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

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٨ أبريل إلى ١٥ أبريل. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 8th of April to 15th of April. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity

CVE-2023-27602	apache - linkis	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
		
		<=1.3.1, we suggest turning on the file path check switch in linkis.properties
		
		`wds.linkis.workspace.filesystem.owner.check=true`
		`wds.linkis.workspace.filesystem.path.check=true`
			4/10/2023	9.8	Critical

CVE-2023-27603	apache - linkis	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. We recommend users upgrade the version of Linkis to version 1.3.2.	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-2023-29216	apache - linkis	In Apache Linkis <=1.3.1, because the parameters are not effectively filtered, the attacker uses the MySQL 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.			
CVE-2022-46709	apple - iphone_os	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 16. An app may be able to execute arbitrary code with kernel privileges	4/10/2023	9.8	Critical
CVE-2023-27497	sap - diagnostics_agent	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. On successful exploitation, the attacker can completely compromise confidentiality, integrity and availability of the system.	4/11/2023	9.8	Critical
CVE-2023-28765	sap - multiple products	An attacker with basic privileges in SAP BusinessObjects Business Intelligence Platform (Promotion Management) - versions 420, 430, can get access to lcmbiar file and further decrypt the file. After this attacker can gain access to BI user's passwords and depending on the privileges of the BI user, the attacker can perform operations that can completely compromise the application.	4/11/2023	9.8	Critical
CVE-2023-28489	siemens - cp-8031_firmware	A vulnerability has been identified in CP-8031 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. The vulnerability could allow an unauthenticated remote attacker to perform arbitrary code execution on the device.	4/11/2023	9.8	Critical
CVE-2022-41331	fortinet - fortiproxy	A missing authentication for critical function vulnerability [CWE-306] in FortiPresence infrastructure server before version 1.2.1 allows a remote, unauthenticated attacker to access the Redis and MongoDB instances via crafted authentication requests.	4/11/2023	9.8	Critical
CVE-2023-21554	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	4/11/2023	9.8	Critical
CVE-2023-23384	microsoft - multiple products	Microsoft SQL Server Remote Code Execution Vulnerability	4/11/2023	9.8	Critical
CVE-2023-28250	microsoft - multiple products	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	4/11/2023	9.8	Critical
CVE-2023-28808	hikvision - ds-a71024_firmware	Some Hikvision Hybrid SAN/Cluster Storage products have an access control vulnerability which can be used to obtain the admin permission. The attacker can exploit the vulnerability by sending crafted messages to the affected devices.	4/11/2023	9.8	Critical
CVE-2022-25678	qualcomm - mdm8207_firmware	Memory correction in modem due to buffer overwrite during coap connection	4/13/2023	9.8	Critical
CVE-2022-25740	qualcomm - mdm8207_firmware	Memory corruption in modem due to buffer overwrite while building an IPv6 multicast address based on the MAC address of the iface	4/13/2023	9.8	Critical
CVE-2022-33211	qualcomm - mdm8207_firmware	memory corruption in modem due to improper check while calculating size of serialized CoAP message	4/13/2023	9.8	Critical
CVE-2022-33259	qualcomm - mdm8207_firmware	Memory corruption due to buffer copy without checking the size of input in modem while decoding raw SMS received.	4/13/2023	9.8	Critical
CVE-2023-27987	apache - linkis	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 token for the attack. Generation rules should add random values.	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-2023-28062	dell - multiple products	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 unauthorized actions.	4/11/2023	8.8	High
CVE-2022-27487	fortinet - multiple products	A improper privilege management in Fortinet FortiSandbox version 4.2.0 through 4.2.2, 4.0.0 through 4.0.2 and before 3.2.3 and FortiDeceptor version 4.1.0, 4.0.0 through 4.0.2 and before 3.3.3 allows a remote authenticated attacker to perform unauthorized API calls via crafted HTTP or HTTPS requests.	4/11/2023	8.8	High
CVE-2022-43947	fortinet - multiple products	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-force attacks on other user accounts via injecting valid login sessions.	4/11/2023	8.8	High
CVE-2023-27995	fortinet - fortisoar	A improper neutralization of special elements used 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	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	8.8	High
CVE-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	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	8.8	High
CVE-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	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	8.8	High
CVE-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

CVE-2023-28243	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	8.8	High
CVE-2023-28275	microsoft - multiple products	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	4/11/2023	8.8	High
CVE-2023-28297	microsoft - multiple products	Windows Remote Procedure Call Service (RPCSS) Elevation of Privilege Vulnerability	4/11/2023	8.8	High
CVE-2023-30525	jenkins - report_portal	A cross-site request forgery (CSRF) vulnerability in Jenkins Report Portal Plugin 0.5 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified bearer token authentication.	4/12/2023	8.8	High
CVE-2022-33288	qualcomm - 315_5g_iot_modem_firmware	Memory corruption due to buffer copy without checking the size of input in Core while sending SCM command to get write protection information.	4/13/2023	8.8	High
CVE-2023-2033	google - chrome	Type confusion in V8 in Google Chrome prior to 112.0.5615.121 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	4/14/2023	8.8	High
CVE-2023-26458	sap - landscape_management	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 only be accessed by authenticated SAP Landscape Management users, but they can escalate their privileges to the SAP Solution Manager system.	4/11/2023	8.7	High
CVE-2023-28206	apple - multiple products	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, macOS Ventura 13.3.1. An app may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.	4/10/2023	8.6	High
CVE-2023-27267	sap - diagnostics_agent	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 successful exploitation, the attacker can completely compromise confidentiality, integrity and availability of the system.	4/11/2023	8.1	High
CVE-2022-43946	fortinet - forticlient	Multiple vulnerabilities including an incorrect permission assignment for critical resource [CWE-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
CVE-2023-22642	fortinet - multiple products	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.	4/11/2023	8.1	High
CVE-2023-28219	microsoft - multiple products	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	4/11/2023	8.1	High
CVE-2023-28220	microsoft - multiple products	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	4/11/2023	8.1	High
CVE-2023-28244	microsoft - multiple products	Windows Kerberos Elevation of Privilege Vulnerability	4/11/2023	8.1	High
CVE-2023-28268	microsoft - multiple products	Netlogon RPC Elevation of Privilege Vulnerability	4/11/2023	8.1	High

