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 ٧ مايو إلى ١٣ مايو. 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 7th of May to 13th of May. 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-2023-27407	siemens - scalance_lpe9403_firmware	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). The web based management of affected device does not properly validate user input, making it susceptible to command injection. This could allow an authenticated remote attacker to access the underlying operating system as the root user.	2023-05-09	9.9	Critical
CVE-2023-31039	apache - brpc	Security vulnerability in Apache bRPC <1.5.0 on all platforms allows attackers to execute arbitrary code via ServerOptions::pid_file. An attacker that can influence the ServerOptions pid_file parameter with which the bRPC server is started can execute arbitrary code with the permissions of the bRPC process. Solution: 1. upgrade to bRPC >= 1.5.0, download link: https://dist.apache.org/repos/dist/release/brpc/1.5.0/ https://dist.apache.org/repos/dist/release/brpc/1.5.0/ 2. If you are using an old version of bRPC and hard to upgrade, you can apply this patch: https://github.com/apache/brpc/pull/2218 https://github.com/apache/brpc/pull/2218	2023-05-08	9.8	Critical
CVE-2023-25754	apache - airflow	Privilege Context Switching Error vulnerability in Apache Software Foundation Apache Airflow.This issue affects Apache Airflow: before 2.6.0.	2023-05-08	9.8	Critical
CVE-2023-22779	hp - multiple products	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2023-05-08	9.8	Critical
CVE-2023-22780	hp - multiple products	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2023-05-08	9.8	Critical
CVE-2023-22781	hp - multiple products	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2023-05-08	9.8	Critical
CVE-2023-22782	hp - multiple products	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the	2023-05-08	9.8	Critical

		ability to execute arbitrary code as a privileged user on the underlying operating system.			
CVE-2023-22783	hp - multiple products	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2023-05-08	9.8	Critical
CVE-2023-22784	hp - multiple products	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2023-05-08	9.8	Critical
CVE-2023-22785	hp - multiple products	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2023-05-08	9.8	Critical
CVE-2023-22786	hp - multiple products	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2023-05-08	9.8	Critical
CVE-2023-23526	apple - multiple products	This was addressed with additional checks by Gatekeeper on files downloaded from an iCloud shared-by-me folder. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. A file from an iCloud shared-by-me folder may be able to bypass Gatekeeper	2023-05-08	9.8	Critical
CVE-2023-27953	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7.5, macOS Monterey 12.6.4, macOS Ventura 13.3. A remote user may be able to cause unexpected system termination or corrupt kernel memory	2023-05-08	9.8	Critical
CVE-2023-28201	apple - multiple products	This issue was addressed with improved state management. This issue is fixed in Safari 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4, macOS Ventura 13.3. A remote user may be able to cause unexpected app termination or arbitrary code execution	2023-05-08	9.8	Critical
CVE-2023-24941	microsoft - multiple products	Windows Network File System Remote Code Execution Vulnerability	2023-05-09	9.8	Critical
CVE-2023-24943	microsoft - multiple products	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	2023-05-09	9.8	Critical
CVE-2023-32569	veritas - multiple products	An issue was discovered in Veritas InfoScale Operations Manager (VIOM) before 7.4.2.800 and 8.x before 8.0.410. The InfoScale VIOM web application is vulnerable to SQL Injection in some of the areas of the application. This allows attackers to submit arbitrary SQL commands on the back-end database to create, read, update, or delete any sensitive data stored in the database.	2023-05-10	9.8	Critical
CVE-2023-32113	sap - multiple products	SAP GUI for Windows - version 7.70, 8.0, allows an unauthorized attacker to gain NTLM authentication information of a victim by tricking it into clicking a prepared shortcut file. Depending on the authorizations of the victim, the attacker can read and modify potentially sensitive information after successful exploitation.	2023-05-09	9.3	Critical
CVE-2023-27958	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7.5, macOS Monterey 12.6.4, macOS Ventura 13.3. A remote user may be able to cause unexpected system termination or corrupt kernel memory	2023-05-08	9.1	Critical
CVE-2023-30744	sap - netweaver_application_server_for_java	In SAP AS NetWeaver JAVA - versions SERVERCORE 7.50, J2EE-FRMW 7.50, CORE-TOOLS 7.50, an unauthenticated attacker can attach to an open interface and make use of an open naming and directory API to instantiate an object which has methods which can be called without further authorization and authentication. A subsequent call to one of these methods can read or change the state of existing services without any effect on availability.	2023-05-09	9.1	Critical
CVE-2023-31038	apache - log4cxx	SQL injection in Log4cxx when using the ODBC appender to send log messages to a database. No fields sent to the database were properly escaped for SQL injection. This has been the case since at least version 0.9.0(released 2003-08-06) Note that Log4cxx is a C++ framework, so only C++ applications are affected.	2023-05-08	8.8	High

		Before version 1.1.0, the ODBC appender was automatically part of Log4cxx if the library was found when compiling the library. As of version 1.1.0, this must be both explicitly enabled in order to be compiled in. Three preconditions must be met for this vulnerability to be possible: 1. Log4cxx compiled with ODBC support(before version 1.1.0, this was auto-detected at compile time) 2. ODBCAppender enabled for logging messages to, generally done via a config file 3. User input is logged at some point. If your application does not have user input, it is unlikely to be affected. Users are recommended to upgrade to version 1.1.0 which properly binds the parameters to the SQL statement, or migrate to the new DBAppender class which supports an ODBC connection in addition to other databases. Note that this fix does require a configuration file update, as the old configuration files will not configure properly. An example is shown below, and more information may be found in the Log4cxx documentation on the ODBCAppender. Example of old configuration snippet: <appender name="SqlODBCAppender" class="ODBCAppender"> <param name="sql" value="INSERT INTO logs (message) VALUES ('%m')" /> ... other params here ... </appender> The migrated configuration snippet with new ColumnMapping parameters: <appender name="SqlODBCAppender" class="ODBCAppender"> <param name="sql" value="INSERT INTO logs (message) VALUES (?)" /> <param name="ColumnMapping" value="message"/> ... other params here ... </appender>			
CVE-2023-22788	arubanetworks - multiple products	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	2023-05-08	8.8	High
CVE-2023-22789	arubanetworks - multiple products	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	2023-05-08	8.8	High
CVE-2023-22790	arubanetworks - multiple products	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface.	2023-05-08	8.8	High

		Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.			
CVE-2023-23532	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to break out of its sandbox	2023-05-08	8.8	High
CVE-2023-27934	apple - macos	A memory initialization issue was addressed. This issue is fixed in macOS Ventura 13.3. A remote user may be able to cause unexpected app termination or arbitrary code execution	2023-05-08	8.8	High
CVE-2023-27935	apple - multiple products	The issue was addressed with improved bounds checks. This issue is fixed in macOS Big Sur 11.7.5, macOS Monterey 12.6.4, macOS Ventura 13.3. A remote user may be able to cause unexpected app termination or arbitrary code execution	2023-05-08	8.8	High
CVE-2023-30898	siemens - multiple products	A vulnerability has been identified in Siveillance Video 2020 R2 (All versions < V20.2 HotfixRev14), Siveillance Video 2020 R3 (All versions < V20.3 HotfixRev12), Siveillance Video 2021 R1 (All versions < V21.1 HotfixRev12), Siveillance Video 2021 R2 (All versions < V21.2 HotfixRev8), Siveillance Video 2022 R1 (All versions < V22.1 HotfixRev7), Siveillance Video 2022 R2 (All versions < V22.2 HotfixRev5), Siveillance Video 2022 R3 (All versions < V22.3 HotfixRev2), Siveillance Video 2023 R1 (All versions < V23.1 HotfixRev1). The Event Server component of affected applications deserializes data without sufficient validations. This could allow an authenticated remote attacker to execute code on the affected system.	2023-05-09	8.8	High
CVE-2023-30899	siemens - multiple products	A vulnerability has been identified in Siveillance Video 2020 R2 (All versions < V20.2 HotfixRev14), Siveillance Video 2020 R3 (All versions < V20.3 HotfixRev12), Siveillance Video 2021 R1 (All versions < V21.1 HotfixRev12), Siveillance Video 2021 R2 (All versions < V21.2 HotfixRev8), Siveillance Video 2022 R1 (All versions < V22.1 HotfixRev7), Siveillance Video 2022 R2 (All versions < V22.2 HotfixRev5), Siveillance Video 2022 R3 (All versions < V22.3 HotfixRev2), Siveillance Video 2023 R1 (All versions < V23.1 HotfixRev1). The Management Server component of affected applications deserializes data without sufficient validations. This could allow an authenticated remote attacker to execute code on the affected system.	2023-05-09	8.8	High
CVE-2023-20046	cisco - multiple products	A vulnerability in the key-based SSH authentication feature of Cisco StarOS Software could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied credentials. An attacker could exploit this vulnerability by sending a valid low-privileged SSH key to an affected device from a host that has an IP address that is configured as the source for a high-privileged user account. A successful exploit could allow the attacker to log in to the affected device through SSH as a high-privileged user. There are workarounds that address this vulnerability.	2023-05-09	8.8	High
CVE-2023-24947	microsoft - multiple products	Windows Bluetooth Driver Remote Code Execution Vulnerability	2023-05-09	8.8	High
CVE-2022-41979	intel - data_center_manager	Protection mechanism failure in the Intel(R) DCM software before version 5.1 may allow an authenticated user to potentially enable escalation of privilege via network access.	2023-05-10	8.8	High
CVE-2022-44610	intel - data_center_manager	Improper authentication in the Intel(R) DCM software before version 5.1 may allow an authenticated user to potentially enable escalation of privilege via network access.	2023-05-10	8.8	High
CVE-2023-27298	intel - wake_up_latency_tracer	Uncontrolled search path in the WULT software maintained by Intel(R) before version 1.0.0 (commit id 592300b) may allow an unauthenticated user to potentially enable escalation of privilege via network access.	2023-05-10	8.8	High
CVE-2023-2457	google - chrome	Out of bounds write in ChromeOS Audio Server in Google Chrome on ChromeOS prior to 113.0.5672.114 allowed a remote attacker to potentially exploit heap corruption via crafted audio file. (Chromium security severity: High)	2023-05-12	8.8	High
CVE-2023-2458	google - chrome	Use after free in ChromeOS Camera in Google Chrome on ChromeOS prior to 113.0.5672.114 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via UI interaction. (Chromium security severity: High)	2023-05-12	8.8	High
CVE-2022-46720	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.1, iOS 16.2 and iPadOS 16.2. An app may be able to break out of its sandbox	2023-05-08	8.6	High
CVE-2023-27944	apple - multiple products	This issue was addressed with a new entitlement. This issue is fixed in macOS Big Sur 11.7.5, macOS Monterey 12.6.4, macOS Ventura 13.3. An app may be able to break out of its sandbox	2023-05-08	8.6	High

CVE-2023-27967	apple - xcode	The issue was addressed with improved memory handling. This issue is fixed in Xcode 14.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges	2023-05-08	8.6	High
CVE-2023-24903	microsoft - multiple products	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	2023-05-09	8.1	High
CVE-2023-28283	microsoft - multiple products	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	2023-05-09	8.1	High
CVE-2023-23525	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7.5, macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to gain root privileges	2023-05-08	7.8	High
CVE-2023-23536	apple - multiple products	The issue was addressed with improved bounds checks. This issue is fixed in macOS Big Sur 11.7.5, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4, macOS Ventura 13.3. An app may be able to execute arbitrary code with kernel privileges	2023-05-08	7.8	High
CVE-2023-23540	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges	2023-05-08	7.8	High
CVE-2023-27936	apple - multiple products	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory	2023-05-08	7.8	High
CVE-2023-27937	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, macOS Big Sur 11.7.5, watchOS 9.4, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously crafted plist may lead to an unexpected app termination or arbitrary code execution	2023-05-08	7.8	High
CVE-2023-27938	apple - macos	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in GarageBand for macOS 10.4.8. Parsing a maliciously crafted MIDI file may lead to an unexpected application termination or arbitrary code execution	2023-05-08	7.8	High
CVE-2023-27946	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Ventura 13.3. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution	2023-05-08	7.8	High
CVE-2023-27949	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Ventura 13.3. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution	2023-05-08	7.8	High
CVE-2023-27957	apple - macos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution	2023-05-08	7.8	High
CVE-2023-27959	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges	2023-05-08	7.8	High
CVE-2023-27960	apple - mac_os_x	This issue was addressed by removing the vulnerable code. This issue is fixed in GarageBand for macOS 10.4.8. An app may be able to gain elevated privileges during the installation of GarageBand	2023-05-08	7.8	High
CVE-2023-27965	apple - macos	A memory corruption issue was addressed with improved state management. This issue is fixed in Studio Display Firmware Update 16.4, macOS Ventura 13.3. An app may be able to execute arbitrary code with kernel privileges	2023-05-08	7.8	High
CVE-2023-27969	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.7.4 and iPadOS 15.7.4, macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges	2023-05-08	7.8	High
CVE-2023-27970	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges	2023-05-08	7.8	High
CVE-2023-28181	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7.7, macOS Ventura 13.3, tvOS 16.4, iOS 15.7.6 and iPadOS 15.7.6, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges	2023-05-08	7.8	High
CVE-2023-32233	linux - linux_kernel	In the Linux kernel through 6.3.1, a use-after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled.	2023-05-08	7.8	High
CVE-2022-44433	google - android	In phoneEx service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High

