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 ٦ أغسطس إلى ١٢ أغسطس. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **عالي جدًا: النتيجة الأساسية لـ CVSS 9.0-10.0**
- **عالي: النتيجة الأساسية لـ CVSS 7.0-8.9**
- **متوسط: النتيجة الأساسية لـ CVSS 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 6th of August to 12th of August. 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-2023-38928	netgear - r7100lg_firmware	Netgear R7100LG 1.0.0.78 was discovered to contain a command injection vulnerability via the password parameter at usb_remote_invite.cgi.	2023-08-07	9.8	Critical
CVE-2023-37483	sap - powerdesigner	SAP PowerDesigner - version 16.7, has improper access control which might allow an unauthenticated attacker to run arbitrary queries against the back-end database via Proxy.	2023-08-08	9.8	Critical
CVE-2023-39439	sap - multiple products	SAP Commerce Cloud may accept an empty passphrase for user ID and passphrase authentication, allowing users to log into the system without a passphrase.	2023-08-08	9.8	Critical
CVE-2022-40510	qualcomm - apq8009_firmware	Memory corruption due to buffer copy without checking size of input in Audio while voice call with EVS vocoder.	2023-08-08	9.8	Critical
CVE-2023-24845	siemens - ruggedcom_ros	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC, RUGGEDCOM i802, RUGGEDCOM i802NC, RUGGEDCOM i803, RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM M2100F, RUGGEDCOM M2100NC, RUGGEDCOM M2200, RUGGEDCOM M2200F, RUGGEDCOM M2200NC, RUGGEDCOM M969, RUGGEDCOM M969F, RUGGEDCOM M969NC, RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC, RUGGEDCOM RS400, RUGGEDCOM RS400F, RUGGEDCOM RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC, RUGGEDCOM RS416, RUGGEDCOM RS416F, RUGGEDCOM RS416NC, RUGGEDCOM RS416NC v2, RUGGEDCOM RS416P, RUGGEDCOM RS416PF, RUGGEDCOM RS416PNC, RUGGEDCOM RS416PNC v2, RUGGEDCOM RS416Pv2, RUGGEDCOM RS416v2, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC, RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900F, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GF, RUGGEDCOM RS900GNC, RUGGEDCOM RS900GNC(32M) V4.X, RUGGEDCOM RS900GNC(32M) V5.X, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPF, RUGGEDCOM RS900GPNC, RUGGEDCOM RS900L, RUGGEDCOM RS900L, RUGGEDCOM RS900LNC, RUGGEDCOM RS900LNC, RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-GETS-XX, RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM RS900MNC-STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM RS900NC, RUGGEDCOM RS900NC(32M) V4.X, RUGGEDCOM RS900NC(32M) V5.X, RUGGEDCOM RS900W, RUGGEDCOM RS910,	2023-08-08	9.8	Critical

		RUGGEDCOM RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GF, RUGGEDCOM RS940GNC, RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100F, RUGGEDCOM RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PF, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200F, RUGGEDCOM RSG2200NC, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300F, RUGGEDCOM RSG2300NC V4.X, RUGGEDCOM RSG2300NC V5.X, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PF, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488F, RUGGEDCOM RSG2488NC V4.X, RUGGEDCOM RSG2488NC V5.X, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM RSL910, RUGGEDCOM RSL910NC, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. The affected products insufficiently block data from being forwarded over the mirror port into the mirrored network. An attacker could use this behavior to transmit malicious packets to systems in the mirrored network, possibly influencing their configuration and runtime behavior.			
