

في 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 8th of (NIST) National 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 LVSS 7.0-8.9
 - متوسط: النتيجة الأساسية CVSS 4.0-6.9 متوسط: النتيجة الأساسية CVSS 0.0-3.9
 - منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
		In Apache Linkis <=1.3.1, The PublicService module uploads files without restrictions on the path to the uploaded files, and file types.			
		We recommend users upgrade the version of Linkis to version 1.3.2.			
		For versions			
0.5		<=1.3.1, we suggest turning on the file path check switch in linkis.properties			
CVE- 2023- 27602	apache - linkis	`wds.linkis.workspace.filesystem.owner.check=true` `wds.linkis.workspace.filesystem.path.check=true`	4/10/2023	9.8	Critical
		In Apache Linkis <=1.3.1, due to the Manager module engineConn material upload does not check the zip path, This is a Zip Slip issue, which will lead to a potential RCE vulnerability.			
CVE-		We recommend users upgrade the version of Linkis to version 1.3.2.			
2023- 27603	apache - linkis		4/10/2023	9.8	Critical
CVE- 2023- 29215	apache - linkis	In Apache Linkis <=1.3.1, due to the lack of effective filtering of parameters, an attacker configuring malicious Mysql JDBC parameters in JDBC EengineConn Module will trigger a deserialization vulnerability and eventually lead to remote code execution. Therefore, the parameters in the Mysql JDBC URL should be blacklisted. Versions of Apache Linkis <= 1.3.0 will be affected. We recommend users upgrade the version of Linkis to version 1.3.2.	4/10/2023	9.8	Critical
CVE- 2023-		In Apache Linkis <=1.3.1, because the parameters are not effectively filtered, the attacker uses the MySQL			
29216	apache - linkis	data source and malicious parameters to	4/10/2023	9.8	Critical

			, , , , , , , , , , , , , , , , , , ,		
		configure a new data source to trigger a deserialization vulnerability, eventually leading to			
		remote code execution.			
		Versions of Apache Linkis <= 1.3.0 will be affected.			
		We recommend users upgrade the version of Linkis to version 1.3.2.			
		A memory corruption issue was addressed with			
CVE-		improved state management. This issue is fixed in			
2022-		iOS 16. An app may be able to execute arbitrary			
46709	apple - iphone_os	code with kernel privileges	4/10/2023	9.8	Critical
		Due to missing authentication and input sanitization of code the EventLogServiceCollector of			
		SAP Diagnostics Agent - version 720, allows an			
		attacker to execute malicious scripts on all			
		connected Diagnostics Agents running on Windows.			
CVE- 2023-		On successful exploitation, the attacker can completely compromise confidentiality, integrity			
27497	sap - diagnostics_agent	and availability of the system.	4/11/2023	9.8	Critical
		An attacker with basic privileges in SAP			
		BusinessObjects Business Intelligence Platform			
		(Promotion Management) - versions 420, 430, can get access to Icmbiar file and further decrypt the			
		file. After this attacker can gain access to BI user's			
CVE-		passwords and depending on the privileges of the			
2023-	con multiple and write	BI user, the attacker can perform operations that	1/11/2022	0.0	Cr:+:!
28765	sap - multiple products	can completely compromise the application. A vulnerability has been identified in CP-8031	4/11/2023	9.8	Critical
		MASTER MODULE (All versions < CPCI85 V05), CP-			
		8050 MASTER MODULE (All versions < CPCI85 V05).			
		Affected devices are vulnerable to command			
		injection via the web server port 443/tcp, if the parameter "Remote Operation" is enabled. The			
		parameter is disabled by default.			
CVE-		The vulnerability could allow an unauthenticated			
2023-		The vulnerability could allow an unauthenticated remote attacker to perform arbitrary code			
28489	siemens - cp-8031_firmware	execution on the device.	4/11/2023	9.8	Critical
		A missing authentication for critical function			
		vulnerability [CWE-306] in FortiPresence infrastructure server before version 1.2.1 allows a			
CVE-		remote, unauthenticated attacker to access the			
2022-		Redis and MongoDB instances via crafted			
41331	fortinet - fortiproxy	authentication requests.	4/11/2023	9.8	Critical
CVE- 2023-		Microsoft Message Queuing Remote Code			
21554	microsoft - multiple products	Execution Vulnerability	4/11/2023	9.8	Critical
CVE- 2023-		Microsoft SQL Server Remote Code Execution			
2023- 23384	microsoft - multiple products	Vulnerability	4/11/2023	9.8	Critical
CVE-			, ,		
2023-		Windows Pragmatic General Multicast (PGM)			
28250	microsoft - multiple products	Remote Code Execution Vulnerability Some Hikvision Hybrid SAN/Cluster Storage	4/11/2023	9.8	Critical
		products have an access control vulnerability which			
CVE-		can be used to obtain the admin permission. The			
2023-		attacker can exploit the vulnerability by sending	A /A A /2000	0.0	
28808 CVE-	hikvision - ds-a71024_firmware	crafted messages to the affected devices.	4/11/2023	9.8	Critical
2022-		Memory correction in modem due to buffer			
25678	qualcomm - mdm8207_firmware	overwrite during coap connection	4/13/2023	9.8	Critical
CVE- 2022-		Memory corruption in modem due to buffer overwrite while building an IPv6 multicast address			
2022- 25740	gualcomm - mdm8207 firmware	based on the MAC address of the iface	4/13/2023	9.8	Critical
CVE-	· · · · · · · · · · · · · · · · · · ·	memory corruption in modem due to improper	, _,		
2022-		check while calculating size of serialized CoAP	4/12/2022	0.0	
33211 CVE-	qualcomm - mdm8207_firmware	message Memory corruption due to buffer copy without	4/13/2023	9.8	Critical
2022-		checking the size of input in modem while decoding			
33259	qualcomm - mdm8207_firmware	raw SMS received.	4/13/2023	9.8	Critical
		In Apache Linkis <=1.3.1, due to the default token			
		generated by Linkis Gateway deployment being too			
		simple, it is easy for attackers to obtain the default			
			1		
		token for the attack. Generation rules should add			
CVF-					
CVE- 2023- 27987	apache - linkis	token for the attack. Generation rules should add	4/10/2023	9.1	Critical

					[]
		We recommend users upgrade the version of Linkis to version 1.3.2 And modify the default token value. You can refer to Token authorization[1] https://linkis.apache.org/docs/latest/auth/token https://linkis.apache.org/docs/latest/auth/token			
CVE- 2023- 28205	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, Safari 16.4.1, iOS 16.4.1 and iPadOS 16.4.1, macOS Ventura 13.3.1. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.	4/10/2023	8.8	High
CVE- 2023-		Dell PPDM versions 19.12, 19.11 and 19.10, contain an improper access control vulnerability. A remote authenticated malicious user with low privileges could potentially exploit this vulnerability to bypass intended access restrictions and perform	4/10/2023	0.0	
28062	dell - multiple products	unauthorized actions.A improper privilege management in FortinetFortiSandbox version 4.2.0 through 4.2.2, 4.0.0through 4.0.2 and before 3.2.3 and FortiDeceptorversion 4.1.0, 4.0.0 through 4.0.2 and before 3.3.3	4/11/2023	8.8	High
CVE- 2022- 27487 CVE-	fortinet - multiple products	 allows a remote authenticated attacker to perform unauthorized API calls via crafted HTTP or HTTPS requests. An improper restriction of excessive authentication attempts vulnerability [CWE-307] in Fortinet FortiOS version 7.2.0 through 7.2.3 and before 7.0.10, FortiProxy version 7.2.0 through 7.2.2 and before 7.0.8 administrative interface allows an attacker with a valid user account to perform brute- 	4/11/2023	8.8	High
2022- 43947	fortinet - multiple products	force attacks on other user accounts via injecting valid login sessions. A improper neutralization of special elements used	4/11/2023	8.8	High
CVE- 2023- 27995	fortinet - fortisoar	in a template engine vulnerability in Fortinet FortiSOAR 7.3.0 through 7.3.1 allows an authenticated, remote attacker to execute arbitrary code via a crafted payload.	4/11/2023	8.8	High
CVE- 2023- 21727	microsoft - multiple products	Remote Procedure Call Runtime Remote Code Execution Vulnerability	4/11/2023	8.8	High
CVE- 2023- 24884 CVE-	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	8.8	High
2023- 24886	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	8.8	High
CVE- 2023- 24887	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	8.8	High
CVE- 2023- 24924 CVE-	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	8.8	High
2023- 24925	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	8.8	High
CVE- 2023- 24926	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	8.8	High
CVE- 2023- 24927 CVE-	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	8.8	High
2023- 24928	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	8.8	High
CVE- 2023- 24929	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	8.8	High
CVE- 2023- 28240	microsoft - multiple products	Windows Network Load Balancing Remote Code Execution Vulnerability	4/11/2023	8.8	High

		1	1		
CVE-		Mission of Deptember and DCLC Class Driver Driver			
2023- 28243	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	1/11/2022	8.8	High
28243 CVE-	microsoft - multiple products		4/11/2023	0.0	High
2023-		Microsoft WDAC OLE DB provider for SQL Server			
28275	microsoft - multiple products	Remote Code Execution Vulnerability	4/11/2023	8.8	High
CVE-			.,,	0.0	
2023-		Windows Remote Procedure Call Service (RPCSS)			
28297	microsoft - multiple products	Elevation of Privilege Vulnerability	4/11/2023	8.8	High
	· ·	A cross-site request forgery (CSRF) vulnerability in			-
		Jenkins Report Portal Plugin 0.5 and earlier allows			
CVE-		attackers to connect to an attacker-specified URL			
2023-		using attacker-specified bearer token			
30525	jenkins - report_portal	authentication.	4/12/2023	8.8	High
CVE-	· · · ·	Memory corruption due to buffer copy without			
2022-		checking the size of input in Core while sending			
33288	qualcomm - 315_5g_iot_modem_firmware	SCM command to get write protection information.	4/13/2023	8.8	High
		Type confusion in V8 in Google Chrome prior to			
CVE-		112.0.5615.121 allowed a remote attacker to			
2023-		potentially exploit heap corruption via a crafted			
2033	google - chrome	HTML page. (Chromium security severity: High)	4/14/2023	8.8	High
		An information disclosure vulnerability exists in SAP			
		Landscape Management - version 3.0, enterprise			
		edition. It allows an authenticated SAP Landscape			
		Management user to obtain privileged access to			
		other systems making those other systems			
		vulnerable to information disclosure and			
		modification. The disclosed information is for			
		Diagnostics Agent Connection via Java SCS Message			
		Server of an SAP Solution Manager system and can			
CVE-		only be accessed by authenticated SAP Landscape			
2023-		Management users, but they can escalate their			
26458	sap - landscape_management	privileges to the SAP Solution Manager system.	4/11/2023	8.7	High
		An out-of-bounds write issue was addressed with			
		improved input validation. This issue is fixed in iOS			
		15.7.5 and iPadOS 15.7.5, macOS Monterey 12.6.5,			
		iOS 16.4.1 and iPadOS 16.4.1, macOS Big Sur 11.7.6,			
0.45		macOS Ventura 13.3.1. An app may be able to			
CVE-		execute arbitrary code with kernel privileges. Apple			
2023-		is aware of a report that this issue may have been			
28206	apple - multiple products	actively exploited.	4/10/2023	8.6	High
		Due to missing authentication and insufficient input			
		validation, the OSCommand Bridge of SAP			
		Diagnostics Agent - version 720, allows an attacker			
		with deep knowledge of the system to execute			
		scripts on all connected Diagnostics Agents. On			
CVE- 2023-		successful exploitation, the attacker can completely			
2023- 27267	can diagnostics agent	compromise confidentiality, integrity and	4/11/2022	8.1	Lliah
2/20/	sap - diagnostics_agent	availability of the system.	4/11/2023	0.1	High
		Multiple vulnerabilities including an incorrect			
		permission assignment for critical resource [CWE-			
		732] vulnerability and a time-of-check time-of-use			
		732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in			
CVF		732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows			
CVE-		732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to			
2022-	fortingt - forticliant	732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows	A/11/2022	Q 1	High
	fortinet - forticlient	732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe.	4/11/2023	8.1	High
2022-	fortinet - forticlient	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability 	4/11/2023	8.1	High
2022-	fortinet - forticlient	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 	4/11/2023	8.1	High
2022-	fortinet - forticlient	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 	4/11/2023	8.1	High
2022-	fortinet - forticlient	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated 	4/11/2023	8.1	High
2022- 43946	fortinet - forticlient	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on 	4/11/2023	8.1	High
2022- 43946 CVE-	fortinet - forticlient	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device 	4/11/2023	8.1	High
2022- 43946		 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and the remote FortiGuard server hosting 			
2022- 43946 CVE- 2023- 22642	fortinet - forticlient fortinet - multiple products	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device 	4/11/2023 4/11/2023	8.1	High High
2022- 43946 CVE- 2023- 22642 CVE-		 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and the remote FortiGuard server hosting outbreakalert ressources. 			
2022- 43946 CVE- 2023- 22642 CVE- 2023-	fortinet - multiple products	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and the remote FortiGuard server hosting outbreakalert ressources. Layer 2 Tunneling Protocol Remote Code Execution 	4/11/2023	8.1	High
2022- 43946 CVE- 2023- 22642 CVE- 2023- 2023- 28219		 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and the remote FortiGuard server hosting outbreakalert ressources. 			
2022- 43946	fortinet - multiple products	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and the remote FortiGuard server hosting outbreakalert ressources. Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 	4/11/2023	8.1	High
2022- 43946 CVE- 2023- 22642 CVE- 2023- 28219 CVE- 2023- 28219	fortinet - multiple products microsoft - multiple products	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and the remote FortiGuard server hosting outbreakalert ressources. Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 	4/11/2023 4/11/2023	8.1	High High
2022- 43946 CVE- 2023- 22642 CVE- 2023- 28219 CVE- 2023- 28220	fortinet - multiple products	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and the remote FortiGuard server hosting outbreakalert ressources. Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 	4/11/2023	8.1	High
2022- 43946	fortinet - multiple products microsoft - multiple products	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and the remote FortiGuard server hosting outbreakalert ressources. Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 	4/11/2023 4/11/2023	8.1	High High
2022- 43946 CVE- 2023- 22642 CVE- 2023- 28219 CVE- 2023- 28220 CVE- 2023- 28220 CVE- 2023- 28220	fortinet - multiple products microsoft - multiple products microsoft - multiple products	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and the remote FortiGuard server hosting outbreakalert ressources. Layer 2 Tunneling Protocol Remote Code Execution Vulnerability Layer 2 Tunneling Protocol Remote Code Execution Vulnerability Windows Kerberos Elevation of Privilege 	4/11/2023 4/11/2023 4/11/2023	8.1 8.1 8.1	High High High
2022- 43946 CVE- 2023- 22642 CVE- 2023- 28219 CVE- 2023- 28220 CVE- 2023- 28220 CVE- 2023- 28220	fortinet - multiple products microsoft - multiple products	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and the remote FortiGuard server hosting outbreakalert ressources. Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 	4/11/2023 4/11/2023	8.1	High High
2022- 43946 CVE- 2023- 22642 CVE- 2023- 28219 CVE- 2023- 28220 CVE- 2023- 28220 CVE- 2023- 28220	fortinet - multiple products microsoft - multiple products microsoft - multiple products	 732] vulnerability and a time-of-check time-of-use (TOCTOU) race condition [CWE-367] vulnerability in Fortinet FortiClientWindows before 7.0.7 allows attackers on the same file sharing network to execute commands via writing data into a windows pipe. An improper certificate validation vulnerability [CWE-295] in FortiAnalyzer and FortiManager 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4.8 through 6.4.10 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the communication channel between the device and the remote FortiGuard server hosting outbreakalert ressources. Layer 2 Tunneling Protocol Remote Code Execution Vulnerability Layer 2 Tunneling Protocol Remote Code Execution Vulnerability Windows Kerberos Elevation of Privilege 	4/11/2023 4/11/2023 4/11/2023	8.1 8.1 8.1	High High High

CVE-					
2023-		DHCP Server Service Remote Code Execution			
28231	microsoft - multiple products	Vulnerability	4/11/2023	8	High
		An issue was discovered in			
CVE-		arch/x86/kvm/vmx/nested.c in the Linux kernel			
2023- 30456	linux - multiple products	before 6.2.8. nVMX on x86_64 lacks consistency checks for CR0 and CR4.	4/10/2023	7.8	High
50450		A memory corruption issue was addressed with	4/10/2023	7.0	піgн
CVE-		improved input validation. This issue is fixed in			
2022-		macOS Ventura 13.1. An app may be able to			
42858	apple - macos	execute arbitrary code with kernel privileges	4/10/2023	7.8	High
		A vulnerability has been identified in TIA Portal V15			
		(All versions), TIA Portal V16 (All versions), TIA			
		Portal V17 (All versions), TIA Portal V18 (All versions			
		< V18 Update 1). Affected products contain a path			
		traversal vulnerability that could allow the creation or overwrite of arbitrary files in the engineering			
		system. If the user is tricked to open a malicious PC			
CVE-		system configuration file, an attacker could exploit			
2023-		this vulnerability to achieve arbitrary code			
26293	siemens - multiple products	execution.	4/11/2023	7.8	High
		A vulnerability has been identified in JT Open (All			
		versions < V11.3.2.0), JT Utilities (All versions <			
		V13.3.0.0). The affected applications contain an out			
		of bounds read past the end of an allocated			
CVE-		structure while parsing specially crafted JT files.			
2023-	sigmans, multiple products	This could allow an attacker to execute code in the	4/11/2022	70	⊔iah
29053	siemens - multiple products	context of the current process.An improper neutralization of special elements	4/11/2023	7.8	High
		used in an OS command vulnerability [CWE-78] in			
		FortiADC 5.x all versions, 6.0 all versions, 6.1 all			
		versions, 6.2.0 through 6.2.4, 7.0.0 through 7.0.3,			
		7.1.0; FortiDDoS 4.x all versions, 5.0 all versions,			
		5.1 all versions, 5.2 all versions, 5.3 all versions,			
		5.4 all versions, 5.5 all versions, 5.6 all versions and			
		FortiDDoS-F 6.4.0, 6.3.0 through 6.3.3, 6.2.0			
0.15		through 6.2.2, 6.1.0 through 6.1.4 may allow an			
CVE-		authenticated attacker to execute unauthorized			
2022- 40679	fortinet - multiple products	commands via specifically crafted arguments to existing commands.	4/11/2023	7.8	High
40075		A incorrect authorization in Fortinet FortiClient	4/11/2023	7.0	Tilgii
		(Windows) 7.0.0 - 7.0.7, 6.4.0 - 6.4.9, 6.2.0 - 6.2.9			
CVE-		and 6.0.0 - 6.0.10 allows an attacker to execute			
2022-		unauthorized code or commands via sending a			
40682	fortinet - multiple products	crafted request to a specific named pipe.	4/11/2023	7.8	High
		A relative path traversal vulnerability in Fortinet			
		FortiClient (Windows) 7.0.0 - 7.0.7, 6.4.0 - 6.4.9,			
CVE-		6.2.0 - 6.2.9 and 6.0.0 - 6.0.10 allows an attacker to			
2022-		execute unauthorized code or commands via	4/11/2022	7.0	11:ah
42470	fortinet - multiple products	sending a crafted request to a specific named pipe.A improper neutralization of special elements used	4/11/2023	7.8	High
		in an os command ('os command injection') in			
		Fortinet FortiWeb version 7.0.0 through 7.0.3,			
		FortiADC version 7.1.0 through 7.1.1, FortiADC			
		version 7.0.0 through 7.0.3, FortiADC 6.2 all			
		versions, FortiADC 6.1 all versions, FortiADC 6.0 all			
		versions, FortiADC 5.4 all versions, FortiADC 5.3 all			
		versions, FortiADC 5.2 all versions, FortiADC 5.1 all			
CVE-		versions allows attacker to execute unauthorized			
2022-		code or commands via specifically crafted	A /A A /2000	7.0	
43948	fortinet - multiple products	arguments to existing commands.	4/11/2023	7.8	High
		A download of code without Integrity check vulnerability [CWE-494] in FortiClientMac version			
		7.0.0 through 7.0.7, 6.4 all versions, 6.2 all			
		versions, 6.0 all versions, 5.6 all versions, 5.4 all			
CVE-		versions, 5.2 all versions, 5.0 all versions and 4.0 all			
2023-		versions may allow a local attacker to escalate their			
22635	fortinet - multiple products	privileges via modifying the installer upon upgrade.	4/11/2023	7.8	High
CVE-	_	Microsoft ODBC and OLE DB Remote Code		_	
2023-		Execution Vulnerability	4/11/2023	7.8	High
2023- 23375	microsoft - multiple products				
2023- 23375 CVE-	microsoft - multiple products				
2023- 23375 CVE- 2023-		Visual Studio Code Remote Code Execution	1/11/2022	7.0	111-1
2023- 23375 CVE- 2023- 24893	microsoft - multiple products microsoft - visual_studio_code	Visual Studio Code Remote Code Execution Vulnerability	4/11/2023	7.8	High
2023- 23375 CVE- 2023-			4/11/2023	7.8	High