CVE-2022-48243	google - multiple products	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High
CVE-2022-48244	google - multiple products	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High
CVE-2022-48245	google - multiple products	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High
CVE-2022-48246	google - multiple products	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High
CVE-2022-48247	google - multiple products	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High
CVE-2022-48248	google - multiple products	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High
CVE-2022-48249	google - multiple products	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High
CVE-2022-48250	google - multiple products	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High
CVE-2022-48368	google - multiple products	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High
CVE-2022-48369	google - multiple products	In audio service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High
CVE-2022-48383	google - multiple products	.In srtd service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High
CVE-2022-48384	google - multiple products	In srtd service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High
CVE-2022-48388	google - multiple products	In powerEx service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-05-09	7.8	High
CVE-2023-29092	samsung - exynos_5123_firmware	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface.	2023-05-09	7.8	High
CVE-2023-30986	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < VX.223.0 Update 3), Solid Edge SE2023 (All versions < VX.223.0 Update 2). Affected applications contain a memory corruption vulnerability while parsing specially crafted STP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-19561)	2023-05-09	7.8	High
CVE-2023-24902	microsoft - multiple products	Win32k Elevation of Privilege Vulnerability	2023-05-09	7.8	High
CVE-2023-24905	microsoft - multiple products	Remote Desktop Client Remote Code Execution Vulnerability	2023-05-09	7.8	High
CVE-2023-24946	microsoft - multiple products	Windows Backup Service Elevation of Privilege Vulnerability	2023-05-09	7.8	High
CVE-2023-24949	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-05-09	7.8	High
CVE-2023-24953	microsoft - multiple products	Microsoft Excel Remote Code Execution Vulnerability	2023-05-09	7.8	High
CVE-2023-29336	microsoft - multiple products	Win32k Elevation of Privilege Vulnerability	2023-05-09	7.8	High
CVE-2023-29340	microsoft - av1_video_extension	AV1 Video Extension Remote Code Execution Vulnerability	2023-05-09	7.8	High
CVE-2023-29341	microsoft - av1_video_extension	AV1 Video Extension Remote Code Execution Vulnerability	2023-05-09	7.8	High
CVE-2023-29343	microsoft - windows_sysmon	SysInternals Sysmon for Windows Elevation of Privilege Vulnerability	2023-05-09	7.8	High
CVE-2022-21804	intel - quickassist_technology	Out-of-bounds write in software for the Intel QAT Driver for Windows before version 1.9.0-0008 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-29508	intel - virtual_raid_on_cpu	Null pointer dereference in the Intel(R) VROC software before version 7.7.6.1003 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-29919	intel - virtual_raid_on_cpu	Use after free in the Intel(R) VROC software before version 7.7.6.1003 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High

CVE-2022-30338	intel - virtual_raid_on_cpu	Incorrect default permissions in the Intel(R) VROC software before version 7.7.6.1003 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-32766	intel - compute_stick_stk2 mv64cc_firmware	Improper input validation for some Intel(R) BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-33894	intel - xeon_e-2314_firmware	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-33963	intel - unite	Incorrect default permissions in the software installer for Intel(R) Unite(R) Client software for Windows before version 4.2.34870 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-38103	intel - nuc_software_studi o_service	Insecure inherited permissions in the Intel(R) NUC Software Studio Service installer before version 1.17.38.0 may allow an authenticated user to potentially enable escalation of privilege via local access	2023-05-10	7.8	High
CVE-2022-40210	intel - data_center_manag er	Exposure of data element to wrong session in the Intel DCM software before version 5.0.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-40972	intel - quickassist_technol ogy	Improper access control in some Intel(R) QAT drivers for Windows before version 1.9.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-41658	intel - vtune_profiler	Insecure inherited permissions in the Intel(R) VTune(TM) Profiler software before version 2023.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-41699	intel - quickassist_technol ogy	Incorrect permission assignment for critical resource in some Intel(R) QAT drivers for Windows before version 1.9.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-41784	intel - one_boot_flash_up date	Improper access control in kernel mode driver for the Intel(R) OFU software before version 14.1.30 may allow an authenticated user to potentially enable escalation of privilege via local access	2023-05-10	7.8	High
CVE-2022-41982	intel - vtune_profiler	Uncontrolled search path element in the Intel(R) VTune(TM) Profiler software before version 2023.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-41998	intel - data_center_manag er	Uncontrolled search path in the Intel(R) DCM software before version 5.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-43475	intel - data_center_manag er	Insecure storage of sensitive information in the Intel(R) DCM software before version 5.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-44619	intel - data_center_manag er	Insecure storage of sensitive information in the Intel(R) DCM software before version 5.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2022-46656	intel - nuc_pro_software_s uite	Insecure inherited permissions for the Intel(R) NUC Pro Software Suite before version 2.0.0.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2023-22297	intel - server_system_d50t np1mhcrlc_firmwar e	Access of memory location after end of buffer in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2023-22312	intel - nuc_11_performanc e_kit_nuc11pahi70z _firmware	Improper access control for some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2023-22355	intel - multiple products	Uncontrolled search path in some Intel(R) oneAPI Toolkit and component software installers before version 4.3.0.251 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2023-22440	intel - setup_and_configur ation_software	Incorrect default permissions in the Intel(R) SCS Add-on software installer for Microsoft SCCM all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2023-22661	intel - server_system_d50t np1mhcrlc_firmwar e	Buffer overflow in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2023-23569	intel - multiple products	Stack-based buffer overflow for some Intel(R) Trace Analyzer and Collector software before version 2021.8.0 published Dec 2022 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2023-23580	intel - multiple products	Stack-based buffer overflow for some Intel(R) Trace Analyzer and Collector software before version 2021.8.0 published Dec 2022 may allow an authenticated user to potentially escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2023-23910	intel - multiple products	Out-of-bounds write for some Intel(R) Trace Analyzer and Collector software before version 2021.8.0 published Dec 2022 may allow	2023-05-10	7.8	High