CVE-2023-28231	microsoft - multiple products	DHCP Server Service Remote Code Execution Vulnerability	4/11/2023	8	High
CVE-2023-30456	linux - multiple products	An issue was discovered in arch/x86/kvm/vmx/nested.c in the Linux kernel before 6.2.8. nVMX on x86_64 lacks consistency checks for CR0 and CR4.	4/10/2023	7.8	High
CVE-2022-42858	apple - macos	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.1. An app may be able to execute arbitrary code with kernel privileges	4/10/2023	7.8	High
CVE-2023-26293	siemens - multiple products	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 system configuration file, an attacker could exploit this vulnerability to achieve arbitrary code execution.	4/11/2023	7.8	High
CVE-2023-29053	siemens - multiple products	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 structure while parsing specially crafted JT files. This could allow an attacker to execute code in the context of the current process.	4/11/2023	7.8	High
CVE-2022-40679	fortinet - multiple products	An improper neutralization of special elements 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 through 6.2.2, 6.1.0 through 6.1.4 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands.	4/11/2023	7.8	High
CVE-2022-40682	fortinet - multiple products	A incorrect authorization in Fortinet FortiClient (Windows) 7.0.0 - 7.0.7, 6.4.0 - 6.4.9, 6.2.0 - 6.2.9 and 6.0.0 - 6.0.10 allows an attacker to execute unauthorized code or commands via sending a crafted request to a specific named pipe.	4/11/2023	7.8	High
CVE-2022-42470	fortinet - multiple products	A relative path traversal vulnerability in Fortinet FortiClient (Windows) 7.0.0 - 7.0.7, 6.4.0 - 6.4.9, 6.2.0 - 6.2.9 and 6.0.0 - 6.0.10 allows an attacker to execute unauthorized code or commands via sending a crafted request to a specific named pipe.	4/11/2023	7.8	High
CVE-2022-43948	fortinet - multiple products	A improper neutralization of special elements used 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 versions allows attacker to execute unauthorized code or commands via specifically crafted arguments to existing commands.	4/11/2023	7.8	High
CVE-2023-22635	fortinet - multiple products	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 versions, 5.2 all versions, 5.0 all versions and 4.0 all versions may allow a local attacker to escalate their privileges via modifying the installer upon upgrade.	4/11/2023	7.8	High
CVE-2023-23375	microsoft - multiple products	Microsoft ODBC and OLE DB Remote Code Execution Vulnerability	4/11/2023	7.8	High
CVE-2023-24893	microsoft - visual_studio_code	Visual Studio Code Remote Code Execution Vulnerability	4/11/2023	7.8	High
CVE-2023-24912	microsoft - multiple products	Windows Graphics Component Elevation of Privilege Vulnerability	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-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-2023-28246	microsoft - multiple products	Windows Registry Elevation of Privilege Vulnerability	4/11/2023	7.8	High
CVE-2023-28248	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	4/11/2023	7.8	High
CVE-2023-28252	microsoft - multiple products	Windows Common Log File System Driver Elevation of Privilege Vulnerability	4/11/2023	7.8	High
CVE-2023-28260	microsoft - multiple products	.NET DLL Hijacking Remote Code Execution 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-2023-28274	microsoft - multiple products	Windows Win32k Elevation of Privilege Vulnerability	4/11/2023	7.8	High
CVE-2023-28285	microsoft - multiple products	Microsoft Office Remote Code Execution Vulnerability	4/11/2023	7.8	High
CVE-2023-28291	microsoft - raw_image_extension	Raw Image Extension Remote Code Execution Vulnerability	4/11/2023	7.8	High
CVE-2023-28292	microsoft - raw_image_extension	Raw Image Extension Remote Code Execution Vulnerability	4/11/2023	7.8	High
CVE-2023-28293	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	4/11/2023	7.8	High
CVE-2023-28296	microsoft - multiple products	Visual Studio Remote Code Execution Vulnerability	4/11/2023	7.8	High
CVE-2023-28304	microsoft - multiple products	Microsoft ODBC and OLE DB Remote Code Execution Vulnerability	4/11/2023	7.8	High
CVE-2023-28311	microsoft - multiple products	Microsoft Word Remote Code Execution Vulnerability	4/11/2023	7.8	High
CVE-2023-1829	linux - linux_kernel	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 privileges to root. We recommend upgrading past commit 8c710f75256bb3cf05ac7b1672c82b92c43f3d28.	4/12/2023	7.8	High
CVE-2023-26371	adobe - dimension	Adobe Dimension version 3.4.8 (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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26372	adobe - dimension	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 context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High

CVE-2023-26373	adobe - dimension	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 context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26395	adobe - multiple products	Adobe Acrobat Reader versions 23.001.20093 (and 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 the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26396	adobe - multiple products	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 user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26405	adobe - multiple products	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 context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26406	adobe - multiple products	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 context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26407	adobe - multiple products	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 context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26408	adobe - multiple products	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 context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26417	adobe - multiple products	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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26418	adobe - multiple products	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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26419	adobe - multiple products	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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26420	adobe - multiple products	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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High