			· · · ·		
CVE-					
2023- 28225	microsoft - multiple products	Windows NTLM Elevation of Privilege Vulnerability	4/11/2023	7.8	High
CVE-	melosoft multiple products		4/11/2025	7.0	111811
2023-					
28236	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	4/11/2023	7.8	High
CVE-					
2023- 28237	microsoft - multiple products	Windows Kernel Remote Code Execution Vulnerability	4/11/2023	7.8	High
CVE-		Vullerability	4/11/2023	7.0	i ligit
2023-		Windows Registry Elevation of Privilege			
28246	microsoft - multiple products	Vulnerability	4/11/2023	7.8	High
CVE-					
2023-		Minday (America Flavetice of Driviland Mula and ility)	4/11/2022	7.0	11i ala
28248 CVE-	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	4/11/2023	7.8	High
2023-		Windows Common Log File System Driver Elevation			
28252	microsoft - multiple products	of Privilege Vulnerability	4/11/2023	7.8	High
CVE-					
2023-		.NET DLL Hijacking Remote Code Execution		7.0	
28260	microsoft - multiple products	Vulnerability	4/11/2023	7.8	High
CVE- 2023-					
28262	microsoft - multiple products	Visual Studio Elevation of Privilege Vulnerability	4/11/2023	7.8	High
CVE-	· ·				
2023-				_	
28272	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	4/11/2023	7.8	High
CVE- 2023-		Windows Win32k Elevation of Privilege			
2023- 28274	microsoft - multiple products	Vulnerability	4/11/2023	7.8	High
CVE-			.,,		
2023-		Microsoft Office Remote Code Execution			
28285	microsoft - multiple products	Vulnerability	4/11/2023	7.8	High
CVE-		Deve las de Estas ing Devente Code Estas tien			
2023- 28291	microsoft - raw_image_extension	Raw Image Extension Remote Code Execution Vulnerability	4/11/2023	7.8	High
CVE-			τ, 11/2023	7.0	111811
2023-		Raw Image Extension Remote Code Execution			
28292	microsoft - raw_image_extension	Vulnerability	4/11/2023	7.8	High
CVE-				_	
2023- 28293	microsoft - multiple products	Windows Karnal Elevation of Privilage Wylnershility	4/11/2023	7.8	Liah
28293 CVE-	meroson - multiple products	Windows Kernel Elevation of Privilege Vulnerability	4/11/2023	1.0	High
2023-					
28296	microsoft - multiple products	Visual Studio Remote Code Execution Vulnerability	4/11/2023	7.8	High
CVE-					
2023-		Microsoft ODBC and OLE DB Remote Code	1/11/2022	7.0	112.1
28304 CVE-	microsoft - multiple products	Execution Vulnerability	4/11/2023	7.8	High
2023-		Microsoft Word Remote Code Execution			
28311	microsoft - multiple products	Vulnerability	4/11/2023	7.8	High
	· · ·	A use-after-free vulnerability in the Linux Kernel			
		traffic control index filter (tcindex) can be exploited			
		to achieve local privilege escalation. The			
		tcindex_delete function which does not properly deactivate filters in case of a perfect hashes while			
		deleting the underlying structure which can later			
		lead to double freeing the structure. A local			
		attacker user can use this vulnerability to elevate its			
CVE-		privileges to root.			
2023-	linux linux kornal	We recommend upgrading past commit	4/12/2022	7 0	11:
1829	linux - linux_kernel	8c710f75256bb3cf05ac7b1672c82b92c43f3d28. Adobe Dimension version 3.4.8 (and earlier) is	4/12/2023	7.8	High
		affected by an out-of-bounds read vulnerability			
		when parsing a crafted file, which could result in a			
		read past the end of an allocated memory			
		structure. An attacker could leverage this			
CVE		vulnerability to execute code in the context of the			
CVE- 2023-		current user. Exploitation of this issue requires user interaction in that a victim must open a malicious			
2023-26371	adobe - dimension	file.	4/12/2023	7.8	High
		Adobe Dimension version 3.4.8 (and earlier) is	,,		
		affected by an out-of-bounds write vulnerability			
		that could result in arbitrary code execution in the			
CVE- 2023-		context of the current user. Exploitation of this issue requires user interaction in that a victim must			
2023- 26372	adobe - dimension	open a malicious file.	4/12/2023	7.8	High
			1/12/2023	,.0	ப்தா

		Adobe Dimension version 3.4.8 (and earlier) is			
		affected by an out-of-bounds write vulnerability			
		that could result in arbitrary code execution in the			
CVE-		context of the current user. Exploitation of this			
2023-		issue requires user interaction in that a victim must			
26373	adobe - dimension	open a malicious file.	4/12/2023	7.8	High
		Adobe Acrobat Reader versions 23.001.20093 (and			0
		earlier) and 20.005.30441 (and earlier) are affected			
		by an out-of-bounds write vulnerability that could			
		result in arbitrary code execution in the context of			
CVE-		the current user. Exploitation of this issue requires			
2023-					
	adaha multipla products	user interaction in that a victim must open a malicious file.	4/12/2022	70	Lliah
26395	adobe - multiple products		4/12/2023	7.8	High
		Adobe Acrobat Reader versions 23.001.20093 (and			
		earlier) and 20.005.30441 (and earlier) are affected			
		by a Creation of Temporary File in Directory with			
		Incorrect Permissions vulnerability that could result			
		in privilege escalation in the context of the current			
CVE-		user. Exploitation of this issue requires user			
2023-		interaction in that a victim must open a malicious			
26396	adobe - multiple products	file.	4/12/2023	7.8	High
		Adobe Acrobat Reader versions 23.001.20093 (and			
		earlier) and 20.005.30441 (and earlier) are affected			
		by an Improper Input Validation vulnerability that			
		could result in arbitrary code execution in the			
CVE-		context of the current user. Exploitation of this			
2023-		issue requires user interaction in that a victim must			
26405	adobe - multiple products	open a malicious file.	4/12/2023	7.8	High
		Adobe Acrobat Reader versions 23.001.20093 (and			
		earlier) and 20.005.30441 (and earlier) are affected			
		by an Improper Access Control vulnerability that			
		could result in arbitrary code execution in the			
CVE-		context of the current user. Exploitation of this			
2023-		issue requires user interaction in that a victim must			
26406	adobe - multiple products	open a malicious file.	4/12/2023	7.8	High
20100		Adobe Acrobat Reader versions 23.001.20093 (and	1/12/2023	7.0	
		earlier) and 20.005.30441 (and earlier) are affected			
		by an Improper Input Validation vulnerability that			
		could result in arbitrary code execution in the			
CVE-		•			
		context of the current user. Exploitation of this			
2023-		issue requires user interaction in that a victim must	4/42/2022	7.0	11:
26407	adobe - multiple products	open a malicious file.	4/12/2023	7.8	High
		Adobe Acrobat Reader versions 23.001.20093 (and			
		earlier) and 20.005.30441 (and earlier) are affected			
		by an Improper Access Control vulnerability that			
		could result in arbitrary code execution in the			
CVE-		context of the current user. Exploitation of this			
2023-		issue requires user interaction in that a victim must			
26408	adobe - multiple products	open a malicious file.	4/12/2023	7.8	High
		Adobe Acrobat Reader versions 23.001.20093 (and			
		earlier) and 20.005.30441 (and earlier) are affected			
		by a Use After Free vulnerability that could result in			
		arbitrary code execution in the context of the			
CVE-		current user. Exploitation of this issue requires user			
2023-		interaction in that a victim must open a malicious			
26417	adobe - multiple products	file.	4/12/2023	7.8	High
		Adobe Acrobat Reader versions 23.001.20093 (and	. ,	-	5
		earlier) and 20.005.30441 (and earlier) are affected			
		by a Use After Free vulnerability that could result in			
		arbitrary code execution in the context of the			
CVE-		current user. Exploitation of this issue requires user			
2023-		interaction in that a victim must open a malicious			
2023-26418	adobe - multiple products	file.	4/12/2023	7.8	High
20710			7/12/2023	<i>.</i> 0	i ligit
		Adobe Acrobat Reader versions 23.001.20093 (and			
		earlier) and 20.005.30441 (and earlier) are affected			
		by a Use After Free vulnerability that could result in			
		arbitrary code execution in the context of the			
CVE-		current user. Exploitation of this issue requires user			
2023-		interaction in that a victim must open a malicious			
26419	adobe - multiple products	file.	4/12/2023	7.8	High
		Adobe Acrobat Reader versions 23.001.20093 (and			
		contian) and 20 005 20441 (and contian) are officiated	1		
		earlier) and 20.005.30441 (and earlier) are affected			
		by a Use After Free vulnerability that could result in			
		by a Use After Free vulnerability that could result in			
CVE-		by a Use After Free vulnerability that could result in arbitrary code execution in the context of the			
		by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user			
CVE- 2023- 26420	adobe - multiple products	by a Use After Free vulnerability that could result in arbitrary code execution in the context of the	4/12/2023	7.8	High

			1		
		Adobe Acrobat Reader versions 23.001.20093 (and			
		earlier) and 20.005.30441 (and earlier) are affected			
		by an Integer Underflow or Wraparound			
		vulnerability that could result in arbitrary code			
CVE-		execution in the context of the current user.			
2023- 26421	adobe - multiple products	Exploitation of this issue requires user interaction in	4/12/2022	7.8	Lliah
20421	adobe - multiple products	that a victim must open a malicious file. Adobe Acrobat Reader versions 23.001.20093 (and	4/12/2023	7.8	High
		earlier) and 20.005.30441 (and earlier) are affected			
		by a Use After Free vulnerability that could result in			
		arbitrary code execution in the context of the			
CVE-		current user. Exploitation of this issue requires user			
2023-		interaction in that a victim must open a malicious			
26422	adobe - multiple products	file.	4/12/2023	7.8	High
20422	adobe - mattiple products	Adobe Acrobat Reader versions 23.001.20093 (and	4/12/2023	7.0	Tilgii
		earlier) and 20.005.30441 (and earlier) are affected			
		by a Use After Free vulnerability that could result in			
		arbitrary code execution in the context of the			
CVE-		current user. Exploitation of this issue requires user			
2023-		interaction in that a victim must open a malicious			
26423	adobe - multiple products	file.	4/12/2023	7.8	High
20423		Adobe Acrobat Reader versions 23.001.20093 (and	4/12/2023	7.0	Tilgii
		-			
		earlier) and 20.005.30441 (and earlier) are affected by a Use After Free vulnerability that could result in			
		arbitrary code execution in the context of the			
CVE-					
2023-		current user. Exploitation of this issue requires user interaction in that a victim must open a malicious			
	adaba multipla products	file.	4/12/2022	70	⊔iah
26424	adobe - multiple products	Adobe Acrobat Reader versions 23.001.20093 (and	4/12/2023	7.8	High
		earlier) and 20.005.30441 (and earlier) are affected			
		by an out-of-bounds read vulnerability when			
		parsing a crafted file, which could result in a read			
		past the end of an allocated memory structure. An			
		attacker could leverage this vulnerability to execute			
CVE-		code in the context of the current user. Exploitation			
2023-		of this issue requires user interaction in that a			
26425	adobe - multiple products	victim must open a malicious file.	4/12/2023	7.8	High
20423		Adobe Digital Editions version 4.5.11.187303 (and	4/12/2023	7.0	Tilgii
		earlier) is affected by an out-of-bounds write			
		vulnerability that could result in arbitrary code			
CVE-		execution in the context of the current user.			
2023-		Exploitation of this issue requires user interaction in			
2023-	adobe - digital_editions	that a victim must open a malicious file.	4/12/2023	7.8	High
21302		InCopy versions 18.1 (and earlier), 17.4 (and earlier)	4/12/2023	7.0	Tingi
		are affected by a Use After Free vulnerability that			
		could result in arbitrary code execution in the			
CVE-		context of the current user. Exploitation of this			
2023-		issue requires user interaction in that a victim must			
22235	adobe - multiple products	open a malicious file.	4/12/2023	7.8	High
		Adobe Substance 3D Stager version 2.0.1 (and	.,,		
		earlier) is affected by a Stack-based Buffer Overflow			
		vulnerability that could result in arbitrary code			
CVE-		execution in the context of the current user.			
2023-		Exploitation of this issue requires user interaction in			
26383	adobe - substance_3d_stager	that a victim must open a malicious file.	4/12/2023	7.8	High
		Adobe Substance 3D Stager version 2.0.1 (and	., 12, 2025	,.5	
		earlier) is affected by a Use After Free vulnerability			
		that could result in arbitrary code execution in the			
CVE-		context of the current user. Exploitation of this			
2023-		issue requires user interaction in that a victim must			
26384	adobe - substance_3d_stager	open a malicious file.	4/12/2023	7.8	High
		Adobe Substance 3D Stager version 2.0.1 (and	., 12, 2025	,.5	
		earlier) is affected by an Improper Input Validation			
		vulnerability that could result in arbitrary code			
CVE-		execution in the context of the current user.			
2023-		Exploitation of this issue requires user interaction in			
26388	adobe - substance 3d stager	that a victim must open a malicious file.	4/12/2023	7.8	High
		Adobe Substance 3D Stager version 2.0.1 (and	·, ±2,2023	,.0	
		earlier) is affected by an out-of-bounds read			
		vulnerability when parsing a crafted file, which			
		could result in a read past the end of an allocated			
		memory structure. An attacker could leverage this			
		vulnerability to execute code in the context of the			
CVE		current user. Exploitation of this issue requires user			
CVE-		Interaction in that a victim must appear a maliare			
2023-	adoba substance ad stars	interaction in that a victim must open a malicious	1/12/2022	70	Lliah
2023- 26389	adobe - substance_3d_stager	file.	4/12/2023	7.8	High
2023- 26389 CVE-	adobe - substance_3d_stager	file. Adobe Substance 3D Stager version 2.0.1 (and	4/12/2023	7.8	High
2023- 26389	adobe - substance_3d_stager adobe - substance 3d stager	file.	4/12/2023	7.8	High High

			,		
		execution in the context of the current user.			
		Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
		Adobe Substance 3D Stager version 2.0.1 (and			
		earlier) is affected by an out-of-bounds read			
		vulnerability when parsing a crafted file, which			
		could result in a read past the end of an allocated			
		memory structure. An attacker could leverage this			
		vulnerability to execute code in the context of the			
CVE-		current user. Exploitation of this issue requires user			
2023-		interaction in that a victim must open a malicious			
26391	adobe - substance_3d_stager	file.	4/12/2023	7.8	High
	V	Adobe Substance 3D Stager version 2.0.1 (and			Ŭ
		earlier) is affected by a Use After Free vulnerability			
		that could result in arbitrary code execution in the			
CVE-		context of the current user. Exploitation of this			
2023-		issue requires user interaction in that a victim must			
26392	adobe - substance_3d_stager	open a malicious file.	4/12/2023	7.8	High
		Adobe Substance 3D Stager version 2.0.1 (and			
		earlier) is affected by an out-of-bounds read			
		vulnerability when parsing a crafted file, which			
		could result in a read past the end of an allocated			
		memory structure. An attacker could leverage this			
		vulnerability to execute code in the context of the			
CVE-		current user. Exploitation of this issue requires user			
2023-		interaction in that a victim must open a malicious			
26393	adobe - substance_3d_stager	file.	4/12/2023	7.8	High
		Adobe Substance 3D Stager version 2.0.1 (and	I T		_
		earlier) is affected by a Heap-based Buffer Overflow			
		vulnerability that could result in arbitrary code			
CVE-		execution in the context of the current user.			
2023-		Exploitation of this issue requires user interaction in			
26394	adobe - substance_3d_stager	that a victim must open a malicious file.	4/12/2023	7.8	High
		Adobe Substance 3D Stager version 2.0.1 (and			
		earlier) is affected by an out-of-bounds read			
		vulnerability when parsing a crafted file, which			
		could result in a read past the end of an allocated			
		memory structure. An attacker could leverage this			
		vulnerability to execute code in the context of the			
CVE-		current user. Exploitation of this issue requires user			
2023-		interaction in that a victim must open a malicious			
26402	adobe - substance_3d_stager	file.	4/12/2023	7.8	High
CVE-		Memory corruption due to integer overflow to			
2022-	and a surface way of the second se	buffer overflow in Modem while parsing Traffic	4/42/2022	7.0	11:
33296 CVE-	qualcomm - 315_5g_iot_modem_firmware	Channel Neighbor List Update message. Memory corruption due to integer overflow or	4/13/2023	7.8	High
2022-		wraparound in WLAN while sending WMI cmd from			
40532	qualcomm - 315_5g_iot_modem_firmware	host to target.	4/13/2023	7.8	High
40332 CVE-		Memory Corruption in Multimedia Framework due	4/13/2023	7.0	Tilgii
2023-		to integer overflow when synx bind is called along			
21630	qualcomm - qca6391_firmware	with synx signal.	4/13/2023	7.8	High
21050		Adobe Substance 3D Designer version 12.4.0 (and	4/13/2023	7.0	Ingi
		earlier) is affected by an out-of-bounds read			
		vulnerability when parsing a crafted file, which			
		could result in a read past the end of an allocated			
		memory structure. An attacker could leverage this			
		vulnerability to execute code in the context of the			
CVE-		current user. Exploitation of this issue requires user			
2023-		interaction in that a victim must open a malicious			
26398	adobe - substance_3d_designer	file.	4/13/2023	7.8	High
		Adobe Substance 3D Designer version 12.4.0 (and	, _,	-	0
		earlier) is affected by an out-of-bounds read			
		vulnerability when parsing a crafted file, which			
		could result in a read past the end of an allocated			
		memory structure. An attacker could leverage this			
		vulnerability to execute code in the context of the			
CVE-		current user. Exploitation of this issue requires user			
2023-		interaction in that a victim must open a malicious			
26409	adobe - substance_3d_designer	file.	4/13/2023	7.8	High
		Adobe Substance 3D Designer version 12.4.0 (and			
1		earlier) is affected by a Use After Free vulnerability			
		that could result in arbitrary code execution in the			
CVE-		context of the current user. Exploitation of this			
CVE- 2023-		•			
	adobe - substance_3d_designer	context of the current user. Exploitation of this	4/13/2023	7.8	High
2023-	adobe - substance_3d_designer	context of the current user. Exploitation of this issue requires user interaction in that a victim must	4/13/2023	7.8	High
2023-	adobe - substance_3d_designer	context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/13/2023	7.8	High
2023- 26410	adobe - substance_3d_designer	 context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Designer version 12.4.0 (and 	4/13/2023	7.8	High