		an authenticated user to potentially escalation of privilege via local access.			
CVE-2023-27382	intel - nuc_p14e_laptop_element	Incorrect default permissions in the Audio Service for some Intel(R) NUC P14E Laptop Element software for Windows 10 before version 1.0.0.156 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2023-28410	intel - i915_graphics	Improper restriction of operations within the bounds of a memory buffer in some Intel(R) i915 Graphics drivers for linux before kernel version 6.2.10 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.8	High
CVE-2023-29273	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (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.	2023-05-11	7.8	High
CVE-2023-29274	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (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.	2023-05-11	7.8	High
CVE-2023-29275	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (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.	2023-05-11	7.8	High
CVE-2023-29276	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (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.	2023-05-11	7.8	High
CVE-2023-29278	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-05-11	7.8	High
CVE-2023-29280	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (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.	2023-05-11	7.8	High
CVE-2023-29281	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (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.	2023-05-11	7.8	High
CVE-2023-29282	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (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.	2023-05-11	7.8	High
CVE-2023-29283	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (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.	2023-05-11	7.8	High
CVE-2023-29284	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (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.	2023-05-11	7.8	High
CVE-2023-29285	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (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.	2023-05-11	7.8	High
CVE-2023-30740	sap - multiple products	SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an authenticated attacker to access sensitive information which is otherwise restricted. On successful	2023-05-09	7.6	High

		exploitation, there could be a high impact on confidentiality, limited impact on integrity and availability of the application.			
CVE-2023-29104	siemens - 6gk1411-1ac00_firmware	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to overwrite any file the Linux user `ccuser` has write access to, or to download any file the Linux user `ccuser` has read-only access to.	2023-05-09	7.6	High
CVE-2023-22787	arubanetworks - multiple products	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point.	2023-05-08	7.5	High
CVE-2023-27963	apple - multiple products	The issue was addressed with additional permissions checks. This issue is fixed in iOS 15.7.4 and iPadOS 15.7.4, macOS Ventura 13.3, watchOS 9.4, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. A shortcut may be able to use sensitive data with certain actions without prompting the user	2023-05-08	7.5	High
CVE-2023-32111	sap - powerdesigner_proxy	In SAP PowerDesigner (Proxy) - version 16.7, an attacker can send a crafted request from a remote host to the proxy machine and crash the proxy server, due to faulty implementation of memory management causing a memory corruption. This leads to a high impact on availability of the application.	2023-05-09	7.5	High
CVE-2023-29105	siemens - 6gk1411-1ac00_firmware	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device is vulnerable to a denial of service while parsing a random (non-JSON) MQTT payload. This could allow an attacker who can manipulate the communication between the MQTT broker and the affected device to cause a denial of service (DoS).	2023-05-09	7.5	High
CVE-2023-29106	siemens - 6gk1411-1ac00_firmware	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint is accessible via REST API without authentication. This could allow an unauthenticated remote attacker to download the files available via the endpoint.	2023-05-09	7.5	High
CVE-2023-24898	microsoft - windows_server_2022	Windows SMB Denial of Service Vulnerability	2023-05-09	7.5	High
CVE-2023-24901	microsoft - multiple products	Windows NFS Portmapper Information Disclosure Vulnerability	2023-05-09	7.5	High
CVE-2023-24939	microsoft - multiple products	Server for NFS Denial of Service Vulnerability	2023-05-09	7.5	High
CVE-2023-24940	microsoft - multiple products	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability	2023-05-09	7.5	High
CVE-2023-24942	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-05-09	7.5	High
CVE-2023-29325	microsoft - multiple products	Windows OLE Remote Code Execution Vulnerability	2023-05-09	7.5	High
CVE-2023-29335	microsoft - multiple products	Microsoft Word Security Feature Bypass Vulnerability	2023-05-09	7.5	High
CVE-2023-28127	ivanti - avalanche	A path traversal vulnerability exists in Avalanche version 6.3.x and below that when exploited could result in possible information disclosure.	2023-05-09	7.5	High
CVE-2023-2156	linux - linux_kernel	A flaw was found in the networking subsystem of the Linux kernel within the handling of the RPL protocol. This issue results from the lack of proper handling of user-supplied data, which can lead to an assertion failure. This may allow an unauthenticated remote attacker to create a denial of service condition on the system.	2023-05-09	7.5	High
CVE-2023-24948	microsoft - multiple products	Windows Bluetooth Driver Elevation of Privilege Vulnerability	2023-05-09	7.4	High
CVE-2022-21162	intel - nuc_hdmi_firmware_update_tool	Uncontrolled search path for the Intel(R) HDMI Firmware Update tool for NUC before version 1.79.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.3	High
CVE-2023-27386	intel - pathfinder_for_risc-v	Uncontrolled search path in some Intel(R) Pathfinder for RISC-V software may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-05-10	7.3	High
CVE-2023-28762	sap - multiple products	SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an authenticated attacker with administrator privileges to get the login token of any logged-in BI user over the network without any user interaction. The attacker can impersonate any user on the platform resulting into accessing and modifying data. The attacker can also make the system partially or entirely unavailable.	2023-05-09	7.2	High