CVE-2023-26421	adobe - multiple products	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 execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26422	adobe - multiple products	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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26423	adobe - multiple products	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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26424	adobe - multiple products	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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26425	adobe - multiple products	Adobe Acrobat Reader versions 23.001.20093 (and 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 code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-21582	adobe - digital_editions	Adobe Digital Editions version 4.5.11.187303 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-22235	adobe - multiple products	InCopy versions 18.1 (and earlier), 17.4 (and earlier) are affected 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 interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26383	adobe - substance_3d_stager	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 execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26384	adobe - substance_3d_stager	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected 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 interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26388	adobe - substance_3d_stager	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26389	adobe - substance_3d_stager	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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26390	adobe - substance_3d_stager	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	4/12/2023	7.8	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.			
CVE-2023-26391	adobe - substance_3d_stager	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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26392	adobe - substance_3d_stager	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected 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 interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26393	adobe - substance_3d_stager	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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26394	adobe - substance_3d_stager	Adobe Substance 3D Stager version 2.0.1 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2023-26402	adobe - substance_3d_stager	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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	7.8	High
CVE-2022-33296	qualcomm - 315_5g_iot_modem_firmware	Memory corruption due to integer overflow to buffer overflow in Modem while parsing Traffic Channel Neighbor List Update message.	4/13/2023	7.8	High
CVE-2022-40532	qualcomm - 315_5g_iot_modem_firmware	Memory corruption due to integer overflow or wraparound in WLAN while sending WMI cmd from host to target.	4/13/2023	7.8	High
CVE-2023-21630	qualcomm - qca6391_firmware	Memory Corruption in Multimedia Framework due to integer overflow when synx bind is called along with synx signal.	4/13/2023	7.8	High
CVE-2023-26398	adobe - substance_3d_designer	Adobe Substance 3D Designer version 12.4.0 (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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/13/2023	7.8	High
CVE-2023-26409	adobe - substance_3d_designer	Adobe Substance 3D Designer version 12.4.0 (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 current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/13/2023	7.8	High
CVE-2023-26410	adobe - substance_3d_designer	Adobe Substance 3D Designer version 12.4.0 (and earlier) is affected 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 interaction in that a victim must open a malicious file.	4/13/2023	7.8	High
CVE-2023-26411	adobe - substance_3d_designer	Adobe Substance 3D Designer version 12.4.0 (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	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.			
CVE-2023-26412	adobe - substance_3d_designer	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 execution in the 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
CVE-2023-26413	adobe - substance_3d_designer	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 execution in the 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
CVE-2023-26414	adobe - substance_3d_designer	Adobe Substance 3D Designer version 12.4.0 (and earlier) is affected 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 interaction in that a victim must open a malicious file.	4/13/2023	7.8	High
CVE-2023-26415	adobe - substance_3d_designer	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 execution in the 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
CVE-2023-26416	adobe - substance_3d_designer	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 execution in the 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
CVE-2023-29491	gnu - ncurses	ncurses before 6.4 20230408, when used by a setuid application, allows local users to trigger security-relevant memory corruption via malformed data in a terminfo database file that is found in $HOME/.terminfo or reached via the TERMINFO or TERM environment variable.	4/14/2023	7.8	High
CVE-2023-27727	f5 - nginx	Nginx NJS v0.7.10 was discovered to contain a segmentation violation via the function njs_function_frame at src/njs_function.h.	4/9/2023	7.5	High
CVE-2023-27728	f5 - nginx	Nginx NJS v0.7.10 was discovered to contain a segmentation violation via the function njs_dump_is_recursive at src/njs_vmcode.c.	4/9/2023	7.5	High
CVE-2023-27729	f5 - nginx	Nginx NJS v0.7.10 was discovered to contain an illegal memcpy via the function njs_vmcode_return at src/njs_vmcode.c.	4/9/2023	7.5	High
CVE-2023-27730	f5 - nginx	Nginx NJS v0.7.10 was discovered to contain a segmentation violation via the function njs_lvlhsh_find at src/njs_lvlhsh.c.	4/9/2023	7.5	High
CVE-2022-46716	apple - multiple products	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.1, iOS 16.2 and iPadOS 16.2. Private Relay functionality did not match system settings	4/10/2023	7.5	High
CVE-2022-43716	siemens - simatic_cp_1242-7_v2_firmware	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 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	4/11/2023	7.5	High

		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.			
CVE-2022-43767	siemens - simatic_cp_1242-7_v2_firmware	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 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 service condition. An attacker may cause a denial of service situation of the webserver of the affected product.	4/11/2023	7.5	High
CVE-2022-43768	siemens - simatic_cp_1242-7_v2_firmware	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 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 service condition. An attacker may cause a denial of service situation of the webserver of the affected product.	4/11/2023	7.5	High
CVE-2023-28766	siemens - siprotec_5_6md85_firmware	A vulnerability has been identified in SIPROTEC 5 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 7SA84 (CP200) (All versions), SIPROTEC 5 7SA86 (CP200) (All versions), SIPROTEC 5 7SA86 (CP300) (All versions < V9.40), SIPROTEC 5 7SA87 (CP200) (All versions), SIPROTEC 5 7SA87 (CP300) (All versions < V9.40), SIPROTEC 5 7SD82 (CP100) (All versions), SIPROTEC 5 7SD82 (CP150) (All versions < V9.40), SIPROTEC 5 7SD84 (CP200) (All versions), SIPROTEC 5 7SD86 (CP200) (All versions),	4/11/2023	7.5	High