		memory structure. An attacker could leverage this			
		vulnerability to execute code in the context of the			
		current user. Exploitation of this issue requires user			
		interaction in that a victim must open a malicious			
		file.			
		Adobe Substance 3D Designer version 12.4.0 (and			
		earlier) is affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code			
CVE-		execution in the context of the current user.			
2023-		Exploitation of this issue requires user interaction in			
26412	adobe - substance_3d_designer	that a victim must open a malicious file.	4/13/2023	7.8	High
20412		Adobe Substance 3D Designer version 12.4.0 (and	4/13/2023	7.0	Tingii
		earlier) is affected by a Heap-based Buffer Overflow			
		vulnerability that could result in arbitrary code			
CVE-		execution in the context of the current user.			
2023-		Exploitation of this issue requires user interaction in			
26413	adobe - substance_3d_designer	that a victim must open a malicious file.	4/13/2023	7.8	High
		Adobe Substance 3D Designer version 12.4.0 (and	, , ,		0
		earlier) is affected by a Use After Free vulnerability			
		that could result in arbitrary code execution in the			
CVE-		context of the current user. Exploitation of this			
2023-		issue requires user interaction in that a victim must			
26414	adobe - substance_3d_designer	open a malicious file.	4/13/2023	7.8	High
		Adobe Substance 3D Designer version 12.4.0 (and			
		earlier) is affected by an out-of-bounds write			
		vulnerability that could result in arbitrary code			
CVE-		execution in the context of the current user.			
2023-		Exploitation of this issue requires user interaction in			
26415	adobe - substance_3d_designer	that a victim must open a malicious file.	4/13/2023	7.8	High
		Adobe Substance 3D Designer version 12.4.0 (and			
		earlier) is affected by a Heap-based Buffer Overflow			
		vulnerability that could result in arbitrary code			
CVE-		execution in the context of the current user.			
2023-	adaba substance 24 daris su	Exploitation of this issue requires user interaction in	1/12/2022	70	11:
26416	adobe - substance_3d_designer	that a victim must open a malicious file.	4/13/2023	7.8	High
		ncurses before 6.4 20230408, when used by a			
		setuid application, allows local users to trigger			
CVE-		security-relevant memory corruption via malformed data in a terminfo database file that is			
2023-		found in \$HOME/.terminfo or reached via the			
2023-29491	gnu - ncurses	TERMINFO or TERM environment variable.	4/14/2023	7.8	High
29491 CVE-	5nu neuroco	Nginx NJS v0.7.10 was discovered to contain a	·, ⊥¬, ∠∪∠J	7.0	111611
2023-		segmentation violation via the function			
27727	f5 - nginx	njs_function_frame at src/njs_function.h.	4/9/2023	7.5	High
CVE-		Nginx NJS v0.7.10 was discovered to contain a	., 0, 2020		0''
2023-		segmentation violation via the function			
27728	f5 - nginx	njs_dump_is_recursive at src/njs_vmcode.c.	4/9/2023	7.5	High
CVE-	5	Nginx NJS v0.7.10 was discovered to contain an			
2023-		illegal memcpy via the function njs_vmcode_return			
27729	f5 - nginx	at src/njs_vmcode.c.	4/9/2023	7.5	High
CVE-	-	Nginx NJS v0.7.10 was discovered to contain a			-
2023-		segmentation violation via the function			
27730	f5 - nginx	njs_lvlhsh_find at src/njs_lvlhsh.c.	4/9/2023	7.5	High
		A logic issue was addressed with improved state			
CVE-		management. This issue is fixed in macOS Ventura			
2022-		13.1, iOS 16.2 and iPadOS 16.2. Private Relay			
46716	apple - multiple products	functionality did not match system settings	4/10/2023	7.5	High
		A vulnerability has been identified in SIMATIC CP			
		1242-7 V2 (All versions), SIMATIC CP 1243-1 (All			
		versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS			
		variants) (All versions), SIMATIC CP 1243-1 IEC (incl.			
		SIPLUS variants) (All versions), SIMATIC CP 1243-7			
		LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All			
		versions), SIMATIC CP 1243-8 IRC (All versions),			
		SIMATIC CP 1542SP-1 (All versions), SIMATIC CP			
		1542SP-1 IRC (All versions), SIMATIC CP 1543SP-1			
		(All versions), SIMATIC CP 443-1 (All versions < V3.3), SIMATIC CP 443-1 (All versions < V3.3),			
		SIMATIC CP 443-1 Advanced (All versions < V3.3), SIMATIC IPC DiagBase (All versions), SIMATIC IPC			
		DiagMonitor (All versions), SIPLUS ET 200SP CP			
		1542SP-1 IRC TX RAIL (All versions), SIPLUS ET 200SP CP			
		200SP CP 1543SP-1 ISEC (All versions), SIPLUS ET			
		200SP CP 1543SP-1 ISEC (All versions), SIPLOS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions),			
		SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET			
		CP 443-1 (All versions < V3.3), SIPLUS NET CP 443-1			
CVE-		Advanced (All versions < V3.3), SIPLUS NET CF 443-1 Advanced (All versions < V3.3), SIPLUS S7-1200 CP			
2022-		1243-1 (All versions), SIPLUS S7-1200 CP 1243-1			
43716	siemens - simatic_cp_1242-7_v2_firmware	RAIL (All versions), SIPLUS TIM 1531 IRC (All	4/11/2023	7.5	High
			.,, _020		· · · o' ·

		versions < V2.3.6), TIM 1531 IRC (All versions <			
		V2.3.6). The webserver of the affected products			
		contains a vulnerability that may lead to a denial of			
		service condition. An attacker may cause a denial of			
		service situation which leads to a restart of the webserver of the affected product.			
		A vulnerability has been identified in SIMATIC CP			
		1242-7 V2 (All versions), SIMATIC CP 1243-1 (All			
		versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS			
		variants) (All versions), SIMATIC CP 1243-1 IEC (incl.			
		SIPLUS variants) (All versions), SIMATIC CP 1243-7			
		LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All			
		versions), SIMATIC CP 1243-8 IRC (All versions),			
		SIMATIC CP 1542SP-1 (All versions), SIMATIC CP			
		1542SP-1 IRC (All versions), SIMATIC CP 1543SP-1			
		(All versions), SIMATIC CP 443-1 (All versions <			
		V3.3), SIMATIC CP 443-1 (All versions < V3.3),			
		SIMATIC CP 443-1 Advanced (All versions < V3.3),			
		SIMATIC IPC DiagBase (All versions), SIMATIC IPC DiagMonitor (All versions), SIPLUS ET 200SP CP			
		1542SP-1 IRC TX RAIL (All versions), SIPLOS ET 2005P CP			
		200SP CP 1543SP-1 ISEC (All versions), SIPLUS ET			
		200SP CP 1543SP-1 ISEC TX RAIL (All versions),			
		SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET			
		CP 443-1 (All versions < V3.3), SIPLUS NET CP 443-1			
		Advanced (All versions < V3.3), SIPLUS S7-1200 CP			
		1243-1 (All versions), SIPLUS S7-1200 CP 1243-1			
		RAIL (All versions), SIPLUS TIM 1531 IRC (All			
		versions < V2.3.6), TIM 1531 IRC (All versions <			
		V2.3.6). The webserver of the affected products			
		contains a vulnerability that may lead to a denial of			
CVE- 2022-		service condition. An attacker may cause a denial of service situation of the webserver of the affected			
43767	siemens - simatic_cp_1242-7_v2_firmware	product.	4/11/2023	7.5	High
43707	siemens - simatic_cp_1242-7_v2_mmware	A vulnerability has been identified in SIMATIC CP	4/11/2023	7.5	Ingi
		1242-7 V2 (All versions), SIMATIC CP 1243-1 (All			
		versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLUS			
		variants) (All versions), SIMATIC CP 1243-1 IEC (incl.			
		SIPLUS variants) (All versions), SIMATIC CP 1243-7			
		LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All			
		versions), SIMATIC CP 1243-8 IRC (All versions),			
		SIMATIC CP 1542SP-1 (All versions), SIMATIC CP			
		1542SP-1 IRC (All versions), SIMATIC CP 1543SP-1			
		(All versions), SIMATIC CP 443-1 (All versions <			
		V3.3), SIMATIC CP 443-1 (All versions $<$ V3.3),			
		SIMATIC CP 443-1 Advanced (All versions < V3.3), SIMATIC IPC DiagBase (All versions), SIMATIC IPC			
		DiagMonitor (All versions), SIPLUS ET 200SP CP			
		1542SP-1 IRC TX RAIL (All versions), SIPLUS ET			
		200SP CP 1543SP-1 ISEC (All versions), SIPLUS ET			
		200SP CP 1543SP-1 ISEC TX RAIL (All versions),			
		SIPLUS NET CP 1242-7 V2 (All versions), SIPLUS NET			
		CP 443-1 (All versions < V3.3), SIPLUS NET CP 443-1			
		Advanced (All versions < V3.3), SIPLUS S7-1200 CP			
		1243-1 (All versions), SIPLUS S7-1200 CP 1243-1			
		RAIL (All versions), SIPLUS TIM 1531 IRC (All			
		versions < V2.3.6), TIM 1531 IRC (All versions <			
		V2.3.6). The webserver of the affected products contains a vulnerability that may lead to a denial of			
CVE-		service condition. An attacker may cause a denial of			
2022-		service situation of the webserver of the affected			
43768	siemens - simatic_cp_1242-7_v2_firmware	product.	4/11/2023	7.5	High
	····	A vulnerability has been identified in SIPROTEC 5	, ,=====	-	0
		6MD85 (CP200) (All versions), SIPROTEC 5 6MD85			
		(CP300) (All versions < V9.40), SIPROTEC 5 6MD86			
		(CP200) (All versions), SIPROTEC 5 6MD86 (CP300)			
		(All versions < V9.40), SIPROTEC 5 6MD89 (CP300)			
		(All versions), SIPROTEC 5 6MU85 (CP300) (All			
		versions < V9.40), SIPROTEC 5 7KE85 (CP200) (All			
		versions), SIPROTEC 5 7KE85 (CP300) (All versions <			
		V9.40), SIPROTEC 5 7SA82 (CP100) (All versions), SIPROTEC 5 7SA82 (CP150) (All versions < V9.40),			
		SIPROTEC 5 7SA82 (CP150) (All versions < v9.40), SIPROTEC 5 7SA84 (CP200) (All versions), SIPROTEC			
		5 7SA86 (CP200) (All versions), SIPROTEC 5 7SA86			
		(CP300) (All versions < V9.40), SIPROTEC 5 75A80			
		(CP200) (All versions), SIPROTEC 5 75A87 (CP300)			
		(All versions < V9.40), SIPROTEC 5 7SD82 (CP100)			
CVE-		(All versions), SIPROTEC 5 7SD82 (CP150) (All			
2023-		versions < V9.40), SIPROTEC 5 7SD84 (CP200) (All			
28766	siemens - siprotec_5_6md85_firmware	versions), SIPROTEC 5 7SD86 (CP200) (All versions),	4/11/2023	7.5	High
·	,				<u> </u>

r r		1	1		
CVE- 2023-		Windows Point-to-Point Tunneling Protocol Remote			
2023- 28232	microsoft - multiple products	Code Execution Vulnerability	4/11/2023	7.5	High
CVE-					
2023-		Windows Secure Channel Denial of Service			
28233	microsoft - multiple products	Vulnerability	4/11/2023	7.5	High
CVE- 2023-		Windows Secure Channel Denial of Service			
2023- 28234	microsoft - multiple products	Vulnerability	4/11/2023	7.5	High
CVE-			4/11/2023	7.5	- ingli
2023-		Windows Internet Key Exchange (IKE) Protocol			
28238	microsoft - multiple products	Extensions Remote Code Execution Vulnerability	4/11/2023	7.5	High
CVE-					
2023- 28241	microsoft - multiple products	Windows Secure Socket Tunneling Protocol (SSTP)	4/11/2022	7.5	⊔iah
28241 CVE-	microsoft - multiple products	Denial of Service Vulnerability	4/11/2023	7.5	High
2023-		Windows Network File System Information			
28247	microsoft - multiple products	Disclosure Vulnerability	4/11/2023	7.5	High
CVE-					
2023-		Azure Service Connector Security Feature Bypass			
28300 CVE-	microsoft - azure_service_connector	Vulnerability	4/11/2023	7.5	High
2023-		Microsoft Message Queuing Denial of Service			
28302	microsoft - multiple products	Vulnerability	4/11/2023	7.5	High
		Jenkins Kubernetes Plugin 3909.v1f2c633e8590 and			<u>U</u>
CVE-		earlier does not properly mask (i.e., replace with			
2023-		asterisks) credentials in the build log when push	A / 1 A / 2		
30513	jenkins - kubernetes	mode for durable task logging is enabled. Jenkins Azure Key Vault Plugin	4/12/2023	7.5	High
		187.va_cd5fecd198a_ and earlier does not properly			
CVE-		mask (i.e., replace with asterisks) credentials in the			
2023-		build log when push mode for durable task logging			
30514	jenkins - azure_key_vault	is enabled.	4/12/2023	7.5	High
0.15		Jenkins Thycotic DevOps Secrets Vault Plugin 1.0.0			
CVE- 2023-		and earlier does not properly mask (i.e., replace with asterisks) credentials in the build log when			
30515	jenkins - thycotic_devops_secrets_vault	push mode for durable task logging is enabled.	4/12/2023	7.5	High
CVE-		Information disclosure in modem data due to array	.,,		
2022-		out of bound access while handling the incoming			
25726	qualcomm - mdm9205_firmware	DNS response packet	4/13/2023	7.5	High
CVE-		Information disclosure in modem due to buffer			
2022- 25731	qualcomm - mdm9205_firmware	over-read while processing packets from DNS server	4/13/2023	7.5	High
CVE-	qualconini indinozos_ininware	Information disclosure in modem due to missing	4/13/2023	7.5	i iigii
2022-		NULL check while reading packets received from			
25737	qualcomm - mdm8207_firmware	local network	4/13/2023	7.5	High
CVE-		Information disclosure in modem due to improper			
2022- 25747	qualcomm - mdm8207_firmware	input validation during parsing of upcoming CoAP message	4/13/2023	7.5	High
CVE-	qualconini - munozor_mmware		4/13/2023	7.5	Ingii
2022-		Information disclosure due to buffer over-read			
33222	qualcomm - mdm9205_firmware	while parsing DNS response packets in Modem.	4/13/2023	7.5	High
CVE-		Transient DOS in Modem due to null pointer			
2022- 33223	augloomm - mdm9207 firmwore	dereference while processing the incoming packet with http chunked encoding.	4/13/2023	7.5	High
33223 CVE-	qualcomm - mdm8207_firmware	Information disclosure sue to buffer over-read in	7/13/2023	د. ر	111811
2022-		modem while processing ipv6 packet with hop-by-			
33228	qualcomm - mdm8207_firmware	hop or destination option in header.	4/13/2023	7.5	High
CVE-					
2022-		Information disclosure due to buffer over-read in	1/12/2022	7 5	- استار ا
33258 CVE-	qualcomm - mdm8207_firmware	modem while reading configuration parameters. Information disclosure in Modem due to buffer	4/13/2023	7.5	High
2022-		over-read while getting length of Unfragmented			
33287	qualcomm - 9205_lte_modem_firmware	headers in an IPv6 packet.	4/13/2023	7.5	High
CVE-		Information disclosure in Modem due to buffer			
2022-		over-read while receiving a IP header with	4/40/0000		
33291 CVE-	qualcomm - 9205_lte_modem_firmware	malformed length. Transient DOS in Modem due to NULL pointer	4/13/2023	7.5	High
2022-		dereference while receiving response of lwm2m			
33294	qualcomm - mdm8207_firmware	registration/update/bootstrap request message.	4/13/2023	7.5	High
CVE-		Information disclosure in Modem due to buffer			
2022-		over-read while parsing the wms message received			
	qualcomm - mdm8207_firmware	given the buffer and its length.	4/13/2023	7.5	High
33295			1		
CVE-		Information disclosure due to buffer average of in			
CVE- 2022-	aualcomm - 9206 Ite modem firmware	Information disclosure due to buffer over-read in Bluetooth Host while A2DP streaming.	4/13/2023	75	High
CVE- 2022- 40503	qualcomm - 9206_lte_modem_firmware	Bluetooth Host while A2DP streaming.	4/13/2023	7.5	High
CVE- 2022-	qualcomm - 9206_lte_modem_firmware		4/13/2023	7.5	High

		IRT PRO (All versions < V5.5.2), SCALANCE X202-			
		2IRT (All versions < V5.5.2), SCALANCE X202-2IRT			
		(All versions < V5.5.2), SCALANCE X202-2P IRT (All			
		versions < V5.5.2), SCALANCE X202-2P IRT PRO (All			
		versions < V5.5.2), SCALANCE X204IRT (All versions			
		< V5.5.2), SCALANCE X204IRT (All versions < V5.5.2),			
		SCALANCE X204IRT PRO (All versions < V5.5.2),			
		SCALANCE XF201-3P IRT (All versions < V5.5.2),			
		SCALANCE XF202-2P IRT (All versions < V5.5.2),			
		SCALANCE XF204-2BA IRT (All versions < V5.5.2),			
		SCALANCE XF204IRT (All versions < V5.5.2), SIPLUS			
		NET SCALANCE X202-2P IRT (All versions < V5.5.2).			
		The SSH server on affected devices is configured to			
		offer weak ciphers by default.			
		offer weak cipiters by default.			
		This could allow an unauthorized attacker in a man-			
		in-the-middle position to read and modify any data			
		passed over the connection between legitimate			
		clients and the affected device.			
		A Windows user with basic user authorization can			
		exploit a DLL hijacking attack in SapSetup (Software			
		Installation Program) - version 9.0, resulting in a			
		privilege escalation running code as administrator			
CVE-		of the very same Windows PC. A successful attack			
2023-		depends on various preconditions beyond the			
29187	sap - sapsetup	attackers control.	4/11/2023	7.3	High
CVE-					
2023-		Windows DNS Server Remote Code Execution			
28254	microsoft - multiple products	Vulnerability	4/11/2023	7.2	High
20204		A vulnerability in the web-based management	., 11, 2023	,.2	
		,			
		interface of Cisco Small Business Routers RV016,			
		RV042, RV042G, RV082, RV320, and RV325 Routers			
		could allow an authenticated, remote attacker to			
		execute arbitrary commands on an affected device.			
		This vulnerability is due to improper validation of			
		user input within incoming HTTP packets. An			
		attacker could exploit this vulnerability by sending a			
		crafted HTTP request to the web-based			
		management interface. A successful exploit could			
		allow the attacker to gain root-level privileges and			
		access unauthorized data. To exploit this			
		vulnerability, an attacker would need to have valid			
		administrative credentials on the affected device.			
CVE-		Characher and the second state of the second			
2023-		Cisco has not and will not release software updates	11000000		
20118	cisco - multiple products	that address this vulnerability.	4/13/2023	7.2	High
CVE-		Zoho ManageEngine ADManager Plus through 7180			
2023-		allows for authenticated users to exploit command			
29084	zohocorp - multiple products	injection via Proxy settings.	4/13/2023	7.2	High
CVE-	· • •	In telecom service, there is a missing permission			
2022-		check. This could lead to local denial of service in			
47338	google - multiple products	telecom service.	4/11/2023	7.1	High
CVE-			., 11, 2023	,. .	ייסייי
2023-	and an and the second state of the second	Windows Kennel Else stress (Contribution)	1111 10000	7 4	112.1
28222	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	4/11/2023	7.1	High
CVE-					
2023-		Windows Point-to-Point Protocol over Ethernet			
28224	microsoft - multiple products	(PPPoE) Remote Code Execution Vulnerability	4/11/2023	7.1	High
		A use-after-free flaw was found in btsdio_remove			
		in drivers\bluetooth\btsdio.c in the Linux Kernel. In			
CVE-		this flaw, a call to btsdio_remove with an			
2023-		unfinished job, may cause a race problem leading			
1989		to a UAF on hdev devices.	4/11/2023	7	High
	linux - multiple products		7/11/2023	/	i ligi i
	linux - multiple products				
CVE-	linux - multiple products				
2023-	· ·				
	linux - multiple products microsoft - windows_11_22h2	Win32k Elevation of Privilege Vulnerability	4/11/2023	7	High
2023-	· ·		4/11/2023	7	High
2023- 24914	· ·	Win32k Elevation of Privilege Vulnerability	4/11/2023	7	High
2023- 24914 CVE- 2023-	microsoft - windows_11_22h2	Win32k Elevation of Privilege Vulnerability Windows Advanced Local Procedure Call (ALPC)			
2023- 24914 CVE- 2023- 28216	· ·	Win32k Elevation of Privilege Vulnerability	4/11/2023 4/11/2023	7	High High
2023- 24914 CVE- 2023- 28216 CVE-	microsoft - windows_11_22h2	Win32k Elevation of Privilege Vulnerability Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability			
2023- 24914 CVE- 2023- 28216	microsoft - windows_11_22h2	Win32k Elevation of Privilege Vulnerability Windows Advanced Local Procedure Call (ALPC)			