CVE-2023-28832	siemens - 6gk1411-1ac00_firmware	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The web based management of affected devices does not properly validate user input, making it susceptible to command injection. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	2023-05-09	7.2	High
CVE-2023-24955	microsoft - multiple products	Microsoft SharePoint Server Remote Code Execution Vulnerability	2023-05-09	7.2	High
CVE-2023-28128	ivanti - avalanche	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.3.x and below that could allow an attacker to achieve a remove code execution.	2023-05-09	7.2	High
CVE-2023-32568	veritas - multiple products	An issue was discovered in Veritas InfoScale Operations Manager (VIOM) before 7.4.2.800 and 8.x before 8.0.410. The VIOM web application does not validate user-supplied data and appends it to OS commands and internal binaries used by the application. An attacker with root/administrator level privileges can leverage this to read sensitive data stored on the servers, modify data or server configuration, and delete data or application configuration.	2023-05-10	7.2	High
CVE-2023-27968	apple - macos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory	2023-05-08	7.1	High
CVE-2023-24904	microsoft - multiple products	Windows Installer Elevation of Privilege Vulnerability	2023-05-09	7.1	High
CVE-2023-22442	intel - server_system_d50tnp1mhcrlc_firmware	Out of bounds write in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable escalation of privilege via local access.	2023-05-10	7.1	High
CVE-2023-24899	microsoft - multiple products	Windows Graphics Component Elevation of Privilege Vulnerability	2023-05-09	7	High
CVE-2023-27933	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. An app with root privileges may be able to execute arbitrary code with kernel privileges	2023-05-08	6.7	Medium
CVE-2023-2513	linux - linux_kernel	A use-after-free vulnerability was found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for extended attributes. This flaw could allow a privileged local user to cause a system crash or other undefined behaviors.	2023-05-08	6.7	Medium
CVE-2023-24932	microsoft - multiple products	Secure Boot Security Feature Bypass Vulnerability	2023-05-09	6.7	Medium
CVE-2022-42465	intel - one_boot_flash_update	Improper access control in kernel mode driver for the Intel(R) OFU software before version 14.1.30 may allow a privileged user to potentially enable escalation of privilege via local access.	2023-05-10	6.7	Medium
CVE-2023-25545	intel - server_system_d50tnp1mhcrlc_firmware	Improper buffer restrictions in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable escalation of privilege via local access.	2023-05-10	6.7	Medium
CVE-2023-1979	google - web_stories	The Web Stories for WordPress plugin supports the WordPress built-in functionality of protecting content with a password. The content is then only accessible to website visitors after entering the password. In WordPress, users with the "Author" role can create stories, but don't have the ability to edit password protected stories. The vulnerability allowed users with said role to bypass this permission check when trying to duplicate the protected story in the plugin's own dashboard, giving them access to the seemingly protected content. We recommend upgrading to version 1.32 or beyond commit ad49781c2a35c5c92ef704d4b621ab4e5cb77d68 https://github.com/GoogleForCreators/web-stories-wp/commit/ad49781c2a35c5c92ef704d4b621ab4e5cb77d68	2023-05-08	6.5	Medium
CVE-2023-23528	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in tvOS 16.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted Bluetooth packet may result in disclosure of process memory	2023-05-08	6.5	Medium
CVE-2023-27954	apple - multiple products	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, tvOS 16.4, watchOS 9.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information	2023-05-08	6.5	Medium
CVE-2023-28180	apple - macos	A denial-of-service issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. A user in a privileged network position may be able to cause a denial-of-service	2023-05-08	6.5	Medium
CVE-2023-28182	apple - multiple products	The issue was addressed with improved authentication. This issue is fixed in iOS 15.7.4 and iPadOS 15.7.4, macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to	2023-05-08	6.5	Medium

		spoof a VPN server that is configured with EAP-only authentication on a device			
CVE-2023-24944	microsoft - multiple products	Windows Bluetooth Driver Information Disclosure Vulnerability	2023-05-09	6.5	Medium
CVE-2023-24950	microsoft - multiple products	Microsoft SharePoint Server Spoofing Vulnerability	2023-05-09	6.5	Medium
CVE-2023-24954	microsoft - multiple products	Microsoft SharePoint Server Information Disclosure Vulnerability	2023-05-09	6.5	Medium
CVE-2023-29324	microsoft - multiple products	Windows MSHTML Platform Security Feature Bypass Vulnerability	2023-05-09	6.5	Medium
CVE-2022-40685	intel - data_center_manager	Insufficiently protected credentials in the Intel(R) DCM software before version 5.0.1 may allow an authenticated user to potentially enable information disclosure via network access.	2023-05-10	6.5	Medium
CVE-2023-27945	apple - xcode	This issue was addressed with improved entitlements. This issue is fixed in macOS Monterey 12.6.6, Xcode 14.3, macOS Big Sur 11.7.7. A sandboxed app may be able to collect system logs	2023-05-08	6.3	Medium
CVE-2023-27966	apple - macos	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3. An app may be able to break out of its sandbox	2023-05-08	6.3	Medium
CVE-2023-30741	sap - multiple products	Due to insufficient input validation, SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an unauthenticated attacker to redirect users to untrusted site using a malicious link. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	2023-05-09	6.1	Medium
CVE-2023-30742	sap - multiple products	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker.	2023-05-09	6.1	Medium
CVE-2023-30743	sap - multiple products	Due to improper neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This blocks user’s interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user’s information through phishing attack.	2023-05-09	6.1	Medium
CVE-2023-31406	sap - multiple products	Due to insufficient input validation, SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an unauthenticated attacker to redirect users to untrusted site using a malicious link. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	2023-05-09	6.1	Medium
CVE-2023-20098	cisco - multiple products	A vulnerability in the CLI of Cisco SDWAN vManage Software could allow an authenticated, local attacker to delete arbitrary files. This vulnerability is due to improper filtering of directory traversal character sequences within system commands. An attacker with administrative privileges could exploit this vulnerability by running a system command containing directory traversal character sequences to target an arbitrary file. A successful exploit could allow the attacker to delete arbitrary files from the system, including files owned by root.	2023-05-09	6	Medium
CVE-2023-28764	sap - multiple products	SAP BusinessObjects Platform - versions 420, 430, Information design tool transmits sensitive information as cleartext in the binaries over the network. This could allow an unauthenticated attacker with deep knowledge to gain sensitive information such as user credentials and domain names, which may have a low impact on confidentiality and no impact on the integrity and availability of the system.	2023-05-09	5.9	Medium
CVE-2023-24900	microsoft - multiple products	Windows NTLM Security Support Provider Information Disclosure Vulnerability	2023-05-09	5.9	Medium
CVE-2023-28125	ivanti - avalanche	An improper authentication vulnerability exists in Avalanche Premise versions 6.3.x and below that could allow an attacker to gain access to the server by registering to receive messages from the server and perform an authentication bypass.	2023-05-09	5.9	Medium
CVE-2023-28126	ivanti - avalanche	An authentication bypass vulnerability exists in Avalanche versions 6.3.x and below that could allow an attacker to gain access by exploiting the SetUser method or can exploit the Race Condition in the authentication message.	2023-05-09	5.9	Medium
CVE-2023-23527	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 16.4 and iPadOS 16.4, macOS Big Sur 11.7.5, watchOS 9.4, macOS Ventura 13.3, tvOS 16.4, macOS Monterey 12.6.4. A user may gain access to protected parts of the file system	2023-05-08	5.5	Medium

