE-2025-25467</u>	ibm -	IBM Cognos Analytics on Cloud Pak for Data 4.0 could allow an	2023-07-10	4.5	INEUIUIII
	cognos_analytics_c	attacker to make system calls that might compromise the security			
	artridge_for_ibm_c	of the containers due to misconfigured security context. IBM X-			
<u>CVE-2023-28953</u>	loud_pak_for_data	Force ID: 251465.	2023-07-10	4.3	Medium
		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			
CVE-2023-35887	apache - mina	recommended to upgrade to 2.10	2023-07-10	4.3	Medium
	citrix - multiple	Users with only access to launch VDA applications can launch an			
CVE-2023-24490	products	unauthorized desktop	2023-07-10	4.3	Medium
		A missing permission check in Jenkins SAML Single Sign On(SSO)			
	jenkins -	Plugin 2.1.0 through 2.3.0 (both inclusive) allows attackers with			
	saml_single_sign_o	Overall/Read permission to download a string representation of			
CVE-2023-37945	n	the current security realm.	2023-07-12	4.3	Medium
		A missing permission check in Jenkins mabl Plugin 0.0.46 and			
	to all the second l	earlier allows attackers with Overall/Read permission to	2022 07 42		
CVE-2023-37950	jenkins - mabl	enumerate credentials IDs of credentials stored in Jenkins.	2023-07-12	4.3	Medium
		A cross-site request forgery (CSRF) vulnerability in Jenkins Rebuilder Plugin 320.v5a_0933a_e7d61 and earlier allows			
CVE-2023-37954	jenkins - rebuilder	attackers to rebuild a previous build.	2023-07-12	4.3	Medium
<u>CVL-2023-37934</u>	Jerikins - rebuilder	In bluetooth service, there is a possible out of bounds write due to	2023-07-12	4.5	Weuluin
	google - multiple	race condition. This could lead to local denial of service with			
CVE-2022-48451	products	System execution privileges needed.	2023-07-12	4.1	Medium
	jenkins -	Jenkins Oracle Cloud Infrastructure Compute Plugin 1.0.16 and			
	cloud_infrastructur	earlier does not validate SSH host keys when connecting OCI			
CVE-2023-37948	e_compute	clouds, enabling man-in-the-middle attacks.	2023-07-12	3.7	Low
		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.			
	apache - multiple	Users should upgrade to 3.14.9, 3.18.8, 3.20.6 or 3.21.0 and for			
CVE-2023-34442	products	users on Camel 4.x update to 4.0.0-M1	2023-07-10	3.3	Low
<u>CVL 2023 34442</u>	products	A clear text storage of sensitive information (CWE-312)	2023 07 10	5.5	2011
		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			
	fortinet - multiple	and Google Cloud Messaging services, via accessing the files on the			
<u>CVE-2022-22302</u>	products	filesystem.	2023-07-11	3.3	Low
	zoom -	Relative path traversal in the Zoom Client SDK before version			
015 2022 24447	zoom_software_de	5.15.0 may allow an unauthorized user to enable information	2022 07 44	2.2	
<u>CVE-2023-34117</u>	velopment_kit	disclosure via local access.	2023-07-11	3.3	Low
	google - multiple	In music service, there is a missing permission check. This could lead to local information disclosure with no additional execution			
CVE-2023-33879	products	privileges needed.	2023-07-12	3.3	Low
<u>UVL-2023-330/3</u>	products	In music service, there is a missing permission check. This could	2023-07-12	3.3	LOW
	google - multiple	lead to local information disclosure with no additional execution			
	products	privileges needed.	2023-07-12	3.3	Low
CVE-2023-33880		0		0.0	
<u>CVE-2023-33880</u>	products	In startInput of AudioPolicyInterfaceImpl.cpp, there is a possible			
<u>CVE-2023-33880</u>	products				
<u>CVE-2023-33880</u>	google - multiple	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.			

Where NCA provides the vulnerability information as published by NIST's وإذ تبقى NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة. implementation of appropriate recommendations.