		SIPROTEC 5 7SD86 (CP300) (All versions < V9.40), SIPROTEC 5 7SD87 (CP200) (All versions), SIPROTEC 5 7SD87 (CP300) (All versions < V9.40), SIPROTEC 5 7SJ81 (CP100) (All versions), SIPROTEC 5 7SJ81 (CP150) (All versions < V9.40), SIPROTEC 5 7SJ82 (CP100) (All versions), SIPROTEC 5 7SJ82 (CP150) (All versions < V9.40), SIPROTEC 5 7SJ85 (CP200) (All versions), SIPROTEC 5 7SJ85 (CP300) (All versions < V9.40), SIPROTEC 5 7SJ86 (CP200) (All versions), SIPROTEC 5 7SJ86 (CP300) (All versions < V9.40), SIPROTEC 5 7SK82 (CP100) (All versions), SIPROTEC 5 7SK82 (CP150) (All versions < V9.40), SIPROTEC 5 7SK85 (CP200) (All versions), SIPROTEC 5 7SK85 (CP300) (All versions < V9.40), SIPROTEC 5 7SL82 (CP100) (All versions), SIPROTEC 5 7SL82 (CP150) (All versions < V9.40), SIPROTEC 5 7SL86 (CP200) (All versions), SIPROTEC 5 7SL86 (CP300) (All versions < V9.40), SIPROTEC 5 7SL87 (CP200) (All versions), SIPROTEC 5 7SL87 (CP300) (All versions < V9.40), SIPROTEC 5 7SS85 (CP200) (All versions), SIPROTEC 5 7SS85 (CP300) (All versions < V9.40), SIPROTEC 5 7ST85 (CP200) (All versions), SIPROTEC 5 7ST85 (CP300) (All versions), SIPROTEC 5 7ST86 (CP300) (All versions < V9.40), SIPROTEC 5 7SX82 (CP150) (All versions < V9.40), SIPROTEC 5 7SX85 (CP300) (All versions < V9.40), SIPROTEC 5 7UM85 (CP300) (All versions < V9.40), SIPROTEC 5 7UT82 (CP100) (All versions), SIPROTEC 5 7UT82 (CP150) (All versions < V9.40), SIPROTEC 5 7UT85 (CP200) (All versions), SIPROTEC 5 7UT85 (CP300) (All versions < V9.40), SIPROTEC 5 7UT86 (CP200) (All versions), SIPROTEC 5 7UT86 (CP300) (All versions < V9.40), SIPROTEC 5 7UT87 (CP200) (All versions), SIPROTEC 5 7UT87 (CP300) (All versions < V9.40), SIPROTEC 5 7VE85 (CP300) (All versions < V9.40), SIPROTEC 5 7VK87 (CP200) (All versions), SIPROTEC 5 7VK87 (CP300) (All versions < V9.40), SIPROTEC 5 7VU85 (CP300) (All versions < V9.40), SIPROTEC 5 Communication Module ETH-BA-2EL (All versions < V9.40), SIPROTEC 5 Communication Module ETH-BB-2FO (All versions < V9.40), SIPROTEC 5 Communication Module ETH-BD-2FO (All versions < V9.40), SIPROTEC 5 Compact 7SX800 (CP050) (All versions < V9.40). Affected devices lack proper validation of http request parameters of the hosted web service. An unauthenticated remote attacker could send specially crafted packets that could cause denial of service condition of the target device.			
CVE-2023-28828	siemens - polarion_alm	A vulnerability has been identified in Polarion ALM (All versions < V2304.0). The application contains a XML External Entity Injection (XXE) vulnerability. This could allow an attacker to view files on the application server filesystem.	4/11/2023	7.5	High
CVE-2022-43951	fortinet - multiple products	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.11 and below, 8.7.6 and below may allow an unauthenticated attacker to access sensitive information via crafted HTTP requests.	4/11/2023	7.5	High
CVE-2023-21769	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	4/11/2023	7.5	High
CVE-2023-24860	microsoft - malware_protection_engine	Microsoft Defender Denial of Service Vulnerability	4/11/2023	7.5	High
CVE-2023-24885	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	4/11/2023	7.5	High
CVE-2023-24931	microsoft - multiple products	Windows Secure Channel Denial of Service Vulnerability	4/11/2023	7.5	High
CVE-2023-28217	microsoft - multiple products	Windows Network Address Translation (NAT) Denial of Service Vulnerability	4/11/2023	7.5	High
CVE-2023-28227	microsoft - multiple products	Windows Bluetooth Driver Remote Code Execution Vulnerability	4/11/2023	7.5	High