· · · · · ·			1		1
CVE- 2023-		Windows Error Bonorting Sorvice Elevation of			
2023- 28221	microsoft - multiple products	Windows Error Reporting Service Elevation of Privilege Vulnerability	4/11/2023	7	High
CVE-			1/11/2023	,	
2023-		Windows CNG Key Isolation Service Elevation of			
28229	microsoft - multiple products	Privilege Vulnerability	4/11/2023	7	High
CVE-					
2023- 28273	microsoft - multiple products	Windows Clip Service Elevation of Privilege Vulnerability	4/11/2023	7	High
20275	microsoft - multiple products	A use-after-free vulnerability in the Linux Kernel	4/11/2025	/	півіі
		io_uring system can be exploited to achieve local			
		privilege escalation.			
		The io_file_get_fixed function lacks the presence of			
		ctx->uring_lock which can lead to a Use-After-Free vulnerability due a race condition with fixed files			
		getting unregistered.			
CVE-					
2023-		We recommend upgrading past commit			
1872	linux - linux_kernel	da24142b1ef9fd5d36b76e36bab328a5b27523e8.	4/12/2023	7	High
CVE-					
2023- 28235	microsoft - multiple products	Windows Lock Screen Security Feature Bypass Vulnerability	4/11/2023	6.8	Medium
28235 CVE-	microsoft - multiple products		4/11/2025	0.0	weaturn
2023-		Windows Boot Manager Security Feature Bypass			
28249	microsoft - multiple products	Vulnerability	4/11/2023	6.8	Medium
CVE-					
2023-		Windows Boot Manager Security Feature Bypass			
28269	microsoft - multiple products	Vulnerability	4/11/2023	6.8	Medium
CVE- 2023-		Windows Lock Screen Security Feature Bypass			
28270	microsoft - multiple products	Vulnerability	4/11/2023	6.8	Medium
CVE-		Memory corruption occurs in Modem due to	.,,		
2022-		improper validation of array index when malformed			
33289	qualcomm - 315_5g_iot_modem_firmware	APDU is sent from card.	4/13/2023	6.8	Medium
CVE-		Windows Domain Name Service Remote Code			
2023- 28223	microsoft - multiple products	Execution Vulnerability	4/11/2023	6.6	Medium
CVE-	melosoft - multiple products		4/11/2023	0.0	Weduum
2023-		Windows DNS Server Remote Code Execution			
28255	microsoft - multiple products	Vulnerability	4/11/2023	6.6	Medium
CVE-					
2023-		Windows DNS Server Remote Code Execution	4/44/2022	C C	
28256 CVE-	microsoft - multiple products	Vulnerability	4/11/2023	6.6	Medium
2023-		Windows DNS Server Remote Code Execution			
28278	microsoft - multiple products	Vulnerability	4/11/2023	6.6	Medium
CVE-					
2023-		Windows DNS Server Remote Code Execution			
28305	microsoft - multiple products	Vulnerability	4/11/2023	6.6	Medium
CVE- 2023-		Windows DNS Server Remote Code Execution			
28306	microsoft - multiple products	Vulnerability	4/11/2023	6.6	Medium
CVE-					
2023-		Windows DNS Server Remote Code Execution			
28307	microsoft - multiple products	Vulnerability	4/11/2023	6.6	Medium
CVE-		Windows DNC Convert Dometer Code Evenution			
2023- 28308	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	4/11/2023	6.6	Medium
		socket.c in GNU Screen through 4.9.0, when	.,, 2025	0.0	
		installed setuid or setgid (the default on platforms			
		such as Arch Linux and FreeBSD), allows local users			
CVE-		to send a privileged SIGHUP signal to any PID,			
2023- 24626	anu - seroon	causing a denial of service or disruption of the	4/8/2023	6.5	Medium
24626 CVE-	gnu - screen	target process. Zoho ManageEngine Applications Manager through	4/0/2023	0.5	
2023-		16320 allows the admin user to conduct an XXE			
28340	zohocorp - multiple products	attack.	4/11/2023	6.5	Medium
		In SAP NetWeaver Enterprise Portal - version			
		7.50, an unauthenticated attacker can attach to an			
		open interface and make use of an open API to			
CVE- 2023-		access a service which will enable them to access or modify server settings and data, leading to limited			
2023- 28761	sap - netweaver_enterprise_portal	impact on confidentiality and integrity.	4/11/2023	6.5	Medium
		SAP NetWeaver AS for ABAP and ABAP Platform -	.,, _020	0.0	
		versions 740, 750, 751, 752, 753, 754, 755, 756,			
CVE-		757, 791, allows an attacker authenticated as a			
2023-		non-administrative user to craft a request with			
28763	sap - multiple products	certain parameters which can consume the server's	4/11/2023	6.5	Medium

		resources sufficiently to make it unavailable over			
		the network without any user interaction.			
		SAP NetWeaver AS for ABAP (Business Server Pages) - versions 700, 701, 702, 731, 740, 750, 751,			
		752, 753, 754, 755, 756, 757, allows an attacker			
		authenticated as a non-administrative user to craft			
		a request with certain parameters in certain			
CVE-		circumstances which can consume the server's			
2023-		resources sufficiently to make it unavailable over			
29185	sap - multiple products	the network without any user interaction.	4/11/2023	6.5	Medium
		In SAP NetWeaver (BI CONT ADDON) - versions 707, 737, 747, 757, an attacker can exploit a directory			
		traversal flaw in a report to upload and overwrite			
		files on the SAP server. Data cannot be read but if a			
CVE-		remote attacker has sufficient (administrative)			
2023-		privileges then potentially critical OS files can be			
29186	sap - multiple products	overwritten making the system unavailable.	4/11/2023	6.5	Mediun
		A improper neutralization of special elements used in an sql command ('sql injection') vulnerability			
		[CWE-89] in Fortinet FortiSandbox version 4.2.0,			
		4.0.0 through 4.0.2, 3.2.0 through 3.2.3, 3.1.x and			
		3.0.x allows a remote and authenticated attacker			
CVE-		with read permission to retrieve arbitrary files from			
2022-		the underlying Linux system via a crafted HTTP			
27485 CVE-	fortinet - multiple products	request.	4/11/2023	6.5	Mediun
2023-		Microsoft PostScript and PCL6 Class Printer Driver			
24883	microsoft - multiple products	Information Disclosure Vulnerability	4/11/2023	6.5	Medium
CVE-	· ·				
2023-		Remote Desktop Protocol Client Information			
28267	microsoft - multiple products	Disclosure Vulnerability	4/11/2023	6.5	Medium
CVE- 2023-					
2023- 28288	microsoft - multiple products	Microsoft SharePoint Server Spoofing Vulnerability	4/11/2023	6.5	Medium
CVE-			4/11/2023	0.5	Wealun
2023-		Azure Machine Learning Information Disclosure			
28312	microsoft - azure_machine_learning	Vulnerability	4/11/2023	6.5	Medium
		client.c in gdhcp in ConnMan through 1.41 could be			
0.15		used by network-adjacent attackers (operating a			
CVE- 2023-		crafted DHCP server) to cause a stack-based buffer			
2023- 28488	intel - connman	overflow and denial of service, terminating the connman process.	4/12/2023	6.5	Medium
20100		A local file deletion vulnerability in Palo Alto	1/12/2023	0.5	Incului
		Networks PAN-OS software enables an			
		authenticated administrator to delete files from the			
		local file system with elevated privileges.			
CVE-		These files can include logs and system components			
2023-		that impact the integrity and availability of PAN-OS			
0004	paloaltonetworks - multiple products	software.	4/12/2023	6.5	Medium
		Jenkins Image Tag Parameter Plugin 2.0 improperly			
		introduces an option to opt out of SSL/TLS			
		certificate validation when connecting to Docker			
CVE-		registries, resulting in job configurations using Image Tag Parameters that were created before 2.0			
2023-		having SSL/TLS certificate validation disabled by			
30516	jenkins - image_tag_parameter	default.	4/12/2023	6.5	Medium
		A missing permission check in Jenkins Report Portal			
		Plugin 0.5 and earlier allows attackers with			
CVE-		Overall/Read permission to connect to an attacker-			
2023- 30526	ionking report portal	specified URL using attacker-specified bearer token authentication.	4/12/2023	6.5	Medium
50520	jenkins - report_portal	Jenkins WSO2 Oauth Plugin 1.0 and earlier does not	7/12/2023	0.5	weuluff
CVE-		mask the WSO2 Oauth client secret on the global			
2023-		configuration form, increasing the potential for			
30528	jenkins - wso2_oauth	attackers to observe and capture it.	4/12/2023	6.5	Medium
		Jenkins Consul KV Builder Plugin 2.0.13 and earlier			
CVE-		does not mask the HashiCorp Consul ACL Token on			
2023- 30531	ionking - consul by huildor	the global configuration form, increasing the potential for attackers to observe and capture it.	4/12/2023	6.5	Medium
70721	jenkins - consul_kv_builder	A missing permission check in Jenkins TurboScript	4/12/2023	0.5	
CVE-		Plugin 1.3 and earlier allows attackers with			
2023-		Item/Read permission to trigger builds of jobs			
30532	jenkins - turboscript	corresponding to the attacker-specified repository.	4/12/2023	6.5	Medium
	······	In spring framework versions prior to 5.2.24			
CVE-		release+ ,5.3.27+ and 6.0.8+ , it is possible for a			
2023- 20863			110 100	<u> </u>	
CVE- 2023-		release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression			
	vmware - multiple products	that may cause a denial-of-service (DoS) condition.	4/13/2023	6.5	Mediu

		In Spring Session version 3.0.0, the session id can be			
		logged to the standard output stream. This			
		vulnerability exposes sensitive information to those			
0.5		who have access to the application logs and can be			
CVE- 2023-		used for session hijacking. Specifically, an			
2023-20866	vmware - spring session	application is vulnerable if it is using HeaderHttpSessionIdResolver.	4/13/2023	6.5	Medium
20800	vmware - spring_session	In SAP CRM - versions 700, 701, 702, 712, 713, an	4/15/2025	0.5	weulum
		attacker who is authenticated with a non-			
		administrative role and a common remote			
		execution authorization can use a vulnerable			
		interface to execute an application function to			
		perform actions which they would not normally be			
		permitted to perform. Depending on the function			
CVE-		executed, the attack can can have limited impact on			
2023-		confidentiality and integrity of non-critical user or			
27897	sap - multiple products	application data and application availability.	4/11/2023	6.3	Medium
		A vulnerability has been identified in SIMATIC			
		IPC1047 (All versions), SIMATIC IPC1047E (All			
		versions with maxView Storage Manager <			
		4.09.00.25611 on Windows), SIMATIC IPC647D (All			
		versions), SIMATIC IPC647E (All versions with			
		maxView Storage Manager < 4.09.00.25611 on			
		Windows), SIMATIC IPC847D (All versions), SIMATIC			
		IPC847E (All versions with maxView Storage			
		Manager < 4.09.00.25611 on Windows). The			
		Adaptec Maxview application on affected devices is			
		using a non-unique TLS certificate across			
		installations to protect the communication from the			
		local browser to the local application.			
		A local attacker may use this key to deep ut			
CVE-		A local attacker may use this key to decrypt intercepted local traffic between the browser and			
2023-		the application and could perform a man-in-the-			
2023-	siemens - simatic ipc647d firmware	middle attack in order to modify data in transit.	4/11/2023	6.3	Medium
23300	sichens sinade_peo+/d_innware	A local file deletion vulnerability in the Palo Alto	4/11/2023	0.5	Wiculum
		Networks GlobalProtect app on Windows devices			
CVE-		enables a user to delete system files from the			
2023-		endpoint with elevated privileges through a race			
0006	paloaltonetworks - multiple products	condition.	4/12/2023	6.3	Medium
		Veritas Appliance v4.1.0.1 is affected by Host			
		Header Injection attacks. HTTP host header can be			
		manipulated and cause the application to behave in			
CVE-		unexpected ways. Any changes made to the header			
2023-		would just cause the request to be sent to a			
26788	veritas - netbackup_appliance_firmware	completely different Domain/IP address.	4/10/2023	6.1	Medium
		Stored Cross site scripting (XSS) vulnerability in			
		Zoho ManageEngine Applications Manager through			
CVE-		16340 allows an unauthenticated user to inject			
2023-		malicious javascript on the incorrect login details			
28341	zohocorp - multiple products	page.	4/11/2023	6.1	Medium
		SAP GUI for HTML - versions KERNEL 7.22, 7.53,			
		7.54, 7.77, 7.81, 7.85, 7.89, 7.91, KRNL64UC, 7.22,			
		7.22EXT, KRNL64UC 7.22, 7.22EXT does not			
		sufficiently encode user-controlled inputs, resulting			
		in a reflected Cross-Site Scripting (XSS)			
		vulnerability. An attacker could craft a malicious			
		URL and lure the victim to click, the script supplied by the attacker will execute in the victim user's			
CVE-		browser. The information from the victim's web			
2023-		browser can either be modified or read and sent to			
2023-27499	sap - multiple products	the attacker.	4/11/2023	6.1	Medium
21733		An improper neutralization of script-related HTML	7/ 11/ 2023	0.1	wiculum
		tags in a web page vulnerability [CWE-80] in			
		FortiAuthenticator versions 6.4.0 through 6.4.4,			
		6.3.0 through 6.3.3, all versions of 6.2 and 6.1 may			
CVE-		allow a remote unauthenticated attacker to trigger			
2022-		a reflected cross site scripting (XSS) attack via the			
35850	fortinet - multiple products	"reset-password" page.	4/11/2023	6.1	Medium
-	· · · · · · · · · · · · · · · · · · ·	An improper neutralization of input during web			1
		page generation vulnerability ('Cross-site Scripting')			
		[CWE-79] in Fortinet FortiOS version 7.2.0 through			
		7.2.3, version 7.0.0 through 7.0.9, version 6.4.0			
1		through 6.4.11 and before 6.2.12 and FortiProxy			
					1
CVE-		version 7.2.0 through 7.2.1 and before 7.0.7 allows			
CVE- 2022-		- · · · · · · · · · · · · · · · · · · ·			
	fortinet - multiple products	version 7.2.0 through 7.2.1 and before 7.0.7 allows	4/11/2023	6.1	Medium
2022- 41330 CVE-	fortinet - multiple products	 version 7.2.0 through 7.2.1 and before 7.0.7 allows an unauthenticated attacker to perform an XSS attack via crafted HTTP GET requests. An improper neutralization of input during web 	4/11/2023	6.1	Medium
2022- 41330	fortinet - multiple products fortinet - multiple products	version 7.2.0 through 7.2.1 and before 7.0.7 allows an unauthenticated attacker to perform an XSS attack via crafted HTTP GET requests.	4/11/2023	6.1	Medium