CVE-2023-28561	qualcomm - qcn7606_firmware	Memory corruption in QESL while processing payload from external ESL device to firmware.	2023-08-08	9.8	Critical
CVE-2023-37372	siemens - ruggedcom_crossbow	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.4). The affected applications is vulnerable to SQL injection. This could allow an unauthenticated remote attackers to execute arbitrary SQL queries on the server database.	2023-08-08	9.8	Critical
CVE-2023-21709	microsoft - multiple products	Microsoft Exchange Server Elevation of Privilege Vulnerability	2023-08-08	9.8	Critical
CVE-2023-35385	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-08-08	9.8	Critical
CVE-2023-36534	zoom - zoom	Path traversal in Zoom Desktop Client for Windows before 5.14.7 may allow an unauthenticated user to enable an escalation of privilege via network access.	2023-08-08	9.8	Critical
CVE-2023-36903	microsoft - multiple products	Windows System Assessment Tool Elevation of Privilege Vulnerability	2023-08-08	9.8	Critical
CVE-2023-36910	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-08-08	9.8	Critical
CVE-2023-36911	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-08-08	9.8	Critical
CVE-2023-38186	microsoft - multiple products	Windows Mobile Device Management Elevation of Privilege Vulnerability	2023-08-08	9.8	Critical
CVE-2023-39216	zoom - zoom	Improper input validation in Zoom Desktop Client for Windows before 5.14.7 may allow an unauthenticated user to enable an escalation of privilege via network access.	2023-08-08	9.8	Critical
CVE-2023-39213	zoom - multiple products	Improper neutralization of special elements in Zoom Desktop Client for Windows and Zoom VDI Client before 5.15.2 may allow an unauthenticated user to enable an escalation of privilege via network access.	2023-08-08	9.8	Critical
CVE-2023-30699	samsung - multiple products	Out-of-bounds write vulnerability in parser_hvcC function of libsimba library prior to SMR Aug-2023 Release 1 allows code execution by remote attackers.	2023-08-10	9.8	Critical
CVE-2023-32567	ivanti - avalanche	Ivanti Avalanche decodeToMap XML External Entity Processing. Fixed in version 6.4.1.	2023-08-10	9.8	Critical
CVE-2023-32560	ivanti - avalanche	An attacker can send a specially crafted message to the Wavelink Avalanche Manager, which could result in service disruption or arbitrary code execution. Thanks to a Researcher at Tenable for finding and reporting. Fixed in version 6.4.1.	2023-08-10	9.8	Critical
CVE-2023-32562	ivanti - avalanche	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.3.x and below that could allow an	2023-08-10	9.8	Critical

		attacker to achieve a remove code execution. Fixed in version 6.4.1.			
CVE-2023-32563	ivanti - avalanche	An unauthenticated attacker could achieve the code execution through a RemoteControl server.	2023-08-10	9.8	Critical
CVE-2023-32564	ivanti - avalanche	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.4.1 and below that could allow an attacker to achieve a remove code execution.	2023-08-10	9.8	Critical
CVE-2023-25775	intel - ethernet_controller_rdma_driver_for_linux	Improper access control in the Intel(R) Ethernet Controller RDMA driver for linux before version 1.9.30 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	2023-08-11	9.8	Critical
CVE-2023-40256	veritas - multiple products	A vulnerability was discovered in Veritas NetBackup Snapshot Manager before 10.2.0.1 that allowed untrusted clients to interact with the RabbitMQ service. This was caused by improper validation of the client certificate due to misconfiguration of the RabbitMQ service. Exploiting this impacts the confidentiality and integrity of messages controlling the backup and restore jobs, and could result in the service becoming unavailable. This impacts only the jobs controlling the backup and restore activities, and does not allow access to (or deletion of) the backup snapshot data itself. This vulnerability is confined to the NetBackup Snapshot Manager feature and does not impact the RabbitMQ instance on the NetBackup primary servers.	2023-08-11	9.8	Critical
CVE-2022-29887	intel - manageability_commander	Cross-site Scripting (XSS) in some Intel(R) Manageability Commander software before version 2.3 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	2023-08-11	9.6	Critical
CVE-2023-27515	intel - driver_\&_support_assistant	Cross-site scripting (XSS) for the Intel(R) DSA software before version 23.1.9 may allow unauthenticated user to potentially enable escalation of privilege via network access.	2023-08-11	9.6	Critical
CVE-2023-33934	apache - multiple products	Improper Input Validation vulnerability in Apache Software Foundation Apache Traffic Server.This issue affects Apache Traffic Server: through 9.2.1.	2023-08-09	9.1	Critical
CVE-2023-32566	ivanti - avalanche	An attacker can send a specially crafted request which could lead to leakage of sensitive data or potentially a resource-based DoS attack. Fixed in version 6.4.1.	2023-08-10	9.1	Critical