CVE-2023-23533	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.6.4, macOS Ventura 13.3. An app may be able to modify protected parts of the file system	2023-05-08	5.5	Medium
CVE-2023-23534	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7.5, macOS Ventura 13.3. Processing a maliciously crafted image may result in disclosure of process memory	2023-05-08	5.5	Medium
CVE-2023-23535	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.6, iOS 15.7.4 and iPadOS 15.7.4, tvOS 16.4, macOS Big Sur 11.7.5, watchOS 9.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory	2023-05-08	5.5	Medium
CVE-2023-23537	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.4 and iPadOS 16.4, macOS Big Sur 11.7.5, iOS 15.7.4 and iPadOS 15.7.4, watchOS 9.4, macOS Ventura 13.3. An app may be able to read sensitive location information	2023-05-08	5.5	Medium
CVE-2023-23538	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4. An app may be able to modify protected parts of the file system	2023-05-08	5.5	Medium
CVE-2023-23542	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Big Sur 11.7.5, macOS Monterey 12.6.4, macOS Ventura 13.3. An app may be able to access user-sensitive data	2023-05-08	5.5	Medium
CVE-2023-27929	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 9.4, iOS 16.4 and iPadOS 16.4, tvOS 16.4, macOS Ventura 13.3. Processing a maliciously crafted image may result in disclosure of process memory	2023-05-08	5.5	Medium
CVE-2023-27931	apple - multiple products	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.3, tvOS 16.4, watchOS 9.4, macOS Big Sur 11.7.3, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data	2023-05-08	5.5	Medium
CVE-2023-27932	apple - multiple products	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted web content may bypass Same Origin Policy	2023-05-08	5.5	Medium
CVE-2023-27941	apple - multiple products	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Big Sur 11.7.5, iOS 15.7.4 and iPadOS 15.7.4, macOS Ventura 13.3. An app may be able to disclose kernel memory	2023-05-08	5.5	Medium
CVE-2023-27942	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, macOS Big Sur 11.7.5, watchOS 9.4, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data	2023-05-08	5.5	Medium
CVE-2023-27943	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in iOS 16.4 and iPadOS 16.4, macOS Ventura 13.3. Files downloaded from the internet may not have the quarantine flag applied	2023-05-08	5.5	Medium
CVE-2023-27951	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7.5, macOS Monterey 12.6.4, macOS Ventura 13.3. An archive may be able to bypass Gatekeeper	2023-05-08	5.5	Medium
CVE-2023-27955	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4, macOS Ventura 13.3. An app may be able to read arbitrary files	2023-05-08	5.5	Medium
CVE-2023-27956	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.7.4 and iPadOS 15.7.4, macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory	2023-05-08	5.5	Medium
CVE-2023-27961	apple - multiple products	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5, watchOS 9.4, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information	2023-05-08	5.5	Medium
CVE-2023-27962	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7.5, macOS Monterey 12.6.4, macOS Ventura 13.3. An app may be able to modify protected parts of the file system	2023-05-08	5.5	Medium
CVE-2023-28178	apple - multiple products	A logic issue was addressed with improved validation. This issue is fixed in macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4, macOS Ventura 13.3. An app may be able to bypass Privacy preferences	2023-05-08	5.5	Medium
CVE-2023-28189	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7.5, macOS Ventura 13.3. An app may be able to view sensitive information	2023-05-08	5.5	Medium
CVE-2023-28190	apple - macos	A privacy issue was addressed by moving sensitive data to a more secure location. This issue is fixed in macOS Ventura 13.3. An app may be able to access user-sensitive data	2023-05-08	5.5	Medium

CVE-2023-28192	apple - multiple products	A permissions issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.7.5, macOS Monterey 12.6.4, macOS Ventura 13.3. An app may be able to read sensitive location information	2023-05-08	5.5	Medium
CVE-2023-28200	apple - multiple products	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Ventura 13.3. An app may be able to disclose kernel memory	2023-05-08	5.5	Medium
CVE-2022-38685	google - multiple products	In bluetooth service, there is a possible missing permission check. This could lead to local denial of service in bluetooth service with no additional execution privileges needed.	2023-05-09	5.5	Medium
CVE-2022-44419	google - multiple products	In modem, there is a possible missing verification of NAS Security Mode Command Replay Attacks in LTE. This could local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-44420	google - multiple products	In modem, there is a possible missing verification of HashMME value in Security Mode Command. This could local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-47340	google - multiple products	In h265 codec firmware, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-47487	google - multiple products	In thermal service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-47490	google - multiple products	In soter service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-47492	google - multiple products	In soter service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-47493	google - multiple products	In soter service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-48231	google - multiple products	In soter service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-48232	google - multiple products	In FM service , there is a possible missing params check. This could lead to local denial of service in FM service .	2023-05-09	5.5	Medium
CVE-2022-48233	google - multiple products	In FM service , there is a possible missing params check. This could lead to local denial of service in FM service .	2023-05-09	5.5	Medium
CVE-2022-48234	google - multiple products	In FM service , there is a possible missing params check. This could lead to local denial of service in FM service .	2023-05-09	5.5	Medium
CVE-2022-48241	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-48242	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-48370	google - multiple products	In dialer service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-48371	google - multiple products	In dialer service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-48375	google - multiple products	In contacts service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-48376	google - multiple products	In dialer service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-48377	google - multiple products	In dialer service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-48378	google - multiple products	In engineermode service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2022-48379	google - multiple products	In dialer service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-05-09	5.5	Medium
CVE-2023-32112	sap - multiple products	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system.	2023-05-09	5.5	Medium
CVE-2023-30985	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < VX.223.0 Update 3), Solid Edge SE2023 (All versions < VX.223.0 Update 2). Affected applications contain an out of bounds read past the end of an allocated buffer while parsing a	2023-05-09	5.5	Medium