CVE- 2023- 24995 microsoft - edge_chromium CVE- 2023- 28313 send_customer_voice_survey_from_dynamics_365 CVE- 2023- 28368 microsoft - multiple products CVE- 2022- 28368 tp-link - multiple products CVE- 2022- 2022- 46703 apple - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2023- 28226 micr	C A all versions C 2 all versions C 1 all versions and			
2023- 24935microsoft - edge_chromiumCVE- 2023- 28314microsoft - survey_from_dynamics_365CVE- 2023- 28368microsoft - multiple productsCVE- 2023- 28368tp-link - multiple productsCVE- 2023- 28368tp-link - multiple productsCVE- 2022- 46703apple - multiple productsCVE- 2022- 447355google - multiple productsCVE- 2022- 44735google - multiple productsCVE- 2022- 447363google - multiple productsCVE- 2022- 447364google - multiple productsCVE- 2022- 447365google - multiple productsCVE- 2022- 447365google - multiple productsCVE- 2022- 447465google - multiple productsCVE- 2022- 44465google - multiple productsCVE- <b< th=""><th>6.4 all versions, 6.2 all versions, 6.1 all versions and 6.0 all versions may allow an unauthenticated and</th><th></th><th></th><th></th></b<>	6.4 all versions, 6.2 all versions, 6.1 all versions and 6.0 all versions may allow an unauthenticated and			
2023- 24935microsoft - edge_chromiumCVE- 2023- 28313send_customer_voice_survey_from_dynamics_365CVE- 2023- 28314microsoft - multiple productsCVE- 2023- 28368tp-link - multiple productsCVE- 2023- 2024- 2022- 2025- 2025- 2025- 2025- 2026- 2026- 2027- 2027- 2027- 2028- 2028- 2029- 2028- 2029- <	remote attacker to perform a reflected cross site			
2023- 24935microsoft - edge_chromiumCVE- 2023- 28313send_customer_voice_survey_from_dynamics_365CVE- 2023- 28314microsoft - multiple productsCVE- 2023- 28368tp-link - multiple productsCVE- 2023- 2024- 2022- 2025- 2025- 2025- 2025- 2026- 2026- 2027- 2027- 2027- 2028- 2028- 2029- 2028- 2029- <	scripting attack (XSS) via injecting malicious payload			
2023- 24935microsoft - edge_chromiumCVE- 2023- 28313send_customer_voice_survey_from_dynamics_365CVE- 2023- 28314microsoft - multiple productsCVE- 2023- 28368tp-link - multiple productsCVE- 2023- 2024- 2022- 2025- 2025- 2025- 2025- 2026- 2026- 2027- 2027- 2027- 2028- 2028- 2029- 2028- 2029- <	in log entries used to build report.			
24935microsoft - edge_chromiumCVE- 2023- send_customer_voice_survey_from_dynamics_365CVE- 2023- 2831428314microsoft - multiple productsCVE- 2023- 28368CVE- 2023- 28368CVE- 2022- 46703CVE- 2022- 2022- 47335google - multiple productsCVE- 2022- 2022- 47337google - multiple productsCVE- 2022- 47337google - multiple productsCVE- 2022- 47337google - multiple productsCVE- 2022- 47337google - multiple productsCVE- 2022- 47362google - multiple productsCVE- 2022- 47362google - multiple productsCVE- 2022- 47362google - multiple productsCVE- 2022- 47464google - multiple productsCVE- 2022- 47465google - multiple productsCVE- 2022- 47464google - multiple productsCVE- 2022- 474652022- 47466google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2023- 20				
CVE- 2023- 28313 microsoft - 28313 send_customer_voice_survey_from_dynamics_365 CVE- 2023- 28314 microsoft - multiple products CVE- 2023- 28368 tp-link - multiple products CVE- 2022- 28368 tp-link - multiple products CVE- 2022- 246703 apple - multiple products CVE- 2022- 247335 google - multiple products CVE- 2022- 247336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47363 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2023- 222- 47468 google - multiple products <td< td=""><td>Microsoft Edge (Chromium-based) Spoofing Vulnerability</td><td>4/11/2023</td><td>6.1</td><td>Medium</td></td<>	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4/11/2023	6.1	Medium
2023- 28313microsoft - survey_from_dynamics_365CVE- 2023- 28314microsoft - multiple productsCVE- 2023- 28368tp-link - multiple productsCVE- 2022- 2022- 2022- 2022- 2022- 2022- 2023- 2023- 2023- 2022- 2023- 2024- 2022- 2024- 2022- 2025- 2022- 2025- 2022- 2026- 2022- 2026- 2022- 2026- 2027- 2026- 2027- 2027- 2027- 2028- 2029- 2029- 2029- 2029- 2029- 2029- 2029- 2020- 		4/11/2023	0.1	WEUlulli
CVE- 21 21 21 28314 microsoft - multiple products 28314 microsoft - multiple products 28368 tp-link - multiple products CVE- 2023- 28368 tp-link - multiple products CVE- 2022- 46703 apple - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47363 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 202- 47465 google - multiple products<	Microsoft Dynamics 365 Customer Voice Cross-Site			
2023- 28314 microsoft - multiple products CVE- 2023- 28368 tp-link - multiple products CVE- 2022- 47335 apple - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 42477 fortinet - multiple products <td>Scripting Vulnerability</td> <td>4/11/2023</td> <td>6.1</td> <td>Medium</td>	Scripting Vulnerability	4/11/2023	6.1	Medium
28314 microsoft - multiple products CVE- 2023- 28368 tp-link - multiple products CVE- 2022- 46703 apple - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47453 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 goo				
CVE- 2023- 28368 tp-link - multiple products CVE- 2022- 46703 apple - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47469 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47469 google - multiple products CVE- 2022- 47469 google - multiple products CVE- 2023- 47469 google - multiple products CVE- 2023- 42477 fortinet - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products	Microsoft Dynamics 365 (on-premises) Cross-site			
2023- 28368 tp-link - multiple products CVE- 2022- 46703 apple - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47338 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 42477 fortinet - multiple products CVE- 2023- 28228 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products <	Scripting Vulnerability	4/11/2023	6.1	Medium
2023- 28368 tp-link - multiple products CVE- 2022- 46703 apple - multiple products CVE- 2022- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47338 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47469 google - multiple products CVE- 2022- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- google - multiple products	TP-Link L2 switch T2600G-28SQ firmware versions prior to 'T2600G-28SQ(UN)_V1_1.0.6 Build			
2023- 28368 tp-link - multiple products CVE- 2022- 46703 apple - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47338 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 42477 fortinet - multiple products CVE- 2023- 28228 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products <	20230227' uses vulnerable SSH host keys. A fake			
2023- 28368 tp-link - multiple products CVE- 2022- 46703 apple - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47338 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 42477 fortinet - multiple products CVE- 2023- 28228 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products <	device may be prepared to spoof the affected			
2023- 28368 tp-link - multiple products CVE- 2022- 46703 apple - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47338 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 42477 fortinet - multiple products CVE- 2022- 42477 fortinet - multiple products CVE- 2023- 28228 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products	device with the vulnerable host key. If the			
28368 tp-link - multiple products CVE-	administrator may be tricked to login to the fake			
CVE- 2022- 46703 apple - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple p	device, the credential information for the affected	4/44/2022		
2022- 46703 apple - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 42477 fortinet - mu	device may be obtained.	4/11/2023	5.7	Medium
2022- 46703 apple - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 42477 fortinet - multiple products CVE- 2022- 42477 fortinet - multiple products CVE- 2023- 28228 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura			
2022- 46703 apple - multiple products CVE- 2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 42477 fortinet - mu	13.1, iOS 16.2 and iPadOS 16.2, iOS 15.7.2 and			
CVE-2022-47335google - multiple productsCVE-2022-47336google - multiple productsCVE-2022-47362google - multiple productsCVE-2022-47363google - multiple productsCVE-2022-47463google - multiple productsCVE-2022-47463google - multiple productsCVE-2022-47464google - multiple productsCVE-2022-47465google - multiple productsCVE-2022-47466google - multiple productsCVE-2022-47467google - multiple productsCVE-2022-47468google - multiple productsCVE-2022-47468google - multiple productsCVE-2022-42477fortinet - multiple productsCVE-2023-28228microsoft - multiple productsCVE-2023-28253microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-28263microsoft - multiple products<	iPadOS 15.7.2. An app may be able to read sensitive			
2022- 47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47337 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47458 google - multiple products CVE- 2023- 2022- 202- <td>location information</td> <td>4/10/2023</td> <td>5.5</td> <td>Medium</td>	location information	4/10/2023	5.5	Medium
47335 google - multiple products CVE- 2022- 47336 google - multiple products CVE- 2022- 2022- 2022- 47337 google - multiple products CVE- 2022- 47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2023- 2022- <td>In telecom service, there is a missing permission</td> <td></td> <td></td> <td></td>	In telecom service, there is a missing permission			
CVE- 2022- 47336google - multiple productsCVE- 2022- 47337google - multiple productsCVE- 2022- 47362google - multiple productsCVE- 2022- 47463google - multiple productsCVE- 2022- 47464google - multiple productsCVE- 2022- 47465google - multiple productsCVE- 2022- 47465google - multiple productsCVE- 2022- 47465google - multiple productsCVE- 2022- 47465google - multiple productsCVE- 2022- 47466google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 42477fortinet - multiple productsCVE- 2023- 2023- 28228microsoft - multiple productsCVE- 2023- 28263microsoft - multiple productsCVE- 2023- 28263microsoft - multiple productsCVE- 2023- 28263microsoft - multiple products	check. This could lead to local denial of service in	4/11/2022		
2022-47336google - multiple productsCVE-2022-47337google - multiple productsCVE-2022-47463google - multiple productsCVE-2022-47463google - multiple productsCVE-2022-47464google - multiple productsCVE-2022-47465google - multiple productsCVE-2022-47466google - multiple productsCVE-2022-47466google - multiple productsCVE-2022-47467google - multiple productsCVE-2022-47468google - multiple productsCVE-2022-47468google - multiple productsCVE-2022-47468google - multiple productsCVE-2022-42477fortinet - multiple productsCVE-2023-28228microsoft - multiple productsCVE-2023-28253microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-28263282642826528265 <td>telecom service. In telecom service, there is a missing permission</td> <td>4/11/2023</td> <td>5.5</td> <td>Medium</td>	telecom service. In telecom service, there is a missing permission	4/11/2023	5.5	Medium
47336 google - multiple products CVE- google - multiple products	check. This could lead to local denial of service in			
2022-47337google - multiple productsCVE-2022-47362google - multiple productsCVE-2022-47463google - multiple productsCVE-2022-47464google - multiple productsCVE-2022-47465google - multiple productsCVE-2022-47466google - multiple productsCVE-2022-47466google - multiple productsCVE-2022-47467google - multiple productsCVE-2022-47468google - multiple productsCVE-2022-47468google - multiple productsCVE-2022-47468google - multiple productsCVE-2022-42477fortinet - multiple productsCVE-2023-28228microsoft - multiple productsCVE-2023-28253microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-2826328263CVE-2023-2826328263CVE-2023-282	telecom service.	4/11/2023	5.5	Medium
47337 google - multiple products CVE- google - multiple products	In media service, there is a missing permission			
CVE- 2022- 47362google - multiple productsCVE- 2022- 47463google - multiple productsCVE- 2022- 47464google - multiple productsCVE- 2022- 47465google - multiple productsCVE- 2022- 47466google - multiple productsCVE- 2022- 47466google - multiple productsCVE- 2022- 47467google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 42477fortinet - multiple productsCVE- 2023- 28228microsoft - multiple productsCVE- 2023- 28253microsoft - multiple productsCVE- 2023- 28263microsoft - multiple productsCVE- 2023- 28263microsoft - multiple productsCVE- 2023- 28263microsoft - multiple products	check. This could lead to local denial of service in	4/44/2022		
2022- google - multiple products CVE- google - multiple products 2022- google - multiple products CVE- google - multiple products	media service. In telecom service, there is a missing permission	4/11/2023	5.5	Medium
47362 google - multiple products CVE- 2022- 47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 42477 fortinet - multiple products CVE- 2023- 28228 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products <td>check. This could lead to local denial of service in</td> <td></td> <td></td> <td></td>	check. This could lead to local denial of service in			
2022- 47463 google - multiple products CVE- goo	telecom service.	4/11/2023	5.5	Medium
47463 google - multiple products CVE- 2022- 47464 google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 42477 fortinet - multiple products CVE- 2023- 28228 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products CVE- 2023- 28263	In telecom service, there is a missing permission			
CVE- 2022- 47464google - multiple productsCVE- 2022- 47465google - multiple productsCVE- 2022- 47466google - multiple productsCVE- 2022- 47467google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 42477fortinet - multiple productsCVE- 2023- 28228microsoft - multiple productsCVE- 2023- 28253microsoft - multiple productsCVE- 2023- 28263microsoft - multiple products	check. This could lead to local denial of service in			
2022- 47464 google - multiple products CVE- google - multiple products 2022- google - multiple products CVE- google - multiple products Google - multiple produc	telecom service.	4/11/2023	5.5	Medium
47464 google - multiple products CVE- google - multiple products CVE- 2022- 47465 google - multiple products CVE- 2022- 47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 42477 fortinet - multiple products CVE- 2023- 28228 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products	In telecom service, there is a missing permission check. This could lead to local denial of service in			
CVE- 2022- 47465google - multiple productsCVE- 2022- 47466google - multiple productsCVE- 2022- 47467google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 42477fortinet - multiple productsCVE- 2023- 28228microsoft - multiple productsCVE- 2023- 28253microsoft - multiple productsCVE- 2023- 28263microsoft - multiple products	telecom service.	4/11/2023	5.5	Medium
47465 google - multiple products CVE- google - multiple products CVE- 2022- 47466 google - multiple products CVE- google - multiple products Google -	In vdsp service, there is a missing permission check.			
CVE- 2022- 47466google - multiple productsCVE- 2022- 47467google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 42477fortinet - multiple productsCVE- 2023- 28228microsoft - multiple productsCVE- 2023- 28253microsoft - multiple productsCVE- 2023- 28263microsoft - multiple products	This could lead to local denial of service in vdsp			
2022-47466google - multiple productsCVE-2022-47467google - multiple productsCVE-2022-47468google - multiple productsCVE-2022-42477fortinet - multiple productsCVE-2023-28228microsoft - multiple productsCVE-2023-28253microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-283-283-283-	service.	4/11/2023	5.5	Medium
47466 google - multiple products CVE- 2022- 47467 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 47468 google - multiple products CVE- 2022- 42477 fortinet - multiple products CVE- 2023- 28228 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products	In telecom service, there is a missing permission check. This could lead to local denial of service in			
CVE- 2022- 47467google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 47468google - multiple productsCVE- 2022- 42477fortinet - multiple productsCVE- 2023- 28228microsoft - multiple productsCVE- 2023- 28253microsoft - multiple productsCVE- 2023- 28253microsoft - multiple productsCVE- 2023- 28253microsoft - multiple productsCVE- 2023- 28253microsoft - multiple products	telecom service.	4/11/2023	5.5	Medium
2022-47467google - multiple productsCVE-2022-47468google - multiple productsCVE-2022-42477fortinet - multiple productsCVE-2023-28228microsoft - multiple productsCVE-2023-28253microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-2826328263CVE-2023-28263282632023-2023-282632023-2023-2023-2023-282632023-	In telecom service, there is a missing permission	,, _020		
CVE- 2022- 47468google - multiple productsCVE- 2022- 42477fortinet - multiple productsCVE- 2023- 28228microsoft - multiple productsCVE- 2023- 28253microsoft - multiple productsCVE- 2023- 28253microsoft - multiple productsCVE- 2023- 28253microsoft - multiple productsCVE- 2023- 28263microsoft - multiple products	check. This could lead to local denial of service in			
2022- 47468google - multiple productsCVE- 2022- 42477fortinet - multiple productsCVE- 2023- 28228microsoft - multiple productsCVE- 2023- 28253microsoft - multiple productsCVE- 2023- 28253microsoft - multiple productsCVE- 2023- 28253microsoft - multiple productsCVE- 2023- 28263microsoft - multiple products	telecom service.	4/11/2023	5.5	Medium
47468google - multiple productsCVE-2022-42477fortinet - multiple productsCVE-2023-28228microsoft - multiple productsCVE-2023-28253microsoft - multiple productsCVE-2023-28253microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-28263CVE-2023-28263microsoft - multiple productsCVE-2023-28263Microsoft - multiple productsCVE-2023-<	In telecom service, there is a missing permission			
CVE- 2022- 42477 fortinet - multiple products CVE- 2023- 28228 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products CVE- 2023- 28263 2023- 2023- 2023-	check. This could lead to local denial of service in telecom service.	4/11/2023	5.5	Medium
2022-42477fortinet - multiple productsCVE-2023-28228microsoft - multiple productsCVE-2023-28253microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-28263CVE-2023-2826328263CVE-2023-2023-2023-	An improper input validation vulnerability [CWE-20]	4/11/2025	5.5	weulum
2022-42477fortinet - multiple productsCVE-2023-28228microsoft - multiple productsCVE-2023-28253microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-2023-28263CVE-2023-28263CVE-2023-2023-2023-	in FortiAnalyzer version 7.2.1 and below, version			
42477fortinet - multiple productsCVE-2023-28228microsoft - multiple productsCVE-2023-28253microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-28263CVE-2023-28263CVE-2023-	7.0.6 and below, 6.4 all versions may allow an			
CVE- 2023- 28228 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products CVE- 2023- 28263 CVE- 2023-	authenticated attacker to disclose file system		_	
2023-28228microsoft - multiple productsCVE-2023-28253microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-28263CVE-2023-	information via custom dataset SQL queries.	4/11/2023	5.5	Medium
28228microsoft - multiple productsCVE-2023-28253microsoft - multiple productsCVE-2023-28263microsoft - multiple productsCVE-2023-28263CVE-2023-				
CVE- 2023- 28253 microsoft - multiple products CVE- 2023- 28263 microsoft - multiple products CVE- 2023- 28263 CVE- 2023- 2023- 2023- 2023-	Windows Spoofing Vulnerability	4/11/2023	5.5	Medium
2023- 28253microsoft - multiple productsCVE- 2023-microsoft - multiple products28263microsoft - multiple productsCVE- 2023-		.,, _020	2.2	
CVE- 2023- 28263 microsoft - multiple products CVE- 2023-	Windows Kernel Information Disclosure			
2023- 28263microsoft - multiple productsCVE- 2023-	Vulnerability	4/11/2023	5.5	Medium
28263microsoft - multiple productsCVE-2023-				
CVE- 2023-	Visual Studio Information Disclosure Vulnerability	4/11/2023	5.5	Medium
2023-		7/11/2023	د.ر	weuluin
	Windows Common Log File System Driver			
	Information Disclosure Vulnerability	4/11/2023	5.5	Medium
CVE-				
2023-28271microsoft - multiple products	Windows Kernel Memory Information Disclosure Vulnerability	4/11/2023	5.5	Medium

CVE-					
2023-					
28298	microsoft - multiple products	Windows Kernel Denial of Service Vulnerability	4/11/2023	5.5	Medium
CVE-					
2023-		Minuel Chudie, Constitute Mula analylity	4/44/2022		N 4 a alterna
28299	microsoft - multiple products	Visual Studio Spoofing Vulnerability Adobe Dimension version 3.4.8 (and earlier) is	4/11/2023	5.5	Medium
		affected by an out-of-bounds read vulnerability that			
		could lead to disclosure of sensitive memory. An			
		attacker could leverage this vulnerability to bypass			
CVE-		mitigations such as ASLR. Exploitation of this issue			
2023-		requires user interaction in that a victim must open			
26374	adobe - dimension	a malicious file.	4/12/2023	5.5	Medium
		Adobe Dimension version 3.4.8 (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			
CVE-		mitigations such as ASLR. Exploitation of this issue			
2023-		requires user interaction in that a victim must open			
26375	adobe - dimension	a malicious file.	4/12/2023	5.5	Medium
		Adobe Dimension version 3.4.8 (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			
CVE-		mitigations such as ASLR. Exploitation of this issue			
2023-		requires user interaction in that a victim must open			
26376	adobe - dimension	a malicious file.	4/12/2023	5.5	Medium
		Adobe Dimension version 3.4.8 (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			
CVE-		mitigations such as ASLR. Exploitation of this issue			
2023-		requires user interaction in that a victim must open			
26377	adobe - dimension	a malicious file.	4/12/2023	5.5	Medium
		Adobe Dimension version 3.4.8 (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			
CVE-		mitigations such as ASLR. Exploitation of this issue			
2023-		requires user interaction in that a victim must open			
26378	adobe - dimension	a malicious file.	4/12/2023	5.5	Medium
		Adobe Dimension version 3.4.8 (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			
CVE-		mitigations such as ASLR. Exploitation of this issue			
2023-		requires user interaction in that a victim must open			
26379	adobe - dimension	a malicious file.	4/12/2023	5.5	Medium
		Adobe Dimension version 3.4.8 (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			
CVE-		mitigations such as ASLR. Exploitation of this issue			
2023-		requires user interaction in that a victim must open			
26380	adobe - dimension	a malicious file.	4/12/2023	5.5	Medium
		Adobe Dimension version 3.4.8 (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			
CVE-		mitigations such as ASLR. Exploitation of this issue			
2023-		requires user interaction in that a victim must open			
26381	adobe - dimension	a malicious file.	4/12/2023	5.5	Medium
		Adobe Dimension version 3.4.8 (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			
CVE-		mitigations such as ASLR. Exploitation of this issue			
2023-		requires user interaction in that a victim must open			
26382	adobe - dimension	a malicious file.	4/12/2023	5.5	Medium
		Adobe Dimension version 3.4.8 (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			
CVE-		mitigations such as ASLR. Exploitation of this issue			
2023-		requires user interaction in that a victim must open			
26400	adobe - dimension	a malicious file.	4/12/2023	5.5	Medium
CVE-		Adobe Dimension version 3.4.8 (and earlier) is			
2023- 26401	adobe - dimension	affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An	4/12/2023	5.5	Medium