CVE-2023-32565	ivanti - avalanche	An attacker can send a specially crafted request which could lead to leakage of sensitive data or potentially a resource-based DoS attack. Fixed in version 6.4.1.	2023-08-10	9.1	Critical
CVE-2023-37490	sap - multiple products	SAP Business Objects Installer - versions 420, 430, allows an authenticated attacker within the network to overwrite an executable file created in a temporary directory during the installation process. On replacing this executable with a malicious file, an attacker can completely compromise the confidentiality, integrity, and availability of the system	2023-08-08	9	Critical
CVE-2023-36499	netgear - xr300_firmware	Netgear XR300 v1.0.3.78 was discovered to contain multiple buffer overflows via the wla_ssid and wlg_ssid parameters at genie_ap_wifi_change.cgi.	2023-08-07	8.8	High
CVE-2023-38412	netgear - r6900p_firmware	Netgear R6900P v1.3.3.154 was discovered to contain multiple buffer overflows via the wla_ssid and wlg_ssid parameters at ia_ap_setting.cgi.	2023-08-07	8.8	High
CVE-2023-38591	netgear - dg834gv5_firmware	Netgear DG834Gv5 1.6.01.34 was discovered to contain multiple buffer overflows via the wla_ssid and wla_temp_ssid parameters at bsw_ssid.cgi.	2023-08-07	8.8	High
CVE-2023-38921	netgear - wg302v2_firmware	Netgear WG302v2 v5.2.9 and WAG302v2 v5.1.19 were discovered to contain multiple command injection vulnerabilities in the upgrade_handler function via the firmwareRestore and firmwareServerip parameters.	2023-08-07	8.8	High
CVE-2023-38922	netgear - jwnr2000v2_firmware	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the update_auth function.	2023-08-07	8.8	High
CVE-2023-38925	netgear - dc112a_firmware	Netgear DC112A 1.0.0.64, EX6200 1.0.3.94 and R6300v2 1.0.4.8 were discovered to contain a buffer overflow via the http_passwd parameter in password.cgi.	2023-08-07	8.8	High
CVE-2023-38926	netgear - ex6200_firmware	Netgear EX6200 v1.0.3.94 was discovered to contain a buffer overflow via the wla_temp_ssid parameter at acosNvramConfig_set.	2023-08-07	8.8	High
CVE-2023-39550	netgear - jwnr2000v2_firmware	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the check_auth function.	2023-08-07	8.8	High
CVE-2023-37491	sap - multiple products	The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EXT, can be bypassed in certain conditions, which may enable an authenticated malicious user to enter the network of the SAP systems served by the attacked SAP Message server.	2023-08-08	8.8	High

		This may lead to unauthorized read and write of data as well as rendering the system unavailable.			
CVE-2023-27411	siemens - ruggedcom_crossbow	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.4). The affected applications is vulnerable to SQL injection. This could allow an authenticated remote attackers to execute arbitrary SQL queries on the server database and escalate privileges.	2023-08-08	8.8	High
CVE-2023-29328	microsoft - multiple products	Microsoft Teams Remote Code Execution Vulnerability	2023-08-08	8.8	High
CVE-2023-29330	microsoft - multiple products	Microsoft Teams Remote Code Execution Vulnerability	2023-08-08	8.8	High
CVE-2023-35368	microsoft - multiple products	Microsoft Exchange Remote Code Execution Vulnerability	2023-08-08	8.8	High
CVE-2023-35381	microsoft - multiple products	Windows Fax Service Remote Code Execution Vulnerability	2023-08-08	8.8	High
CVE-2023-35387	microsoft - multiple products	Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability	2023-08-08	8.8	High
CVE-2023-36541	zoom - zoom	Insufficient verification of data authenticity in Zoom Desktop Client for Windows before 5.14.5 may allow an authenticated user to enable an escalation of privilege via network access.	2023-08-08	8.8	High
CVE-2023-36882	microsoft - multiple products	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2023-08-08	8.8	High
CVE-2023-38169	microsoft - multiple products	Microsoft OLE DB Remote Code Execution Vulnerability	2023-08-08	8.8	High
CVE-2023-38181	microsoft - multiple products	Microsoft Exchange Server Spoofing Vulnerability	2023-08-08	8.8	High
CVE-2023-38185	microsoft - multiple products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-08-08	8.8	High
CVE-2023-36899	microsoft - .net_framework	ASP.NET Elevation of Privilege Vulnerability	2023-08-08	8.8	High
CVE-2023-28380	intel - ai_hackathon	Uncontrolled search path for the Intel(R) AI Hackathon software before version 2.0.0 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	2023-08-11	8.8	High
CVE-2023-39214	zoom - multiple products	Exposure of sensitive information in Zoom Client SDK's before 5.15.5 may allow an authenticated user to enable a denial of service via network access.	2023-08-08	8.1	High
CVE-2023-35388	microsoft - multiple products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-08-08	8	High
CVE-2023-36891	microsoft - multiple products	Microsoft SharePoint Server Spoofing Vulnerability	2023-08-08	8	High