		specially crafted OBJ file. This vulnerability could allow an attacker to disclose sensitive information. (ZDI-CAN-19426)			
CVE-2023-24945	microsoft - multiple products	Windows iSCSI Target Service Information Disclosure Vulnerability	2023-05-09	5.5	Medium
CVE-2023-28251	microsoft - multiple products	Windows Driver Revocation List Security Feature Bypass Vulnerability	2023-05-09	5.5	Medium
CVE-2022-21239	intel - quickassist_technology	Out-of-bounds read in software for the Intel QAT Driver for Windows before version 1.9.0-0008 may allow an authenticated user to potentially enable information disclosure via local access.	2023-05-10	5.5	Medium
CVE-2022-25976	intel - virtual_raid_on_cpu	Improper input validation in the Intel(R) VROC software before version 7.7.6.1003 may allow an authenticated user to potentially enable denial of service via local access.	2023-05-10	5.5	Medium
CVE-2022-37409	intel - integrated_performance_primitives_cryptography	Insufficient control flow management for the Intel(R) IPP Cryptography software before version 2021.6 may allow an authenticated user to potentially enable information disclosure via local access.	2023-05-10	5.5	Medium
CVE-2022-38087	intel - xeon_e-2314_firmware	Exposure of resource to wrong sphere in BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	2023-05-10	5.5	Medium
CVE-2022-40974	intel - integrated_performance_primitives_cryptography	Incomplete cleanup in the Intel(R) IPP Cryptography software before version 2021.6 may allow a privileged user to potentially enable information disclosure via local access.	2023-05-10	5.5	Medium
CVE-2022-41621	intel - quickassist_technology	Improper access control in some Intel(R) QAT drivers for Windows before version 1.9.0 may allow an authenticated user to potentially enable information disclosure via local access.	2023-05-10	5.5	Medium
CVE-2022-41771	intel - quickassist_technology	Incorrect permission assignment for critical resource in some Intel(R) QAT drivers for Windows before version 1.9.0 may allow an authenticated user to potentially enable information disclosure via local access.	2023-05-10	5.5	Medium
CVE-2022-41808	intel - quickassist_technology	Improper buffer restriction in software for the Intel QAT Driver for Linux before version 1.7.l.4.12 may allow an authenticated user to potentially enable denial of service via local access.	2023-05-10	5.5	Medium
CVE-2022-42878	intel - multiple products	Null pointer dereference for some Intel(R) Trace Analyzer and Collector software before version 2021.8.0 published Dec 2022 may allow an authenticated user to potentially enable information disclosure via local access.	2023-05-10	5.5	Medium
CVE-2022-43465	intel - setup_and_configuration_software	Improper authorization in the Intel(R) SCS software all versions may allow an authenticated user to potentially enable denial of service via local access.	2023-05-10	5.5	Medium
CVE-2022-45128	intel - endpoint_management_assistant	Improper authorization in the Intel(R) EMA software before version 1.9.0.0 may allow an authenticated user to potentially enable denial of service via local access.	2023-05-10	5.5	Medium
CVE-2023-22379	intel - server_system_d50tnp1mhcrlc_firmware	Improper input validation in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable information disclosure via local access.	2023-05-10	5.5	Medium
CVE-2023-22443	intel - server_system_d50tnp1mhcrlc_firmware	Integer overflow in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable denial of service via local access.	2023-05-10	5.5	Medium
CVE-2023-23909	intel - multiple products	Out-of-bounds read for some Intel(R) Trace Analyzer and Collector software before version 2021.8.0 published Dec 2022 may allow an authenticated user to potentially enable information disclosure via local access.	2023-05-10	5.5	Medium
CVE-2023-25175	intel - server_system_d50tnp1mhcrlc_firmware	Improper input validation in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable information disclosure via local access.	2023-05-10	5.5	Medium
CVE-2023-25179	intel - unite	Uncontrolled resource consumption in the Intel(R) Unite(R) android application before Release 17 may allow an authenticated user to potentially enable denial of service via local access.	2023-05-10	5.5	Medium
CVE-2023-25771	intel - nuc_8_compute_element_cm8i3cb4n_firmware	Improper access control for some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable denial of service via local access.	2023-05-10	5.5	Medium
CVE-2023-25772	intel - multiple products	Improper input validation in the Intel(R) Retail Edge Mobile Android application before version 3.0.301126-RELEASE may allow an authenticated user to potentially enable denial of service via local access.	2023-05-10	5.5	Medium
CVE-2023-28411	intel - server_system_d50tnp1mhcrlc_firmware	Double free in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable information disclosure via local access.	2023-05-10	5.5	Medium
CVE-2023-29277	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (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	2023-05-11	5.5	Medium

		this issue requires user interaction in that a victim must open a malicious file.			
CVE-2023-29279	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (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.	2023-05-11	5.5	Medium
CVE-2023-29286	adobe - substance_3d_painter	Adobe Substance 3D Painter versions 8.3.0 (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.	2023-05-11	5.5	Medium
CVE-2023-29247	apache - airflow	Task instance details page in the UI is vulnerable to a stored XSS.This issue affects Apache Airflow: before 2.6.0.	2023-05-08	5.4	Medium
CVE-2023-29188	sap - multiple products	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data.	2023-05-09	5.4	Medium
CVE-2023-31407	sap - multiple products	SAP Business Planning and Consolidation - versions 740, 750, allows an authorized attacker to upload a malicious file, resulting in Cross-Site Scripting vulnerability. After successful exploitation, an attacker can cause limited impact on confidentiality and integrity of the application.	2023-05-09	5.4	Medium
CVE-2023-28520	ibm - planning_analytics_local	IBM Planning Analytics Local 2.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 250454.	2023-05-12	5.4	Medium
CVE-2023-23494	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to cause a denial-of-service	2023-05-08	5.3	Medium
CVE-2023-29107	siemens - 6gk1411-1ac00_firmware	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint discloses some undocumented files. This could allow an unauthenticated remote attacker to gain access to additional information resources.	2023-05-09	5.3	Medium
CVE-2023-28290	microsoft - remote_desktop	Microsoft Remote Desktop app for Windows Information Disclosure Vulnerability	2023-05-09	5.3	Medium
CVE-2023-31404	sap - multiple products	Under certain conditions, SAP BusinessObjects Business Intelligence Platform (Central Management Service) - versions 420, 430, allows an attacker to access information which would otherwise be restricted. Some users with specific privileges could have access to credentials of other users. It could let them access data sources which would otherwise be restricted.	2023-05-09	5	Medium
CVE-2023-29338	microsoft - visual_studio_code	Visual Studio Code Information Disclosure Vulnerability	2023-05-09	5	Medium
CVE-2023-27863	ibm - spectrum_protect	IBM Spectrum Protect Plus Server 10.1.13, under specific configurations, could allow an elevated user to obtain SMB credentials that may be used to access vSnap data stores. IBM X-Force ID: 249325.	2023-05-12	4.9	Medium
CVE-2023-22791	arubanetworks - multiple products	A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge-case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive information can occur are complex and depend on factors that are beyond the control of the attacker.	2023-05-08	4.8	Medium
CVE-2023-0007	paloaltonetworks - multiple products	A cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS software on Panorama appliances enables an authenticated read-write administrator to store a JavaScript payload in the web interface that will execute in the context of another administrator's browser when viewed.	2023-05-10	4.8	Medium
CVE-2023-27952	apple - macos	A race condition was addressed with improved locking. This issue is fixed in macOS Ventura 13.3. An app may bypass Gatekeeper checks	2023-05-08	4.7	Medium
CVE-2022-39089	google - multiple products	In mlog service, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium

CVE-2022-47334	google - multiple products	In phasecheck server, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-47469	google - multiple products	In ext4fsfilter driver, there is a possible out of bounds read due to a missing bounds check. This could local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-47470	google - multiple products	In ext4fsfilter driver, there is a possible out of bounds read due to a missing bounds check. This could local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-47485	google - multiple products	In modem control device, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-47486	google - multiple products	In ext4fsfilter driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-47488	google - multiple products	In spipe drive, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-47489	google - multiple products	In soter service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-47491	google - multiple products	In soter service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-47494	google - multiple products	In soter service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-47495	google - multiple products	In soter service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-47496	google - multiple products	In soter service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-47497	google - multiple products	In soter service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-47498	google - multiple products	In soter service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-47499	google - multiple products	In soter service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48235	google - multiple products	In MP3 encoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48236	google - multiple products	In MP3 encoder, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48237	google - multiple products	In Image filter, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48238	google - multiple products	In Image filter, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48239	google - multiple products	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48240	google - multiple products	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48372	google - multiple products	In bootcp service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48373	google - multiple products	In tee service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48374	google - multiple products	In tee service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48380	google - android	In modem control device, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48381	google - android	In modem control device, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48382	google - multiple products	In log service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium

CVE-2022-48385	google - multiple products	In cp_dump driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48386	google - multiple products	the apipe driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48387	google - multiple products	the apipe driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-48389	google - android	In modem control device, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-05-09	4.4	Medium
CVE-2022-32582	intel - nuc_11_performance_kit_nuc11pahi70z_firmware	Improper access control in firmware for some Intel(R) NUC Boards, Intel(R) NUC 11 Performance Kit, Intel(R) NUC 11 Performance Mini PC, Intel(R) NUC Pro Compute Element may allow a privileged user to potentially enable denial of service via local access.	2023-05-10	4.4	Medium
CVE-2023-22447	intel - open_cache_acceleration_software	Insertion of sensitive information into log file in the Open CAS software for Linux maintained by Intel before version 22.6.2 may allow a privileged user to potentially enable information disclosure via local access.	2023-05-10	4.4	Medium
CVE-2023-23573	intel - unite	Improper access control in the Intel(R) Unite(R) android application before Release 17 may allow a privileged user to potentially enable information disclosure via local access.	2023-05-10	4.4	Medium
CVE-2023-24475	intel - server_system_d50tnp1mhcrlc_firmware	Out of bounds read in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable information disclosure via local access.	2023-05-10	4.4	Medium
CVE-2023-25776	intel - server_system_d50tnp1mhcrlc_firmware	Improper input validation in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable information disclosure via local access.	2023-05-10	4.4	Medium
CVE-2023-0008	paloaltonetworks - multiple products	A file disclosure vulnerability in Palo Alto Networks PAN-OS software enables an authenticated read-write administrator with access to the web interface to export local files from the firewall through a race condition.	2023-05-10	4.4	Medium
CVE-2023-29103	siemens - 6gk1411-1ac00_firmware	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device uses a hard-coded password to protect the diagnostic files. This could allow an authenticated attacker to access protected data.	2023-05-09	4.3	Medium
CVE-2023-23543	apple - multiple products	The issue was addressed with additional restrictions on the observability of app states. This issue is fixed in iOS 15.7.4 and iPadOS 15.7.4, macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. A sandboxed app may be able to determine which app is currently using the camera	2023-05-08	3.6	Low
CVE-2023-23523	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Photos belonging to the Hidden Photos Album could be viewed without authentication through Visual Lookup	2023-05-08	3.3	Low
CVE-2023-23541	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to access information about a user's contacts	2023-05-08	3.3	Low
CVE-2023-27928	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, tvOS 16.4, macOS Big Sur 11.7.5, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to access information about a user's contacts	2023-05-08	3.3	Low
CVE-2023-28194	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to unexpectedly create a bookmark on the Home Screen	2023-05-08	3.3	Low
CVE-2023-27408	siemens - scalance_lpe9403_firmware	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). The `i2c` mutex file is created with the permissions bits of `-rw-rw-rw-`. This file is used as a mutex for multiple applications interacting with i2c. This could allow an authenticated attacker with access to the SSH interface on the affected device to interfere with the integrity of the mutex and the data it protects.	2023-05-09	3.3	Low
CVE-2023-27409	siemens - scalance_lpe9403_firmware	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). A path traversal vulnerability was found in the `deviceinfo` binary via the `mac` parameter. This could allow an authenticated attacker with access to the SSH interface on the affected device to read the contents of any file named `address`.	2023-05-09	3.3	Low
CVE-2023-29333	microsoft - multiple products	Microsoft Access Denial of Service Vulnerability	2023-05-09	3.3	Low

CVE-2023-27410	siemens - scalance_lpe9403_firmware	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). A heap-based buffer overflow vulnerability was found in the `edgebox_web_app` binary. The binary will crash if supplied with a backup password longer than 255 characters. This could allow an authenticated privileged attacker to cause a denial of service.	2023-05-09	2.7	Low
CVE-2023-29128	siemens - 6gk1411-1ac00_firmware	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to write any file with the extension `.db`.	2023-05-09	2.7	Low

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

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