			,		
		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 Dimension version 3.4.8 (and earlier) is			
		affected by an out-of-bounds read vulnerability that			
		could lead to disclosure of sensitive memory. An			
0.15		attacker could leverage this vulnerability to bypass			
CVE-		mitigations such as ASLR. Exploitation of this issue			
2023-		requires user interaction in that a victim must open			
26404	adobe - dimension	a malicious file.	4/12/2023	5.5	Medium
		Adobe Acrobat Reader versions 23.001.20093 (and			
		earlier) and 20.005.30441 (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			
CVE-		mitigations such as ASLR. Exploitation of this issue			
2023-		requires user interaction in that a victim must open			
26397	adobe - multiple products	a malicious file.	4/12/2023	5.5	Medium
20357		Adobe Substance 3D Stager version 2.0.1 (and	4/12/2023	J.J	weulum
		earlier) is affected by an out-of-bounds read			
		vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this			
CVE-		vulnerability to bypass mitigations such as ASLR.			
2023-		Exploitation of this issue requires user interaction in			
26385	adobe - substance_3d_stager	that a victim must open a malicious file.	4/12/2023	5.5	Medium
		Adobe Substance 3D Stager version 2.0.1 (and	., 12, 2025		
		earlier) is affected by an Access of Uninitialized			
		Pointer vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this			
CVE-		vulnerability to bypass mitigations such as ASLR.			
2023-		Exploitation of this issue requires user interaction in			
26386	adobe - substance 3d stager	that a victim must open a malicious file.	4/12/2023	5.5	Medium
		Adobe Substance 3D Stager version 2.0.1 (and	, ,		
		earlier) is affected by an Access of Uninitialized			
		Pointer vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this			
CVE-		vulnerability to bypass mitigations such as ASLR.			
2023-		Exploitation of this issue requires user interaction in			
26387	adobe - substance_3d_stager	that a victim must open a malicious file.	4/12/2023	5.5	Medium
		Adobe Substance 3D Stager version 2.0.1 (and			
		earlier) is affected by an out-of-bounds read			
		vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this			
CVE-		vulnerability to bypass mitigations such as ASLR.			
2023-		Exploitation of this issue requires user interaction in			
26403	adobe - substance_3d_stager	that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-		HPE OneView virtual appliance "Migrate server			
2023-		hardware" option may expose sensitive information			
28091	hp - oneview	in an HPE OneView support dump	4/14/2023	5.5	Medium
CVE-					
2023-		Microsoft Defender Security Feature Bypass			
24934	microsoft - malware_protection_engine	Vulnerability	4/14/2023	5.5	Medium
		The SAP Application Interface (Message Dashboard)			
		- versions AIF 703, AIFX 702, S4CORE 100, 101,			
		SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E,			
		application allows the usage HTML tags. An			
		authorized attacker can use some of the basic			
		HTML codes such as heading, basic formatting and			
		lists, then an attacker can inject images from the			
CVE-		foreign domains. After successful exploitations, an			
2023-		attacker can cause limited impact on the			
29110	sap - multiple products	confidentiality and integrity of the application.	4/11/2023	5.4	Medium
		The SAP Application Interface (Message			
		Monitoring) - versions 600, 700, allows an			
		authorized attacker to input links or headings with			
		custom CSS classes into a comment. The comment			
		will render links and custom CSS classes as HTML			
CVE-		objects. After successful exploitations, an attacker			
2023-		can cause limited impact on the confidentiality and	1/11/2000		
29112	sap - multiple products	integrity of the application.	4/11/2023	5.4	Medium
		SAP CRM (WebClient UI) - versions S4FND 102, 103,			
		104, 105, 106, 107, WEBCUIF, 700, 701, 731, 730,			
		746, 747, 748, 800, 801, allows an authenticated			
		attacker to modify HTTP verbs used in requests to			
		the web server. This application is exposed over the			
CVE-					
CVE- 2023- 29189	sap - multiple products	network and successful exploitation can lead to exposure of form fields	4/11/2023	5.4	Medium

CVE- 2022- 43952 CVE- 2023-	fortinet - multiple products	 An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiADC version 7.1.1 and below, version 7.0.3 and below, version 6.2.5 and below may allow an authenticated attacker to perform a cross-site scripting attack via crafted HTTP requests. A url redirection to untrusted site ('open redirect') in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.9, FortiOS versions 6.4.0 through 6.4.12, FortiOS all versions 6.2, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.2, FortiProxy version 7.0.0 through 7.0.9 through 7.2.9 thr	4/11/2023	5.4	Medium
22641 CVE-	fortinet - multiple products	specially crafted requests.	4/11/2023	5.4	Medium
2023- 28309	microsoft - multiple products	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	4/11/2023	5.4	Medium
CVE- 2023- 30520	jenkins - quay.io_trigger	Jenkins Quay.io trigger Plugin 0.1 and earlier does not limit URL schemes for repository homepage URLs submitted via Quay.io trigger webhooks, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to submit crafted Quay.io trigger webhook payloads. SAP NetWeaver AS Java for Deploy Service - version	4/12/2023	5.4	Medium
CVE- 2023- 24527 CVE- 2023-	sap - netweaver_as_java_for_deploy_service	 7.5, does not perform any access control checks for functionalities that require user identity enabling an unauthenticated attacker to attach to an open interface and make use of an open naming and directory API to access a service which will enable them to access but not modify server settings and data with no effect on availability and integrity. The IP filter in ABAP Platform and SAP Web Dispatcher - versions WEBDISP 7.85, 7.89, KERNEL 7.85, 7.89, 7.91, may be vulnerable by erroneous IP netmask handling. This may enable access to 	4/11/2023	5.3	Medium
29108	sap - multiple products	backend applications from unwanted sources.	4/11/2023	5.3	Medium
		Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Software Foundation Apache InLong. This issue affects Apache InLong: from 1.4.0 through 1.5.0. By manipulating the "orderType" parameter and the ordering of the returned content using an SQL injection attack, an attacker can extract the username of the user with ID 1 from the "user" table, one character at a time. Users are advised to upgrade to Apache InLong's 1.6.0 or cherry-pick [1] to solve it. https://programmer.help/blogs/jdbc-			
CVE-		deserialization-vulnerability-learning.html			
2023- 30465	apache - multiple products	[1] https://github.com/apache/inlong/issues/7529 https://github.com/apache/inlong/issues/7529	4/11/2023	5.3	Medium
CVE- 2023-		Remote Procedure Call Runtime Information			
21729	microsoft - multiple products	Disclosure Vulnerability	4/11/2023	5.3	Medium
CVE- 2023- 28226	microsoft - multiple products	Windows Enroll Engine Security Feature Bypass Vulnerability An issue was discovered in x509/x509_verify.c in	4/11/2023	5.3	Medium
CVE- 2022- 48437 CVE- 2023-	openbsd - multiple products	LibreSSL before 3.6.1, and in OpenBSD before 7.2 errata 001. x509_verify_ctx_add_chain does not store errors that occur during leaf certificate verification, and therefore an incorrect error is returned. This behavior occurs when there is an installed verification callback that instructs the verifier to continue upon detecting an invalid certificate. Jenkins NeuVector Vulnerability Scanner Plugin 1.22 and earlier unconditionally disables SSL/TLS certificate and hostname validation when connecting to a configured NeuVector Vulnerability	4/12/2023	5.3	Medium
30517	jenkins - neuvector_vulnerability_scanner	Scanner server.	4/12/2023	5.3	Medium
CVE- 2023- 30519	jenkins - quay.io_trigger	A missing permission check in Jenkins Quay.io trigger Plugin 0.1 and earlier allows	4/12/2023	5.3	Medium