CVE-2023-28232	microsoft - multiple products	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability	4/11/2023	7.5	High
CVE-2023-28233	microsoft - multiple products	Windows Secure Channel Denial of Service Vulnerability	4/11/2023	7.5	High
CVE-2023-28234	microsoft - multiple products	Windows Secure Channel Denial of Service Vulnerability	4/11/2023	7.5	High
CVE-2023-28238	microsoft - multiple products	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability	4/11/2023	7.5	High
CVE-2023-28241	microsoft - multiple products	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability	4/11/2023	7.5	High
CVE-2023-28247	microsoft - multiple products	Windows Network File System Information Disclosure Vulnerability	4/11/2023	7.5	High
CVE-2023-28300	microsoft - azure_service_connector	Azure Service Connector Security Feature Bypass Vulnerability	4/11/2023	7.5	High
CVE-2023-28302	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	4/11/2023	7.5	High
CVE-2023-30513	jenkins - kubernetes	Jenkins Kubernetes Plugin 3909.v1f2c633e8590 and earlier does not properly mask (i.e., replace with asterisks) credentials in the build log when push mode for durable task logging is enabled.	4/12/2023	7.5	High
CVE-2023-30514	jenkins - azure_key_vault	Jenkins Azure Key Vault Plugin 187.va_cd5fecd198a_ and earlier does not properly mask (i.e., replace with asterisks) credentials in the build log when push mode for durable task logging is enabled.	4/12/2023	7.5	High
CVE-2023-30515	jenkins - thycotic_devops_secrets_vault	Jenkins Thycotic DevOps Secrets Vault Plugin 1.0.0 and earlier does not properly mask (i.e., replace with asterisks) credentials in the build log when push mode for durable task logging is enabled.	4/12/2023	7.5	High
CVE-2022-25726	qualcomm - mdm9205_firmware	Information disclosure in modem data due to array out of bound access while handling the incoming DNS response packet	4/13/2023	7.5	High
CVE-2022-25731	qualcomm - mdm9205_firmware	Information disclosure in modem due to buffer over-read while processing packets from DNS server	4/13/2023	7.5	High
CVE-2022-25737	qualcomm - mdm8207_firmware	Information disclosure in modem due to missing NULL check while reading packets received from local network	4/13/2023	7.5	High
CVE-2022-25747	qualcomm - mdm8207_firmware	Information disclosure in modem due to improper input validation during parsing of upcoming CoAP message	4/13/2023	7.5	High
CVE-2022-33222	qualcomm - mdm9205_firmware	Information disclosure due to buffer over-read while parsing DNS response packets in Modem.	4/13/2023	7.5	High
CVE-2022-33223	qualcomm - mdm8207_firmware	Transient DOS in Modem due to null pointer dereference while processing the incoming packet with http chunked encoding.	4/13/2023	7.5	High
CVE-2022-33228	qualcomm - mdm8207_firmware	Information disclosure sue to buffer over-read in modem while processing ipv6 packet with hop-by-hop or destination option in header.	4/13/2023	7.5	High
CVE-2022-33258	qualcomm - mdm8207_firmware	Information disclosure due to buffer over-read in modem while reading configuration parameters.	4/13/2023	7.5	High
CVE-2022-33287	qualcomm - 9205_lte_modem_firmware	Information disclosure in Modem due to buffer over-read while getting length of Unfragmented headers in an IPv6 packet.	4/13/2023	7.5	High
CVE-2022-33291	qualcomm - 9205_lte_modem_firmware	Information disclosure in Modem due to buffer over-read while receiving a IP header with malformed length.	4/13/2023	7.5	High
CVE-2022-33294	qualcomm - mdm8207_firmware	Transient DOS in Modem due to NULL pointer dereference while receiving response of lwm2m registration/update/bootstrap request message.	4/13/2023	7.5	High
CVE-2022-33295	qualcomm - mdm8207_firmware	Information disclosure in Modem due to buffer over-read while parsing the wms message received given the buffer and its length.	4/13/2023	7.5	High
CVE-2022-40503	qualcomm - 9206_lte_modem_firmware	Information disclosure due to buffer over-read in Bluetooth Host while A2DP streaming.	4/13/2023	7.5	High
CVE-2023-29054	siemens - scalance_x200-4p_irt_firmware	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < V5.5.2), SCALANCE X201-3P IRT (All versions < V5.5.2), SCALANCE X201-3P	4/11/2023	7.4	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. 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.			
CVE-2023-29187	sap - sapsetup	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 of the very same Windows PC. A successful attack depends on various preconditions beyond the attackers control.	4/11/2023	7.3	High
CVE-2023-28254	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	4/11/2023	7.2	High
CVE-2023-20118	cisco - multiple products	A vulnerability in the web-based management 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. Cisco has not and will not release software updates that address this vulnerability.	4/13/2023	7.2	High
CVE-2023-29084	zohocorp - multiple products	Zoho ManageEngine ADManager Plus through 7180 allows for authenticated users to exploit command injection via Proxy settings.	4/13/2023	7.2	High
CVE-2022-47338	google - multiple products	In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service.	4/11/2023	7.1	High
CVE-2023-28222	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	4/11/2023	7.1	High
CVE-2023-28224	microsoft - multiple products	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability	4/11/2023	7.1	High
CVE-2023-1989	linux - multiple products	A use-after-free flaw was found in btsdio_remove in drivers\bluetooth\btsdio.c in the Linux Kernel. In this flaw, a call to btsdio_remove with an unfinished job, may cause a race problem leading to a UAF on hdev devices.	4/11/2023	7	High
CVE-2023-24914	microsoft - windows_11_22h2	Win32k Elevation of Privilege Vulnerability	4/11/2023	7	High
CVE-2023-28216	microsoft - multiple products	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability	4/11/2023	7	High
CVE-2023-28218	microsoft - multiple products	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	4/11/2023	7	High