CVE-2023-36892	microsoft - multiple products	Microsoft SharePoint Server Spoofing Vulnerability	2023-08-08	8	High
CVE-2023-38182	microsoft - multiple products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-08-08	8	High
CVE-2022-44611	intel - celeron_j6413_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 adjacent access.	2023-08-11	8	High
CVE-2023-4147	linux - multiple products	A use-after-free flaw was found in the Linux kernel's Netfilter functionality when adding a rule with NFTA_RULE_CHAIN_ID. This flaw allows a local user to crash or escalate their privileges on the system.	2023-08-07	7.8	High
CVE-2023-36923	sap - powerdesigner	SAP SQLA for PowerDesigner 17 bundled with SAP PowerDesigner 16.7 SP06 PL03, allows an attacker with local access to the system, to place a malicious library, that can be executed by the application. An attacker could thereby control the behavior of the application.	2023-08-08	7.8	High
CVE-2021-41544	siemens - software_center	A vulnerability has been identified in Siemens Software Center (All versions < V3.0). A DLL Hijacking vulnerability could allow a local attacker to execute code with elevated privileges by placing a malicious DLL in one of the directories on the DLL search path.	2023-08-08	7.8	High
CVE-2022-39062	siemens - sicam_toolbox_ii	A vulnerability has been identified in SICAM TOOLBOX II (All versions < V07.10). Affected applications do not properly set permissions for product folders. This could allow an authenticated attacker with low privileges to replace DLLs and conduct a privilege escalation.	2023-08-08	7.8	High
CVE-2023-21627	qualcomm - aqt1000_firmware	Memory corruption in Trusted Execution Environment while calling service API with invalid address.	2023-08-08	7.8	High
CVE-2023-21643	qualcomm - apq8064au_firmware	Memory corruption due to untrusted pointer dereference in automotive during system call.	2023-08-08	7.8	High
CVE-2023-21648	qualcomm - aqt1000_firmware	Memory corruption in RIL while trying to send apdu packet.	2023-08-08	7.8	High
CVE-2023-21649	qualcomm - apq8096au_firmware	Memory corruption in WLAN while running doDriverCmd for an unspecific command.	2023-08-08	7.8	High
CVE-2023-21650	qualcomm - aqt1000_firmware	Memory Corruption in GPS HLOS Driver when injectFdclData receives data with invalid data length.	2023-08-08	7.8	High

CVE-2023-21651	qualcomm - aqt1000_firmware	Memory Corruption in Core due to incorrect type conversion or cast in secure_io_read/write function in TEE.	2023-08-08	7.8	High
CVE-2023-22666	qualcomm - apq8009_firmware	Memory Corruption in Audio while playing amrwbplus clips with modified content.	2023-08-08	7.8	High
CVE-2023-28537	qualcomm - 315_5g_iot_modem_firmware	Memory corruption while allocating memory in COmxApeDec module in Audio.	2023-08-08	7.8	High
CVE-2023-28575	qualcomm - aqt1000_firmware	The cam_get_device_priv function does not check the type of handle being returned (device/session/link). This would lead to invalid type usage if a wrong handle is passed to it.	2023-08-08	7.8	High
CVE-2023-28577	qualcomm - fastconnect_6800_firmware	In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function called cam_mem_get_cpu_buf to get the kernel va to use, another thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the kernel va which cause UAF of the kernel address.	2023-08-08	7.8	High
CVE-2023-28830	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13), Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter Visualization V14.1 (All versions < V14.1.0.11), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker could leverage this vulnerability to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-30795	siemens - multiple products	A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4), Parasolid V34.0 (All versions < V34.0.253), Parasolid V34.1 (All versions < V34.1.243), Parasolid V35.0 (All versions < V35.0.177), Parasolid V35.1 (All versions < V35.1.073). 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.	2023-08-08	7.8	High
CVE-2023-30796	siemens - multiple products	A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4). 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.	2023-08-08	7.8	High
CVE-2023-38524	siemens - multiple products	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain null pointer dereference while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-38525	siemens - multiple products	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-38526	siemens - multiple products	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-38527	siemens - multiple products	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-38528	siemens - multiple products	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.197), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected	2023-08-08	7.8	High

		application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted X_T file. This could allow an attacker to execute code in the context of the current process.			