CVE- Jenkins Report Portal Plugin 0.5 and earlier stores 2023- ReportPortal access tokens unencrypted in job 30523 jenkins - report_portal 1 Jenkins Report Portal Plugin 0.5 and earlier stores 2023- with Item/Extended Read permission or access to 30523 jenkins - report_portal 1 Jenkins Report Portal Plugin 0.5 and earlier does CVE- Ite Jenkins Report Portal Plugin 0.5 and earlier does CVE- Jenkins Report Portal Plugin 0.5 and earlier does CVE- Ite configuration form, increasing the potential for 30524 jenkins - report_portal 30524 jenkins - report_portal 30524 jenkins - report_portal 30524 jenkins - report_portal 30520 attackers to observe and capture them. 4/12/2023 4.3 Medium Jenkins WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth Client secret unencrypted in the global config.xml file on the Jenkins controller vol23- where it can be viewed by users with access to the								
CvE. A missing permission check in alexins assemble allows unsubterificated starkers to trigger builds of box corresponding to the attacker-specified allows unsubterificated attackers to trigger builds of box corresponding to the attacker-specified allows unsubterificated attackers to trigger builds of box corresponding to the attacker-specified allows unsubterificated attackers to trigger builds of box corresponding to the attacker of specified allows unsubterificated attributing to the attacker of the 4/11/2023 4.9 2023 microsoft - windows server 2022 Vulnerability in PAB ATO Networds PAN-65 software analysis an subterificated attributing to specificate the analysis of actes to specific the diverse of the particular starts and the specification of the 4/12/2023 4.9 Medium 4/12/2023 4.9 2024 palealtonetworks - multiple products device contained and was attacker to rash the system diverse first and was attacker to rask and was attacker to rask first bits. U.F. Orect the specification diverse diver								
Ovec 2023 immers assemble merge request builder influxs unstrumtistet attackers repective of plot corresponding to the attacker-specified of plot corresponding to the attacker specified of plot corresponding to the attacker specified of plot corresponding to the attacker specified of plot corresponding to the attacker specified of plot corresponding to the attacker and be attacker attacker attacker atheattacker atheattacker attacker atheattacher attacker attacker at								
Ovec parkins - assemble _merge_request_builder allows unsutherinated attackers to trigger builds of plac carepoint gate the attacker specified reportion. 4/12/2023 4.9 Medium of plac carepoint gate attackers perified reportion. 4/12/2023 4.9 Medium 0052 microsoft windows server 2022 Windows DNS Server Information Disclourer expose the planter values of server SMACS 4/12/2023 4.9 Medium 0055 paralent retworks -multiple products Autes affect free Raw saft and in a face care and in a server in a face c								
2023.2 enkins - samehia merge_request; builder of jobs corresponding to the attacker-specified 4/12/2023 5.3 Medium CVC repositors. 4/12/2023 4.3 Medium 2023 microsoft - windows Jenver, 2022 Windows DMS Server Information Dactosure 4/11/2023 4.3 Medium 2023 microsoft - windows Jenver, 2022 Windows DMS Server Information Dactosure 4/12/2023 4.9 Medium 2023 palaatonetworks - multiple products device a configuration and encrypted APM kays. 4/12/2023 4.7 Medium 2023 innex - multiple products due to a rate problem. 4/12/2023 4.7 Medium 2023 innex - multiple products due to a rate problem. 4/12/2023 4.7 Medium 2023 innex - multiple products confidentiality and mergerly of the configuration function for the configuration f								
30212 jenkins - assenbila, merge_request_builder repisibliny. 4/12/2023 5.3 Medlan 2023 microsoft - windows genver 2022 Windows DMS Server Information Bucklosure 4/11/2023 4.5 Medlan CVE A sufferability in Rate Able Networks RAN-CS A sufferability in Rate Able Networks RAN-CS 4.11/2023 4.5 Medlan CVE A sufferability in Rate Able Networks RAN-CS 4.11/2023 4.5 Medlan CVE A sufferability in Rate Able Networks RAN-CS 4.11/2023 4.5 Medlan CVE A sufferability in Rate Able Networks RAN-CS 4.11/2023 4.5 Medlan CVE A sufferability in Rate Able Networks RAN-CS 4.11/2023 4.7 Medlan State								
CVF. 411/2023 4.9 Medium A vitrarability 411/2023 4.9 Medium A vitrarability 411/2023 4.9 CVF. Software enables an authenticated administrator to compose the planker values of sectors stored in the value or ance problem. 411/2023 4.9 CVF. Software enables an authenticated administrator to compose the planker values of sectors stored in the value or ance problem. 411/2023 4.9 CVF. Software enables an authenticated administrator to compose the planker values of sectors and the value or ance problem. 411/2023 4.7 2023. Encore-multiple products The SAP Application interface Framework (Message Databard) Vitrarability 2023. Sap - multiple products Windows Group Foldy Science Tabara 411/2023 4.6 CVF. Sap - multiple products Windows Group Foldy Science Tabara 411/2023 4.6 Medium CVF. Sap - multiple products Windows Group Foldy Science Tabara 411/2023 4.4 Medium CVF. Sap - horn, fileri app, my, forms The SAP 47 (OATA science) - version 411/2023 4.3 Medium CVF								
2023 Mindows DMS Server information Diclosure Ar.17.1020 4.0 Median 2024 Mindrability in field Alto Networks PAN-OS Ar.17.1020 4.0 Median 2023 Software enables an altheritted and encrypted Parkes. Ar.17.1020 4.0 Median 2023 Ar.17.1020 Ar.17.1020 4.0 Median 2023 Ar.18.100 Ar.18.100 Ar.19.100 Ar.19		jenkins - assembla_merge_request_builder	repository.	4/12/2023	5.3	Medium		
24227 mittrosoft - windows_server_2022 Vulnerability Palo Attempting A vulnerability A vulnerabity A vulne								
CVF. Authorszbilis in Polo Alto Network PAN 05 software enables an authorstated administrator to espose the plaintext values of secrets strong in the device configuration and encrypted PAI keys. 4/12/202 4.9 CVF. Device of the the device on cline of the device on		· · · · · · · · · · · · · · · · · · ·						
CVF- paralizationetworks - multiple products service the products device configuration and encrypted API keys. 4/12/202 4.3 Median 2025 applicationetworks - multiple products diverse first frame sub-fit and indit; errowsell 4/12/202 4.3 Median 2026 diverse first frame sub-fit and indit; errowsell 4/12/202 4.7 Median 2026 linux - multiple products diverse first frame sub-fit and indit; errowsell 4/12/202 4.7 Median 2026 linux - multiple products diverse first frame sub-fit and indit; errowsell 4/12/202 4.7 Median 2026 linux - multiple products diverse first frame sub-first frame s	28277	microsoft - windows_server_2022	,	4/11/2023	4.9	Medium		
2020 0005palather wultiple productsexpase the plaintext values of exerts stored in the device and/particle and in redic, remove in divers/right-redic flow was found in male, remove in divers/right-redic/fact in the lunx kernel. This due to a race problem.//1/2023Medium due to a race problem.//1/2023 <th <="" td=""><td></td><td></td><td></td><td></td><td></td><td></td></th>	<td></td> <td></td> <td></td> <td></td> <td></td> <td></td>							
DODS paloaltonetworks - multiple products device configuration and encrypted AP keys. 4/1/2023 4.9 Medium CVF. Aussender free flow was flowed in ording. remove in flow cash the system 4/12/2023 4.7 Medium 1990 linux - multiple products The SAP Application Inferiance Framework (Message in the system of the s								
CVC Ause after free flaw was found in rule_promove in drives/rule_trick-profiled in the Unix Kernet. The SPA patients are considered to crash the system due to a race problem. 4/12/2023 4.7 Medlum 1990 linux - multiple products The SAP Application Interface Framework (Message Dathboard) - versions AF 783, KPX 20, SACORE DDI, SAP_ARAS 755, 556, SAP_ARA 755, 756, SAP_ARA 755, 756, SAP_ARA 756, 758, 758, SAP_ARA 756, 759, 756, SAP_ARA 756, 750, 750, 750, 750, 750, 750, 750, 750								
CVE. drives/infe/24-mc/mldc in the Unax Krenel. This flaw could allow an attacker to rash the system 4/12/2023 4.7 Meduar 1999 linux - multiple products The SAP Apalitation inferface Framework (Measage Dashboard) - versions AIP 703, AIP X02, S4C0RE 101, SAP_ABX 752, 755, SAP_ABX 752, 750, SAPA	0005	paloaltonetworks - multiple products		4/12/2023	4.9	Medium		
2023. Invx - multiple products Have could allow an attacker to crash the system 4/12/2023 4.7 Medure 1999 Invx - multiple products The SAP Application Interface Framework (Message Dashboard) - writions RF 207, 250, 756, 530, 756, 540, 757, 550, 540, 757, 550, 550, 757, 550, 550, 757, 550, 550	0.45		—					
1990 Inux - multiple products due to a race problem. 4/12/2023 4.7 Median 1990 Inux - multiple products The SAP ApOListion inferinger framework (Mediasade Diashboard), versions AIF 703, AIF XO2, SACORE 301, SAP ABA 752, TS95, ABA 754, TS95, ABA								
Image: Section of the SAP Application Interface Framework (Message Dashboard) - vusions AF703, AFX702, SC0E 101, SAP, BASIS 755, 756, SAP, ABA 752, 750, 756, application allows an Excel formula injection. An authorized attacker can light a the Custom Himts List. Once the victim opens the downloaded Excel downent, the formula will be executed. As a result, an attacker can cause limited impact on the confidentiality and integrity of the application. 4/11/2023 4.6 Medium CVF.				4/12/2022	47	Madium		
Obshboard] - versions AIF 703, AIF X02, S4C0RE 101, SAP ABX 755, 756, ABX 755	1990	linux - multiple products		4/12/2023	4.7	Iviedium		
101, SAP, BASIS 755, 756, SAP, BAB 75C, 750, 755, Image: Sape Same Same Same Same Same Same Same Sam								
application allows an Excel formula inject antitory Excel formulas into fields like the Toolit pot the Custom Hints Isti. Once the virtuin genes the downloaded 2023. 2023. 2023. 2023. 2025. 2026. 2027. 2027. 2028. 2029. 2029. 2029. 2029. 2029. 2029. 2029. 2029. 2029. 2029. 2029. 2020. 2021. 2020. 2021. 2020. 2021. 2022. 2021. 2022. 2022. 2022. 2022. 2022. 2022. 2022. 2024. 2024. 2024. 2024. 2024. 2024. 2025. 2026. 2027. 2027. 2028. 2029. 2029. 2029. 2029. 2029. 2029. 2020. 2020. 2021. 2020. 2021. 2021. 2022. 2022. 2021. 2022. 2022. 2022. 2024. 2024. 2024. 2024. 2025. 2026. 2027. 2027. 2028. 2029. 2029. 2029. 2029. 2020. 2020. 2021. 2021. 2021. 2021. 2021. 2021. 2022. 2021. 2021. 2022. 2022. 2022. 2023. 2024. 2024. 2024. 2025. 20			-					
authorized attacker can inject arbitrary Excel formulas to fields like the Toothy of the Cutom Hints List. Once the victim opens the downloaded Excel document, the formula will be executed. As a result, an attacker can cause limited impact on the confidentiality and integrity of the application. 4/11/2023 4.6 Median 2023- 2024- 2023- 2024- 2024- 2024- 2024- 2024- 2024- 2025- 2024- 2025- 2026- 2026- 2026- 2027- 2026- 2027- 2027- 2027- 2027- 2027- 2027- 2027- 2027- 2027- 2027- 2027- 2027- 2027- 2027- 2027- 2027- 2027- 2028- 2029								
cvc. Formulas into fields like the Tooting of the Custom Image: Subscript of the Subscript of the application of the Subscript of the application. Image: Subscript of the application.								
CVE. Excel document, the formula will be exceeded. As a result, an attacker can cause limited impact on the set of								
CVE. Excel document, the formula will be executed. As a part of the application. 4/11/2023 4.6 Medium 2010 2013- sap - multiple products Vulnerability and integrity of the application. 4/11/2023 4.6 Medium 2010 2023- windows Group Policy Security Feature Bypass 4/11/2023 4.6 Medium 2010 2023- SAP HCM Fiori App My Forms (Fiori 2.0) - version 605, does not perform necessary authorization 2010 4/11/2023 4.3 Medium 2010 2023- checks for an unterhicated user exposing TSS, 756, discloses more detailed information than is required. An authorization start science are spoing 755, 756, discloses more detailed information than is required. An authorized tacker cause a low unterhisting 2023- 4.11/2023 4.3 Medium 2012 2023- component. As a result, an ttacker cause a low unterhisting 2014 4/11/2023 4.3 Medium 2012 2023- component. As a result, an ttacker cause a low unterhisting 2014 4/11/2023 4.3 Medium 2012 2023- component. As a result, an ttacker cause a low unterhisting 2014 4/11/2023 4.3 Medium 2012 2023- component. As a result, an ttacker cause a low unterhisting 2014 4/11/2023 4.3 Medium 2012 <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>								
2023- 2019 sap - multiple products confidentiality and integrity of the application. 4/11/2023 4.6 Medlun CVF- 2023- 2024 windows Group Policy Security Feature Bypass 4/11/2023 4.4 Medlun CVF- 2023- 2024 SAP HCM Finit App My Forms (Finit 2.0) - version 4/11/2023 4.4 Medlun CVF- 2023- 2023- 2023- Sap - hcm, fiori_app_my_forms SAP HCM Finit App My Forms (Finit 2.0) - version 4/11/2023 4.4 Medlun CVF- 2023- 2023- sap - hcm, fiori_app_my_forms restricted header data. 4/11/2023 4.3 Medlun CVF- 2023- sap - hcm, fiori_app_my_forms restricted header data. 4/11/2023 4.3 Medlun CVF- 2023- collected information possibly to exploit the component. As a result, an attacker can cause a low 29111 sap - multiple products A permissive list of allowed inputs winerability (CVF- 2022- 4.11/2023 4.3 Medlun CVF- 2023- microsoft - edge Bypass Vulnerability may allow an authenticated SU-VPN water to bypass 4/11/2023 4.3 Medlun CVF- 2023- microsoft - edge Bypass Vulnerability of allowed inputs winerability 4/11/2023 4.3 Medlun CVE- 2023- microsoft - edge Bypass Vulnerability of allowed inputs winer bypass 4/11/2023 4.3 Medlun CVE- 2023- microsoft - edge Bypas	CV/F							
29109 sap - multiple products confidentiality and integrity of the application. 4/11/2023 4.6 Medium 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2024- 2023- 2024- 2023- 2024- 2023- 2024- 2025- 2024- 2025- 2024- 2								
CVE. Windows Group Policy Security Fature Bypass 4/11/2023 4.4 Medium 28376 microsoft - multiple products SAP HCM Flori App My Forms (Flori 2.0) - version 605, does not perform necessary authorization checks for an authenticated user exposing the 1993 4.11/2023 4.4 Medium 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2024 sap - hcm flori app my forms restricted hader data. 4/11/2023 4.3 Medium 1993 sap - hcm flori app my forms restricted hader data. 4/11/2023 4.3 Medium 1993 sap - hcm flori app my forms restricted hader data. 4/11/2023 4.3 Medium 2021- 2022- 2021 microsoft - multiple products In perrificate restrin 7.2 4/11/2023 4.3 Medium 2022- 2022- 2022 microsoft - edge Bypass Vulerexplisity of the policy via bootsmarks in the web portal. 4/11/2023 4.3 Medium 2024- 2025 microsoft - edge Bypass Vulerexplisity authenticate Sity VPN users to bypass attackers with 0 verain Research with ten/fead permission to test in tenkins Thycotic Secret Server Plugin 1.0.2 and earlier allows attackers with 0 verainer allows attackers with 0 verainer allows attackers with 0 verainer allows attacker with ten/fead permission to test in tenkins Togbugy		can multiple products	· · ·	4/11/2022	16	Madium		
2023: 23276 Windows Group Policy Security Feature Bypass Vulnersbillty 4/11/2023 4.4 Medium 23276 SAP HCM Flori App My Forms (Flori 2.0) - version 605, does not perform necessary authorization 605, does not perform necessary apart of 605, does not perform necessary apart of 605, does not perform necess tokens does not not perform alows 7022. 7023 ienkins - report_portal 7023 ienkins - report_portal 7024, ienkins controller file system. 7025 ienkins - report_po		sap - multiple products	confidentiality and integrity of the application.	4/11/2023	4.0	wealum		
28276 microsoft - multiple products Vulnerability 4.11/2023 4.4 Medium CVE SAP HCM Flori App My Forms (Flori 2.0) - version 605, does not perform necessary authorization checks for an authenticated user exposing the discloses more detailed information than is required. An authorized attacker can cause a low collected information possibly to exploit the collected information possibly to exploit the collected information possibly to exploit the component. As a result, an attacker can cause a low zeruine d. An authorized attacker can cause a low discloses more detailed information. 4/11/2023 4.3 Medium 2023- 2023- 2023- 2024 sap - multiple products Impact on the confidentiality of the application. 4/11/2023 4.3 Medium A/2469 fortinet - multiple products Microsoft Edg (Chromium-based) Network 4/11/2023 4.3 Medium CVE- 2022- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2024 Microsoft Edg (Chromium-based) Security Feature Bypass Vulnerability 4/11/2023 4.3 Medium CVE- 2022- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2024 Microsoft Edg (Chromium-based) Security Feature Bypass Vulnerability 4/11/2023 4.3 Medium CVE- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2024- Microsoft Edg (Chromium-based) Security F			Windows Crown Policy Security Feature Bypass					
CVE- 2023 Sap + hcm_flori_app_my_forms SAP HCM flori App My forms (flori 2.0) -version cbc, does not perform necessary suthorization cbc, does not perform necessary suthorization component. As a result, an attacker can use the collected information possibly to exploit the collected information possibly to exploit the component. As a result, an attacker can cause a low impact on the confidentiality of the application. 4/11/2023 4.3 Mediun 2011 sap - multiple products A permissive list or allowed inputs vulnerability [CWE-130] in fortificate version 7.0.3 and below, version 7.0.9 and below Policy-based NGFW Mode may allow an authenticated SL-VPN user to bypass the policy via bookmarks in the web portal. 4/11/2023 4.3 Mediun CVE- 2022- 2023- 2024 Microsoft Edge (Chromium-based) Security Feature Plugn 1.0.2 and earlier allows attackers with Overal/Read permission to enumerate credentials IDs of credentials stored in 20518 4/11/2023 4.3 Mediun CVE- 2023- 2032 Securit performation on the configer builds of lobs attackers with Overal/Read permission to enumerate credentials IDs of credentials stored in 20518 4/11/2023 4.3 Mediun CVE- 2033 Jenkins - fogbugz Securit Plugit 0.5 and earlier allows attackers with Overal/Read permission to enumerate credentials IDs of credentials stores in thackers to observe and capture them. 4/		microsoft - multiple products		4/11/2022	лл	Medium		
CVE- 605, does not perform necessary authorization checks for an authenticated user exposing the discloses more detailed information than is required. An authorized attacker can use the collected information possibly to exploit the component. As a result, an attacker can use the collected information possibly to exploit the component. As a result, an attacker can use a low required. An authorized attacker can use a low required. An authorized attacker can use a low required the application. 4/11/2023 4.3 Medium 20111 sap - multiple products inpact on the confidentiality to exploit the component. As a result, an attacker can use a low wersion 7.0.9 and below Policy-based NGPW Mode may allow an authenticated SSL-VPN user to bypass 4 CVE- version 7.0.9 and below Policy-based NGPW Mode may allow an authenticated SSL-VPN user to bypass 4 4 CVE- wersion 7.0.9 and below Policy-based NGPW Mode may allow an authenticated SSL-VPN user to bypass 4 4 4 CVE- enderson the policy via bookmarks in the web portal. 4/11/2023 4.3 Medium CVE- enderson the policy based NGPW Mode may allow an authenticated SSL-VPN user to bypass 4 4 4 2023- fortinet - multiple products the policy based NGPW Mode may allow an authenticated SSL-VPN user to bypass 4 4 4 4 2023- fortinet - multiple products antising permission or tage with screet S	20270	merosore - maniple products	· ·	4/11/2023	4.4	Weuluili		
2023- 1903 sap - hcm_fiori_app_my_forms checks for an authenticated user exposing the restricted header data. 4/11/2023 4.3 Medium 1903 sap - hcm_fiori_app_my_forms The SAP Aif (DOATA service) - versions 755, 756, discloses more detailed information than is required. An authorized attacker can use the collected information possibly to exploit to	CVF-							
1903 sap - hcm_fiori_app_my_forms restricted header data. 4/11/2023 4.3 Medium 1903 The SAP Alf (QOATA service) - versions 755, 756, discloses more detailed information than is required. An authorized attacker can use the collected information possibly to exploit the component. As a result, an attacker can use a low 4/11/2023 4.3 Medium 2011 sap - multiple products impact on the confidentiality of the application. 4/11/2023 4.3 Medium 2012 ap - multiple products the policy via bookmarks in the web portal. 4/11/2023 4.3 Medium 2026 fortinet - multiple products the policy via bookmarks in the web portal. 4/11/2023 4.3 Medium 2027 fortinet - multiple products the policy via bookmarks in the web portal. 4/11/2023 4.3 Medium 2028 microsoft - edge Bypass Vulnerability 4/11/2023 4.3 Medium 2029 jenkins - thycotic_secret_server Jenkins. 4/11/2023 4.3 Medium 2024 microsoft - edge Bypass Vulnerability 4/11/2023 4.3 Medium 2023 jenkins - thycotic_secret_server Jenkins. Jenkins. 4/12/2023 <								
CVE- CVE- 2023 The SAP AIF (D0ATA service) - versions 755, 756, discloses more detailed information than is required. An authorized attacker can use the collected information possibly to exploit the component. As a result, an authorized attacker can use a low impact on the confidentiality of the application. 4/11/2023 4.3 Medium (Appendix) 29111 sap - multiple products A permission that sa result, an authorized attacker can cause a low impact on the confidentiality of the application. 4/31/2023 4.3 Medium (Appendix) 2022- 2022 Fortinet - multiple products A permission SUS. VPN user to bypass the policy via bookmarks in the web portal. 4/11/2023 4.3 Medium (A/11/2023 4.3		san-hom fiori ann my forms		1/11/2023	13	Medium		
cVE- discloses more detailed information than is required. An authorized attacker can use the collected information possibly to exploit the component. As a result, an attacker can use a low required. An authorized attacker can use the collected information possibly to exploit the component. As a result, an attacker can use a low result. The configuration of th	1903	sap - hem_hom_app_my_forms		4/11/2023	4.5	Weuluili		
CVE- 2023- 29111 sap - multiple products required. An authorized attacker can cuse the collected information possibly to exploit the component. As a result, an attacker can cause a low impact on the confidentiality of the application. 4/11/2023 4.3 Medium 4/11/2023 29111 sap - multiple products A permissive list of allowed inputs vulnerability (CWE-183) in FortiGate version 7.2.3 and below, version 7.0.9 and below Policy-based MoNFW Mode 2022- 2022- 4.3 Medium 4/11/2023 4.3 Medium 4/11/2023 2024- 2023- 2023- 2024- 2024- 2024- 2024- 2025- 2024- 2025- 2024- 2025- 2025- 2025- 2025- 2025- 2025- 2025- 2026- 2026- 2026- 2026- 2026- 2026- 2026- 2026- 2026- 2026- 2026- 2026- 2026- 2026- 2026- 2026- 2026- 2027- 2026- 2026- 2026- 2026- 2027- 2027- 2026- 2027- 2027- 2027- 2027- 2027- 2028- 2028- 2028- 2029- 20								
CVE- 2023- 2011 component. As a result, an attacker can cause a low impact on the confidentiality of the application. 4/11/2023 4.3 Medium 2011 sap - multiple products A permissive list of allowed inputs vulnerability (CWE-18) in FortiGate version 7.2.3 and below, 2022- 4.3 Medium 2024 may allow an authenticated SSL-VPN user to bypas 4/11/2023 4.3 Medium 2025- may allow an authenticated SSL-VPN user to bypas 4/11/2023 4.3 Medium 2024- microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability 4/11/2023 4.3 Medium 2023- microsoft edge Bypass Vulnerability 4/11/2023 4.3 Medium 2024- microsoft edge Bypass Vulnerability 4/11/2023 4.3 Medium 2023- attackers with Overall/Read permission to feat in Jenkins Thycotic 4/12/2023 4.3 Medium 2024- attackers with Overall/Read permission to fredentials stored in enumerate credentials IDs of credentials stored in 10.2 and earlier allows attackers with Herm/Read permission to frege builds of jobs 4/12/2023 4.3 Medium 2023- jenkins - fogbugz specified in al jobnamer fequest parameter, 10.2 ipenkins - fogbugz specified in alybonamer fe								
2023- 2011 sap - multiple products impact on the confidentiality of the application. 4/11/2023 4.3 Medium 2011 Sap - multiple products A permissive list of allowed inputs vulnerability [CWE-138] in Fortifate version 7.2.3 and below, version 7.0.9 and below Policy-based NGFW Mode I I I 2022- 2022- 2022- 2024 Tortifate version 7.2.3 and below, version 7.0.9 and below Policy-based NGFW Mode I I I 2024 fortinet - multiple products the policy via bookmarks in the web portal. 4/11/2023 I.3 Medium 2025- 2026 fortinet - multiple products the policy via bookmarks in the web portal. 4/11/2023 I.3 Medium 2028 microsoft - edge Bypass Vulnerability 4/11/2023 I.3 Medium 2023 attackers with Overall Read permission to feck in Jenkins Thycotic Secret Server Plugin 1.0.2 and earlier allows 4/12/2023 I.3 Medium 2023- 2023 jenkins - thycotic secret server Plugin 2.2.17 and earlier allows attackers with tem/Read permission to fugger builds of joba 4/12/2023 I.3 Medium 2023 jenkins - fogbugz specified in a 'jobname' request parameter. 4/12/2023 I.3 Medium 2023	CVE		•					