CVE-2023-28221	microsoft - multiple products	Windows Error Reporting Service Elevation of Privilege Vulnerability	4/11/2023	7	High
CVE-2023-28229	microsoft - multiple products	Windows CNG Key Isolation Service Elevation of 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
CVE-2023-1872	linux - linux_kernel	A use-after-free vulnerability in the Linux Kernel 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. We recommend upgrading past commit 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
CVE-2023-28249	microsoft - multiple products	Windows Boot Manager Security Feature Bypass Vulnerability	4/11/2023	6.8	Medium
CVE-2023-28269	microsoft - multiple products	Windows Boot Manager Security Feature Bypass Vulnerability	4/11/2023	6.8	Medium
CVE-2023-28270	microsoft - multiple products	Windows Lock Screen Security Feature Bypass Vulnerability	4/11/2023	6.8	Medium
CVE-2022-33289	qualcomm - 315_5g_iot_modem_firmware	Memory corruption occurs in Modem due to improper validation of array index when malformed APDU is sent from card.	4/13/2023	6.8	Medium
CVE-2023-28223	microsoft - multiple products	Windows Domain Name Service Remote Code Execution Vulnerability	4/11/2023	6.6	Medium
CVE-2023-28255	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	4/11/2023	6.6	Medium
CVE-2023-28256	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	4/11/2023	6.6	Medium
CVE-2023-28278	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	4/11/2023	6.6	Medium
CVE-2023-28305	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	4/11/2023	6.6	Medium
CVE-2023-28306	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	4/11/2023	6.6	Medium
CVE-2023-28307	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	4/11/2023	6.6	Medium
CVE-2023-28308	microsoft - multiple products	Windows DNS Server Remote Code Execution Vulnerability	4/11/2023	6.6	Medium
CVE-2023-24626	gnu - screen	socket.c in GNU Screen through 4.9.0, when installed setuid or setgid (the default on platforms such as Arch Linux and FreeBSD), allows local users to send a privileged SIGHUP signal to any PID, causing a denial of service or disruption of the target process.	4/8/2023	6.5	Medium
CVE-2023-28340	zohocorp - multiple products	Zoho ManageEngine Applications Manager through 16320 allows the admin user to conduct an XXE attack.	4/11/2023	6.5	Medium
CVE-2023-28761	sap - netweaver_enterprise_portal	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 access a service which will enable them to access or modify server settings and data, leading to limited impact on confidentiality and integrity.	4/11/2023	6.5	Medium
CVE-2023-28763	sap - multiple products	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker authenticated as a non-administrative user to craft a request with 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.			
CVE-2023-29185	sap - multiple products	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 circumstances which can consume the server's resources sufficiently to make it unavailable over the network without any user interaction.	4/11/2023	6.5	Medium
CVE-2023-29186	sap - multiple products	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 remote attacker has sufficient (administrative) privileges then potentially critical OS files can be overwritten making the system unavailable.	4/11/2023	6.5	Medium
CVE-2022-27485	fortinet - multiple products	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 with read permission to retrieve arbitrary files from the underlying Linux system via a crafted HTTP request.	4/11/2023	6.5	Medium
CVE-2023-24883	microsoft - multiple products	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	4/11/2023	6.5	Medium
CVE-2023-28267	microsoft - multiple products	Remote Desktop Protocol Client Information Disclosure Vulnerability	4/11/2023	6.5	Medium
CVE-2023-28288	microsoft - multiple products	Microsoft SharePoint Server Spoofing Vulnerability	4/11/2023	6.5	Medium
CVE-2023-28312	microsoft - azure_machine_learning	Azure Machine Learning Information Disclosure Vulnerability	4/11/2023	6.5	Medium
CVE-2023-28488	intel - connman	client.c in gdhcp in ConnMan through 1.41 could be used by network-adjacent attackers (operating a crafted DHCP server) to cause a stack-based buffer overflow and denial of service, terminating the connman process.	4/12/2023	6.5	Medium
CVE-2023-0004	paloaltonetworks - multiple products	A local file deletion vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator to delete files from the local file system with elevated privileges. These files can include logs and system components that impact the integrity and availability of PAN-OS software.	4/12/2023	6.5	Medium
CVE-2023-30516	jenkins - image_tag_parameter	Jenkins Image Tag Parameter Plugin 2.0 improperly introduces an option to opt out of SSL/TLS certificate validation when connecting to Docker registries, resulting in job configurations using Image Tag Parameters that were created before 2.0 having SSL/TLS certificate validation disabled by default.	4/12/2023	6.5	Medium
CVE-2023-30526	jenkins - report_portal	A missing permission check in Jenkins Report Portal Plugin 0.5 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified bearer token authentication.	4/12/2023	6.5	Medium
CVE-2023-30528	jenkins - wso2_oauth	Jenkins WSO2 Oauth Plugin 1.0 and earlier does not mask the WSO2 Oauth client secret on the global configuration form, increasing the potential for attackers to observe and capture it.	4/12/2023	6.5	Medium
CVE-2023-30531	jenkins - consul_kv_builder	Jenkins Consul KV Builder Plugin 2.0.13 and earlier does not mask the HashiCorp Consul ACL Token on the global configuration form, increasing the potential for attackers to observe and capture it.	4/12/2023	6.5	Medium
CVE-2023-30532	jenkins - turboscript	A missing permission check in Jenkins TurboScript Plugin 1.3 and earlier allows attackers with Item/Read permission to trigger builds of jobs corresponding to the attacker-specified repository.	4/12/2023	6.5	Medium
CVE-2023-20863	vmware - multiple products	In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.	4/13/2023	6.5	Medium