2911 sap - multiple products impact on the confidentiality of the application. 4/11/2023 4.3 Medium CVE- A permissive list of allowed inputs volumerability Impact on the confidentiality of the application. 4/11/2023 4.3 Medium CVE- Version 7.0.9 and below Policy-based NGFW Mode Impact on the policy via bockmarks in the web portal. 4/11/2023 4.3 Medium 2023- Microsoft Edge (Chronium-based) Security Feature 4/11/2023 4.3 Medium 2023- Microsoft Edge (Chronium-based) Security Feature 4/11/2023 4.3 Medium 2023- attackers with Overall/Read permission to cells and the stored in a store								
CVE- A permissive list of allowed inputs vulnerability ICWE-183] in FortiGate version 7.0.3 and below, version		san - multiple products	•	4/11/2022	12	Madium		
CVE- 2022- 2024 ICWE-183] in FortiGate version 7.2.3 and below, wersion 7.0.9 and below Policy-based NGFW Mode may allow an authenticated SSI-VPN user to bypass the policy via bookmarks in the web portal. IVIII 2023 4.3 Medium 2023- 2024- 2023- 2025- 2025- 2025- 2025- 2025- 2025- 2025- 2025- 2025- 2026- 2026- 2027- 2027- 2027- 2027- 2028- 2028- 2029- 2020- 20	23111	sap - multiple products		4/11/2023	4.5	wearan		
CVE- 2022- 2023- 2024- 2023- 2024- 2025- 2025- 2025- 2025- 2025- 2025- 2025- 2025- 2025- 2025- 2025- 2026- 2027-								
2022- 2023- 	CVF-							
42469 fortinet - multiple products the policy via bookmarks in the web portal. 4/11/2023 4.3 Medium CVE- Microsoft Edge (Chromium-based) Security Feature 4/11/2023 4.3 Medium 28284 microsoft - edge Bypass Vulnerability 4/11/2023 4.3 Medium 28284 microsoft - edge Bypass Vulnerability 4/11/2023 4.3 Medium 28284 A missing permission check in Jenkins Thycotic Secret Server Puign 1.0.2 and earlier allows 4/11/2023 4.3 Medium 2023- attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in allows attackers with 4/11/2023 4.3 Medium 2023- Jenkins. A missing permission to trigger builds of jobs 4 4/11/2023 4.3 Medium 2023- Jenkins - fogbugz specified in a 'jobname' request parameter. 4/11/2023 4.3 Medium 2023- jenkins - report_portal Item/Read permission to trigger builds of jobs 4 4 4 4 2023- jenkins - report_portal Item/Read permission or access to kens unercrypted in job 4 4 4 4								
CVE- 2023- 28284 Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability 4/11/2023 4.3 Medium A missing permission check in Jenkins Thycotic Secret Server Plugin 1.0.2 and earlier allows attackers with Overall/Read permission to enumerate credentials Ds of credentials stored in Jenkins. 4/11/2023 4.3 Medium 30518 jenkins - thycotic_secret_server Jenkins. 4/12/2023 4.3 Medium 2023- 2024- 2023- 2024- 2023- 2024- 2023- 2024- 2023- 2025- 2025- 2025- 2026- 2027- 2027- 2027- 2027- 2027- 2027- 2027- 2028- 2028- 2028- 2028- 2028- 2029- 202		fortinet - multiple products		4/11/2023	43	Medium		
2023- 28284microsoft - edgeMicrosoft Edge (Chromium-based) Security Feature Bypass Vulnerability4/11/20234.3Medium28284microsoft - edgeBypass Vulnerability4/11/20234.3Medium28284microsoft - edgeMicrosoft Edge (Chromium-based) Security Feature Bypass Vulnerability4/11/20234.3Medium2023- 2023- 30518jenkins - thycotic_secret_serverJenkinsJenkins4/12/20234.3Medium2023- 2023- 2023- 2023- 30522jenkins - fogbugzPlugin 2.2.17 and earlier allows attackers with 1 plugin 2.2.17 and earlier allows attackers with 305224/12/20234.3Medium2023- 2023- 2023- 30522jenkins - fogbugzspecified in a 'lobname' request parameter. Report Portal Plugin 0.5 and earlier atores Report Portal Plugin 0.5 and earlier stores request parameter.4/12/20234.3Medium2023- 2023-Medium4/12/20234.3MediumCVE- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023-Jenkins Kopt Portal access tokens displayed on the configuration form, increasing the potential for 2023- 2023- 2023- 2023- 2023- 2023- 2023-4/12/20234.3Medium				4/11/2023	4.5	weaturn		
28284 microsoft - edge Bypass Vulnerability 4/11/2023 4.3 Medium 28284 A missing permission check in Jenkins Thycotic Secret Server Plugin 1.0.2 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in 30518 4 4 4 2023- 30518 jenkins - thycotic_secret_server Jenkins. 4 4 4 Medium 2023- 30522 jenkins - fogbugz Specified in a'jobname' request parameter. 4 4 Medium 2023- 30522 jenkins - fogbugz specified in a'jobname' request parameter. 4/12/2023 4.3 Medium 2023- 30523 jenkins - fogbugz specified in a'jobname' request parameter. 4/12/2023 4.3 Medium 2023- 30523 jenkins - report_portal Ihe Jenkins Report Portal Plugin 0.5 and earlier stores ReportPortal access tokens unencrypted in job config.xml files on the Jenkins controller file system. 4/12/2023 4.3 Medium 2023- 30524 jenkins - report_portal the Jenkins Report Portal Plugin 0.5 and earlier does not mask ReportPortal access tokens displayed on the configuration form, increasing the potential for global config.xml file on the Jenkins controller file system. 4/12/2023 4.3 Medium 2023- 30524 jenkins - report_p			Microsoft Edge (Chromium-based) Security Feature					
CVE- A missing permission check in Jenkins Thycotic Secret Server Plugin 1.0.2 and earlier allows attackers with Overall/Read permission to 30518 jenkins - thycotic_secret_server Jenkins. A missing permission check in Jenkins Fogbugz 4/12/2023 4.3 CVE- Plugin 2.2.17 and earlier allows attackers with 1/12/2023 4.3 CVE- Plugin 2.2.17 and earlier allows attackers with 1/12/2023 4.3 S0522 jenkins - fogbugz Specified in a 'jobname' request parameter. 4/12/2023 4.3 VE- 2023- gentins Report Portal Plugin 0.5 and earlier stores ReportPortal access tokens unencrypted in job 4/12/2023 4.3 Medium S0523 jenkins - report_portal the Jenkins controller file system. 4/12/2023 4.3 Medium S0523 jenkins - report_portal the Jenkins controller file system. 4/12/2023 4.3 Medium S0523 jenkins - report_portal the Jenkins controller file system. 4/12/2023 4.3 Medium S0524 jenkins - report_portal attackers to observe and capture them. 4/12/2023 4.3 Medium S0524 jenkins - re		microsoft - edge		4/11/2023	43	Medium		
CVE- 2023- 30518Secret Server Plugin 1.0.2 and earlier allows attackers with Overail/Read permission to enumerate credentials IDs of credentials stored in Jenkins.Image: Comparise of the com	20204	inclosoft cuge		4/11/2023	4.5	Wicdiam		
CVE- 2023- 30518jenkins - thycotic_secret_serverattackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.Jenkins.4/12/20234.3Mediun30518jenkins - thycotic_secret_serverA missing permission check in Jenkins Fogbugz4/12/20234.3MediunCVE- 2023- 30522jenkins - fogbugzspecified in a 'jobname' request parameter.4/12/20234.3Mediun30518jenkins - fogbugzspecified in a 'jobname' request parameter.4/12/20234.3Mediun30522jenkins - fogbugzspecified in a 'jobname' request parameter.4/12/20234.3Mediun30523jenkins - report_portalJenkins Report Portal Plugin 0.5 and earlier stores with Item/Extended Read permission or access to tis configuration where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.4/12/20234.3Mediun30523jenkins - report_portalJenkins Report Portal Plugin 0.5 and earlier does not mask ReportPortal access tokens displayed on the configuration forn increasing the potential for attackers to observe and capture them.4/12/20234.3Mediun30524jenkins - report_portalJenkins WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth Plugin 387.v938a_ecb_Trfeg and earlier does not require POST requests for an HITP endpoint, allowing attackers to reindex the4/12/20234.3Mediun								
2023- 30518 jenkins - thycotic_secret_server enumerate credentials IDs of credentials stored in Jenkins. 4/12/2023 4.3 Medium CVE- 2023- 30522 Amissing permission check in Jenkins Fogbugz Plugin 2.2.17 and earlier allows attackers with Item/Read permission to trigger builds of jobs 4.3 Medium 30522 jenkins - fogbugz specified in a 'jobname' request parameter. 4/12/2023 4.3 Medium 30522 jenkins - fogbugz specified in a 'jobname' request parameter. 4/12/2023 4.3 Medium CVE- 2023- 30523 jenkins - report_portal Jenkins Report Portal Plugin 0.5 and earlier stores ReportPortal access tokens unencrypted in job config.rml files on the Jenkins controller as part of its configuration where they can be viewed by users with Item/Extended Read permission or access to the Jenkins Report Portal Plugin 0.5 and earlier does not mask ReportPortal access tokens displayed on the configuration form, increasing the potential for attackers to observe and capture them. 4/12/2023 4.3 Medium 2023- 30524 jenkins - report_portal attackers to observe and capture them. 4/12/2023 4.3 Medium 2023- 30524 jenkins - report_portal attackers to observe and capture them. 4/12/2023 4.3 Medium 2023- 30524 jenkins - report_portal attackers to observe and capture them.	CVF-		-					
30518jenkins - thycotic_secret_serverJenkins.4/12/20234.3MediumCVE- 2023- 30522Plugin 2.2.17 and earlier allows attackers with Item/Read permission to trigger builds of jobsA.3Medium30522jenkins - fogbugzspecified in a 'jobname' request parameter.4/12/20234.3Medium30522jenkins - fogbugzspecified in a 'jobname' request parameter.4/12/20234.3MediumCVE- 2023- 30523jenkins - report_portalJenkins Report Portal Plugin 0.5 and earlier stores request parameter.KeportPortal access tokens unencrypted in job config.xml files on the Jenkins controller as part of with Item/Extended Read permission or access to with Item/Extended Read permission or access to the Jenkins Report Portal access tokens displayed on the configuration where they can be viewed by users with Item/Stended Read permission form, increasing the potential for the lenkins controller file system.4/12/20234.3Medium2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023- 2023-jenkins - report_portalthe Jenkins Report Portal access tokens displayed on the configuration form, increasing the potential for the WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth Plugin 387.v938a_ecb_f7feg and earlier does not require POST requests for an and earlier does not require POST requests for an earlier does not require POST frequest for an earlier does not require POST requests for an e			· · ·					
CVE- A missing permission check in Jenkins Fogbugz Plugin 2.2.17 and earlier allows attackers with 30522 jenkins - fogbugz Specified in a 'jobname' request parameter. 4/12/2023 4.3 Mediun 30522 jenkins - fogbugz Jenkins Report Portal Plugin 0.5 and earlier stores ReportPortal access tokens unencrypted in job 4/12/2023 4.3 Mediun CVE- its configuration where they can be viewed by users with Item/Extended Read permission or access to 30523 jenkins - report_portal the Jenkins controller file system. 4/12/2023 4.3 Mediun 2023- with Item/Extended Read permission or access to and make the configuration where they can be viewed by users 4/12/2023 4.3 Mediun 2023- jenkins - report_portal Ienkins Report Portal access tokens displayed on 4/12/2023 4.3 Mediun 2023- jenkins - report_portal attackers to observe and capture them. 4/12/2023 4.3 Mediun 2023- jenkins - report_portal attackers to observe and capture them. 4/12/2023 4.3 Mediun 2023- jenkins - report_portal attackers to observe and capture them. 4/12/2023 4.3 Mediun		jenkins-thucotic secret server		4/12/2022	∆ 2	Medium		
CVE- 2023- 30522Plugin 2.2.17 and earlier allows attackers with Item/Read permission to trigger builds of jobs specified in a 'jobname' request parameter.// <th <th=""><th <th="">//</th></th>	<th <th="">//</th>	//	50510			1/ 12/ 202J	- 1 .J	meanum
2023- 30522 jenkins - fogbugz Item/Read permission to trigger builds of jobs specified in a 'jobname' request parameter. 4/12/2023 4.3 Medium 30522 jenkins Report Portal Plugin 0.5 and earlier stores ReportPortal access tokens unencrypted in job config.xml files on the Jenkins controller as part of its configuration where they can be viewed by users with Item/Extended Read permission or access to 30523 Image: CVE- jenkins - report_portal Image: CVE- the configuration where they can be viewed by users with Item/Extended Read permission or access to attackers to observe and capture them. 4/12/2023 4.3 Medium 2023- 2023- 2023- 2023- 30524 jenkins - report_portal Jenkins Report Portal Plugin 0.5 and earlier does not mask ReportPortal access tokens displayed on the configuration form, increasing the potential for the configuration form, increasing the potential for the WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth Client secret unencrypted in the global config.xml file on the Jenkins controller 4/12/2023 4.3 Medium 2023- 2	CVF-		•••					
30522jenkins - fogbugzspecified in a 'jobname' request parameter.4/12/20234.3MediumJenkins Report Portal Plugin 0.5 and earlier stores ReportPortal access tokens unencrypted in job config.xml files on the Jenkins controller as part of its configuration where they can be viewed by users with Item/Extended Read permission or access to4/12/20234.3Medium2023- 30523jenkins - report_portalthe Jenkins controller file system.4/12/20234.3Medium2023- 2023- 2023- 30523jenkins - report_portalthe Jenkins controller file system.4/12/20234.3Medium2023- 2023- 2023- 2023- 2023- 2023- 30524jenkins - report_portalattackers to observe and capture them.4/12/20234.3Medium2023- 2023- 2023- 2023- 30524jenkins - report_portalattackers to observe and capture them.4/12/20234.3Medium2023- 2023- 2023- 30524jenkins - report_portalattackers to observe and capture them.4/12/20234.3Medium2023- 30527jenkins - report_portalattackers to observe and capture them.4/12/20234.3Medium2023- 30527jenkins - wso2_oauthJenkins Currene-Search Plugin 1.0 and earlier stores the WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth file on the Jenkins controller where it can be viewed by users with access to the global config.xml file on the Jenkins controller where it can be viewed by users with access to the dost on troller file system.4/12/20234.3Medium2023- 2023- 2023-j			-					
CVE- Jenkins Report Portal Plugin 0.5 and earlier stores CVE- ReportPortal access tokens unencrypted in job 2023- with Item/Extended Read permission or access to 30523 jenkins - report_portal the Jenkins controller as part of 2023- jenkins - report_portal the Jenkins controller file system. 4/12/2023 2023- Jenkins Report Portal Plugin 0.5 and earlier does 4/12/2023 4.3 CVE- Jenkins Report Portal Plugin 0.5 and earlier does not mask ReportPortal access tokens displayed on 4/12/2023 2023- jenkins - report_portal attackers to observe and capture them. 4/12/2023 4.3 2023- jenkins - report_portal attackers to observe and capture them. 4/12/2023 4.3 2023- jenkins - report_portal attackers to observe and capture them. 4/12/2023 4.3 2023- jenkins - wso2_oauth Jenkins Controller secret unencrypted in the global config.xml file on the Jenkins controller 2023- jenkins - wso2_oauth Jenkins controller file system. 4/12/2023 4.3 2023- jenkins - wso2_oauth Jenkins controller file system. 4/12/2023 4.3 2023-		ienkins - foghugz		4/12/2023	43	Medium		
CVE- 2023- 30523jenkins - report_portalReportPortal access tokens unencrypted in job config.xml files on the Jenkins controller as part of its configuration where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.4/12/20234.3Medium2023- 30523jenkins - report_portalJenkins Report Portal Plugin 0.5 and earlier does not mask ReportPortal access tokens displayed on the configuration form, increasing the potential for attackers to observe and capture them.4/12/20234.3Medium2023- 2023-jenkins - report_portalattackers to observe and capture them.4/12/20234.3Medium2023- 2023-jenkins - wso2_oauthJenkins Controller file system.4/12/20234.3Medium2023- 2023-jenkins - wso2_oauthJenkins controller file system.4/12/20234.3Medium2023- 2023-jenkins - wso2_oauthJenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex theImage: https://www.mage.com/dom <td></td> <td>Jennine 108008-</td> <td></td> <td>.,,</td> <td></td> <td></td>		Jennine 108008-		.,,				
CVE- 2023- 30523jenkins - report_portalconfig.xml files on the Jenkins controller as part of its configuration where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.4/12/20234.3Medium2023- 30523jenkins - report_portalJenkins Report Portal Plugin 0.5 and earlier does not mask ReportPortal access tokens displayed on the configuration form, increasing the potential for attackers to observe and capture them.4/12/20234.3Medium2023- 30524jenkins - report_portalattackers to observe and capture them.4/12/20234.3Medium2023- 30524jenkins - report_portalattackers to observe and capture them.4/12/20234.3Medium2023- 30524jenkins - report_portalattackers to observe and capture them.4/12/20234.3Medium2023- 30525jenkins - report_portalattackers to observe and capture them.4/12/20234.3Medium2023- 30526jenkins - report_portaljenkins wSO2 Oauth Plugin 1.0 and earlier stores global config.xml file on the Jenkins controller4/12/20234.3Medium2023- 30527jenkins - wso2_oauthjenkins controller file system.4/12/20234.3Medium2023- 30527jenkins - wso2_oauthjenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex theiii								
CVE- 2023- 30523jenkins - report_portalits configuration where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.4/12/20234.3MediumCVE- 2023- 30524Jenkins - report_portalJenkins Report Portal Plugin 0.5 and earlier does not mask ReportPortal access tokens displayed on the configuration form, increasing the potential for attackers to observe and capture them.4/12/20234.3Medium30524jenkins - report_portalattackers to observe and capture them.4/12/20234.3Medium30524jenkins - report_portalJenkins WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth client secret unencrypted in the global config.xml file on the Jenkins controller4/12/20234.3MediumCVE- 2023- 30527jenkins - wso2_oauthJenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex theHTTP endpoint, allowing attackers to reindex theH								
2023- 30523jenkins - report_portalwith Item/Extended Read permission or access to the Jenkins controller file system.4/12/20234.3MediumCVE- 2023- 30524Jenkins - report_portalJenkins Report Portal Plugin 0.5 and earlier does not mask ReportPortal access tokens displayed on the configuration form, increasing the potential for attackers to observe and capture them.4/12/20234.3Medium30524jenkins - report_portalattackers to observe and capture them.4/12/20234.3MediumCVE- 2023- 30527jenkins - report_portalJenkins WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth Client secret unencrypted in the global config.xml file on the Jenkins controller4/12/20234.3MediumCVE- 2023- 30527jenkins - wso2_oauthJenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex the4/12/20234.3Medium	CVF-		-					
30523jenkins - report_portalthe Jenkins controller file system.4/12/20234.3MediumCVE- 2023- 30524Jenkins Report Portal Plugin 0.5 and earlier does not mask ReportPortal access tokens displayed on the configuration form, increasing the potential for attackers to observe and capture them.4/12/20234.3Medium30524jenkins - report_portalattackers to observe and capture them.4/12/20234.3Medium30524jenkins - report_portalattackers to observe and capture them.4/12/20234.3MediumCVE- 2023- 30527jenkins - wso2_oauthJenkins WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth client secret unencrypted in the global config.xml file on the Jenkins controller where it can be viewed by users with access to the 305274.3Medium30527jenkins - wso2_oauthJenkins controller file system.4/12/20234.3MediumCVE- 2023- 2023-Jenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex theIII								
CVE- 2023- 30524Jenkins - report_portalJenkins Report Portal Plugin 0.5 and earlier does not mask ReportPortal access tokens displayed on the configuration form, increasing the potential for attackers to observe and capture them.4/12/20234.3Medium30524jenkins - report_portalattackers to observe and capture them.4/12/20234.3MediumJenkins WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth client secret unencrypted in the global config.xml file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.4/12/20234.3MediumCVE- 2023- 30527jenkins - wso2_oauthJenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex the4/12/20234.3Medium		jenkins - report nortal		4/12/2022	∆ २	Medium		
CVE- 2023- 30524not mask ReportPortal access tokens displayed on the configuration form, increasing the potential for attackers to observe and capture them.4/12/20234.3Medium30524jenkins - report_portalattackers to observe and capture them.4/12/20234.3Medium30524Jenkins WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth client secret unencrypted in the global config.xml file on the Jenkins controller4/12/20234.3Medium2023- 30527jenkins - wso2_oauthJenkins controller file system.4/12/20234.3Medium2023- 2023-jenkins - wso2_oauthJenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex the4/12/20234.3Medium				., 12, 2025				
2023- 30524the configuration form, increasing the potential for attackers to observe and capture them.4/12/20234.3Medium30524jenkins - report_portalJenkins WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth client secret unencrypted in the global config.xml file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.4/12/20234.3Medium2023- 30527jenkins - wso2_oauthJenkins controller file system.4/12/20234.3MediumCVE- 2023-jenkins - wso2_oauthJenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex the4/12/20234.3Medium	CVE-							
30524jenkins - report_portalattackers to observe and capture them.4/12/20234.3Medium30524Jenkins WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth client secret unencrypted in the global config.xml file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.4/12/20234.3Medium2023- 30527jenkins - wso2_oauthJenkins Controller file system.4/12/20234.3MediumCVE- 2023-jenkins - wso2_oauthJenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex the4/12/20234.3Medium								
CVE- 2023- 30527Jenkins WSO2 Oauth Plugin 1.0 and earlier stores the WSO2 Oauth client secret unencrypted in the global config.xml file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.4/12/20234.3MediunCVE- 2023- 2023- CVE- 2023-Jenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex theHTTP endpoint, allowing attackers to reindex theHTTP endpoint, allowing attackers to reindex the		ienkins - report portal		4/12/2023	4.3	Medium		
CVE- 2023- 30527the WSO2 Oauth client secret unencrypted in the global config.xml file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.4/12/20234.3Medium MediumCVE- 2023- 2023-Jenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex theImage: Comparison of the system of th		jemme report_portai		.,, _020				
CVE- global config.xml file on the Jenkins controller plobal config.xml file on the Jenkins controller plobal config.xml file on the Jenkins controller 2023- where it can be viewed by users with access to the plobal config.xml file on the Jenkins controller plobal config.xml file on the Jenkins controller 30527 jenkins - wso2_oauth Jenkins controller file system. plobal config.xml file on the Jenkins controller plobal config.xml file on the Jenkins controller CVE- Jenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 plobal config.xml file on the Jenkins controller file system. plobal config.xml file on the Jenkins Controller CVE- Jenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 plobal config.xml file on the Jenkins controller file system. plobal config.xml file on the Jenkins Controller 2023- HTTP endpoint, allowing attackers to reindex the plobal config.xml file on the Jenkins controller plobal config.xml file on the Jenkins controller			-					
2023- 30527jenkins - wso2_oauthwhere it can be viewed by users with access to the Jenkins controller file system.4/12/20234.3MediumCVE- 2023-Jenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex theImage: CVE- Image: CV	CVF-		<i>,</i> ,					
30527jenkins - wso2_oauthJenkins controller file system.4/12/20234.3MediumCVE- 2023-Jenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex theImage: CVE- Image: CVE								
CVE- Jenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 2023- HTTP endpoint, allowing attackers to reindex the		ienkins - wso2 oauth		4/12/2023	4.3	Medium		
CVE-and earlier does not require POST requests for an2023-HTTP endpoint, allowing attackers to reindex the	55527	jennins wsoz_oudul		., 12, 2023		meanann		
2023- HTTP endpoint, allowing attackers to reindex the	CVF-							
		jenkins - lucene-search		4/12/2022	∆ २	Medium		
	30323	jenkins - เนียยายาริติสิเปน		7/ 12/ 2023	+.J	weaturn		

CVE- 2023- 30530	jenkins - consul_kv_builder	Jenkins Consul KV Builder Plugin 2.0.13 and earlier stores the HashiCorp Consul ACL Token unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.	4/12/2023	4.3	Medium
CVE-					
2023-		Microsoft Edge (Chromium-based) Tampering			
28301	microsoft - edge	Vulnerability	4/11/2023	3.7	Low
		A logic issue was addressed with improved			
CVE-		restrictions. This issue is fixed in iOS 16. A person			
2022-		with physical access to a device may be able to use			
32871	apple - iphone_os	Siri to access private calendar information	4/10/2023	2.4	Low
		A logic issue was addressed with improved			
		restrictions. This issue is fixed in iOS 16.2 and			
CVE-		iPadOS 16.2. A user with physical access to a locked			
2022-		Apple Watch may be able to view user photos via			
46717	apple - multiple products	accessibility features	4/10/2023	2.4	Low

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.