CVE-2023-20866	vmware - spring_session	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 who have access to the application logs and can be used for session hijacking. Specifically, an application is vulnerable if it is using HeaderHttpSessionIdResolver.	4/13/2023	6.5	Medium
CVE-2023-27897	sap - multiple products	In SAP CRM - versions 700, 701, 702, 712, 713, an 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 executed, the attack can can have limited impact on confidentiality and integrity of non-critical user or application data and application availability.	4/11/2023	6.3	Medium
CVE-2023-23588	siemens - simatic_ipc647d_firmware	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 decrypt intercepted local traffic between the browser and the application and could perform a man-in-the-middle attack in order to modify data in transit.	4/11/2023	6.3	Medium
CVE-2023-0006	paloaltonetworks - multiple products	A local file deletion vulnerability in the Palo Alto Networks GlobalProtect app on Windows devices enables a user to delete system files from the endpoint with elevated privileges through a race condition.	4/12/2023	6.3	Medium
CVE-2023-26788	veritas - netbackup_appliance_firmware	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 unexpected ways. Any changes made to the header would just cause the request to be sent to a completely different Domain/IP address.	4/10/2023	6.1	Medium
CVE-2023-28341	zohocorp - multiple products	Stored Cross site scripting (XSS) vulnerability in Zoho ManageEngine Applications Manager through 16340 allows an unauthenticated user to inject malicious javascript on the incorrect login details page.	4/11/2023	6.1	Medium
CVE-2023-27499	sap - multiple products	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 browser. The information from the victim's web browser can either be modified or read and sent to the attacker.	4/11/2023	6.1	Medium
CVE-2022-35850	fortinet - multiple products	An improper neutralization of script-related HTML 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 allow a remote unauthenticated attacker to trigger a reflected cross site scripting (XSS) attack via the "reset-password" page.	4/11/2023	6.1	Medium
CVE-2022-41330	fortinet - multiple products	An improper neutralization of input during web 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 through 6.4.11 and before 6.2.12 and FortiProxy 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-2022-43955	fortinet - multiple products	An improper neutralization of input during web page generation [CWE-79] in the FortiWeb web interface 7.0.0 through 7.0.3, 6.3.0 through 6.3.21,	4/11/2023	6.1	Medium

		6.4 all versions, 6.2 all versions, 6.1 all versions and 6.0 all versions may allow an unauthenticated and remote attacker to perform a reflected cross site scripting attack (XSS) via injecting malicious payload in log entries used to build report.			
CVE-2023-24935	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4/11/2023	6.1	Medium
CVE-2023-28313	microsoft - send_customer_voice_survey_from_dynamics_365	Microsoft Dynamics 365 Customer Voice Cross-Site Scripting Vulnerability	4/11/2023	6.1	Medium
CVE-2023-28314	microsoft - multiple products	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	4/11/2023	6.1	Medium
CVE-2023-28368	tp-link - multiple products	TP-Link L2 switch T2600G-28SQ firmware versions prior to 'T2600G-28SQ(UN)_V1_1.0.6 Build 20230227' uses vulnerable SSH host keys. A fake device may be prepared to spoof the affected device with the vulnerable host key.If the administrator may be tricked to login to the fake device, the credential information for the affected device may be obtained.	4/11/2023	5.7	Medium
CVE-2022-46703	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.1, iOS 16.2 and iPadOS 16.2, iOS 15.7.2 and iPadOS 15.7.2. An app may be able to read sensitive location information	4/10/2023	5.5	Medium
CVE-2022-47335	google - multiple products	In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service.	4/11/2023	5.5	Medium
CVE-2022-47336	google - multiple products	In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service.	4/11/2023	5.5	Medium
CVE-2022-47337	google - multiple products	In media service, there is a missing permission check. This could lead to local denial of service in media service.	4/11/2023	5.5	Medium
CVE-2022-47362	google - multiple products	In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service.	4/11/2023	5.5	Medium
CVE-2022-47463	google - multiple products	In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service.	4/11/2023	5.5	Medium
CVE-2022-47464	google - multiple products	In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service.	4/11/2023	5.5	Medium
CVE-2022-47465	google - multiple products	In vdsp service, there is a missing permission check. This could lead to local denial of service in vdsp service.	4/11/2023	5.5	Medium
CVE-2022-47466	google - multiple products	In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service.	4/11/2023	5.5	Medium
CVE-2022-47467	google - multiple products	In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service.	4/11/2023	5.5	Medium
CVE-2022-47468	google - multiple products	In telecom service, there is a missing permission check. This could lead to local denial of service in telecom service.	4/11/2023	5.5	Medium
CVE-2022-42477	fortinet - multiple products	An improper input validation vulnerability [CWE-20] in FortiAnalyzer version 7.2.1 and below, version 7.0.6 and below, 6.4 all versions may allow an authenticated attacker to disclose file system information via custom dataset SQL queries.	4/11/2023	5.5	Medium
CVE-2023-28228	microsoft - multiple products	Windows Spoofing Vulnerability	4/11/2023	5.5	Medium
CVE-2023-28253	microsoft - multiple products	Windows Kernel Information Disclosure Vulnerability	4/11/2023	5.5	Medium
CVE-2023-28263	microsoft - multiple products	Visual Studio Information Disclosure Vulnerability	4/11/2023	5.5	Medium
CVE-2023-28266	microsoft - multiple products	Windows Common Log File System Driver Information Disclosure Vulnerability	4/11/2023	5.5	Medium
CVE-2023-28271	microsoft - 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-2023-28299	microsoft - multiple products	Visual Studio Spoofing Vulnerability	4/11/2023	5.5	Medium
CVE-2023-26374	adobe - dimension	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 mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26375	adobe - dimension	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 mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26376	adobe - dimension	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 mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26377	adobe - dimension	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 mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26378	adobe - dimension	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 mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26379	adobe - dimension	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 mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26380	adobe - dimension	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 mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26381	adobe - dimension	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 mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26382	adobe - dimension	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 mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26400	adobe - dimension	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 mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26401	adobe - dimension	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	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.			
CVE-2023-26404	adobe - dimension	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 mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26397	adobe - multiple products	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 mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26385	adobe - substance_3d_stager	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 vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26386	adobe - substance_3d_stager	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 vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26387	adobe - substance_3d_stager	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 vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-26403	adobe - substance_3d_stager	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 vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	4/12/2023	5.5	Medium
CVE-2023-28091	hp - oneview	HPE OneView virtual appliance "Migrate server hardware" option may expose sensitive information in an HPE OneView support dump	4/14/2023	5.5	Medium
CVE-2023-24934	microsoft - malware_protection_engine	Microsoft Defender Security Feature Bypass Vulnerability	4/14/2023	5.5	Medium
CVE-2023-29110	sap - multiple products	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 foreign domains. After successful exploitations, an attacker can cause limited impact on the confidentiality and integrity of the application.	4/11/2023	5.4	Medium
CVE-2023-29112	sap - multiple products	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 objects. After successful exploitations, an attacker can cause limited impact on the confidentiality and integrity of the application.	4/11/2023	5.4	Medium
CVE-2023-29189	sap - multiple products	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 network and successful exploitation can lead to exposure of form fields	4/11/2023	5.4	Medium

CVE-2022-43952	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.	4/11/2023	5.4	Medium
CVE-2023-22641	fortinet - multiple products	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 7.0.8, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specially crafted requests.	4/11/2023	5.4	Medium
CVE-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.	4/12/2023	5.4	Medium
CVE-2023-24527	sap - netweaver_as_java_for_deploy_service	SAP NetWeaver AS Java for Deploy Service - version 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.	4/11/2023	5.3	Medium
CVE-2023-29108	sap - multiple products	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 backend applications from unwanted sources.	4/11/2023	5.3	Medium
CVE-2023-30465	apache - multiple products	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-deserialization-vulnerability-learning.html [1] https://github.com/apache/inlong/issues/7529 https://github.com/apache/inlong/issues/7529	4/11/2023	5.3	Medium
CVE-2023-21729	microsoft - multiple products	Remote Procedure Call Runtime Information Disclosure Vulnerability	4/11/2023	5.3	Medium
CVE-2023-28226	microsoft - multiple products	Windows Enroll Engine Security Feature Bypass Vulnerability	4/11/2023	5.3	Medium
CVE-2022-48437	openbsd - multiple products	An issue was discovered in x509/x509_verify.c in 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.	4/12/2023	5.3	Medium
CVE-2023-30517	jenkins - neuvector_vulnerability_scanner	Jenkins NeuVector Vulnerability Scanner Plugin 1.22 and earlier unconditionally disables SSL/TLS certificate and hostname validation when connecting to a configured NeuVector Vulnerability 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

		unauthenticated attackers to trigger builds of jobs corresponding to the attacker-specified repository.			
CVE-2023-30521	jenkins - assembla_merge_request_builder	A missing permission check in Jenkins Assembla merge request builder Plugin 1.1.13 and earlier allows unauthenticated attackers to trigger builds of jobs corresponding to the attacker-specified repository.	4/12/2023	5.3	Medium
CVE-2023-28277	microsoft - windows_server_2022	Windows DNS Server Information Disclosure Vulnerability	4/11/2023	4.9	Medium
CVE-2023-0005	paloaltonetworks - multiple products	A vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator to expose the plaintext values of secrets stored in the device configuration and encrypted API keys.	4/12/2023	4.9	Medium
CVE-2023-1990	linux - multiple products	A use-after-free flaw was found in ndlc_remove in drivers/nfc/st-nci/ndlc.c in the Linux Kernel. This flaw could allow an attacker to crash the system due to a race problem.	4/12/2023	4.7	Medium
CVE-2023-29109	sap - multiple products	The SAP Application Interface Framework (Message Dashboard) - versions AIF 703, AIFX 702, S4CORE 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E, application allows an Excel formula injection. An authorized attacker can inject arbitrary Excel formulas into fields like the Tooltip of the Custom 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	Medium
CVE-2023-28276	microsoft - multiple products	Windows Group Policy Security Feature Bypass Vulnerability	4/11/2023	4.4	Medium
CVE-2023-1903	sap - hcm_fiori_app_my_forms	SAP HCM Fiori App My Forms (Fiori 2.0) - version 605, does not perform necessary authorization checks for an authenticated user exposing the restricted header data.	4/11/2023	4.3	Medium
CVE-2023-29111	sap - multiple products	The SAP AIF (ODATA 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 cause a low impact on the confidentiality of the application.	4/11/2023	4.3	Medium
CVE-2022-42469	fortinet - 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 NGFW Mode may allow an authenticated SSL-VPN user to bypass the policy via bookmarks in the web portal.	4/11/2023	4.3	Medium
CVE-2023-28284	microsoft - edge	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	4/11/2023	4.3	Medium
CVE-2023-30518	jenkins - thycotic_secret_server	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 Jenkins.	4/12/2023	4.3	Medium
CVE-2023-30522	jenkins - fogbugz	A missing permission check in Jenkins Fogbugz Plugin 2.2.17 and earlier allows attackers with Item/Read permission to trigger builds of jobs 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.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.	4/12/2023	4.3	Medium
CVE-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 attackers to observe and capture them.	4/12/2023	4.3	Medium
CVE-2023-30527	jenkins - wso2_oauth	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 where it can be viewed by users with access to the Jenkins controller file system.	4/12/2023	4.3	Medium
CVE-2023-30529	jenkins - lucene-search	Jenkins Lucene-Search Plugin 387.v938a_ecb_f7fe9 and earlier does not require POST requests for an HTTP endpoint, allowing attackers to reindex the database.	4/12/2023	4.3	Medium

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-2023-28301	microsoft - edge	Microsoft Edge (Chromium-based) Tampering Vulnerability	4/11/2023	3.7	Low
CVE-2022-32871	apple - iphone_os	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 16. A person with physical access to a device may be able to use Siri to access private calendar information	4/10/2023	2.4	Low
CVE-2022-46717	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 16.2 and iPadOS 16.2. A user with physical access to a locked Apple Watch may be able to view user photos via accessibility features	4/10/2023	2.4	Low

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

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