CVE-2023-38529	siemens - multiple products	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-38530	siemens - multiple products	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-38531	siemens - multiple products	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-38641	siemens - sicam_toolbox_ii	A vulnerability has been identified in SICAM TOOLBOX II (All versions < V07.10). The affected application's database service is executed as `NT AUTHORITY\SYSTEM`. This could allow a local attacker to execute operating system commands with elevated privileges.	2023-08-08	7.8	High
CVE-2023-38679	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21106)	2023-08-08	7.8	High
CVE-2023-38680	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21132)	2023-08-08	7.8	High
CVE-2023-38681	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted IGS file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21270)	2023-08-08	7.8	High
CVE-2023-38682	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Teamcenter Visualization V13.2 (All versions < V13.2.0.14), Teamcenter Visualization V14.1 (All versions < V14.1.0.10), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted TIFF files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-38683	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Teamcenter Visualization V13.2 (All versions < V13.2.0.14), Teamcenter Visualization V14.1 (All versions < V14.1.0.10), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted TIFF file. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-39181	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High

CVE-2023-39182	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-39183	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PSM files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-39184	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PSM files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-39185	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-39186	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-39187	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-39188	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-39419	siemens - solid_edge	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an out of bounds write past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
CVE-2023-39549	siemens - solid_edge	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 2). The affected application contains a use-after-free vulnerability that could be triggered while parsing specially crafted DWG file. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19562)	2023-08-08	7.8	High
CVE-2023-35359	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-08-08	7.8	High
CVE-2023-35371	microsoft - multiple products	Microsoft Office Remote Code Execution Vulnerability	2023-08-08	7.8	High
CVE-2023-35372	microsoft - multiple products	Microsoft Office Visio Remote Code Execution Vulnerability	2023-08-08	7.8	High
CVE-2023-35379	microsoft - windows_server_2008	Reliability Analysis Metrics Calculation Engine (RACEng) Elevation of Privilege Vulnerability	2023-08-08	7.8	High
CVE-2023-35380	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-08-08	7.8	High
CVE-2023-35382	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-08-08	7.8	High
CVE-2023-35386	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-08-08	7.8	High
CVE-2023-35390	microsoft - multiple products	.NET and Visual Studio Remote Code Execution Vulnerability	2023-08-08	7.8	High
CVE-2023-36540	zoom - zoom	Untrusted search path in the installer for Zoom Desktop Client for Windows before 5.14.5 may allow an authenticated user to enable an escalation of privilege via local access.	2023-08-08	7.8	High
CVE-2023-36865	microsoft - multiple products	Microsoft Office Visio Remote Code Execution Vulnerability	2023-08-08	7.8	High
CVE-2023-36866	microsoft - multiple products	Microsoft Office Visio Remote Code Execution Vulnerability	2023-08-08	7.8	High
CVE-2023-36895	microsoft - multiple products	Microsoft Outlook Remote Code Execution Vulnerability	2023-08-08	7.8	High
CVE-2023-36896	microsoft - multiple products	Microsoft Excel Remote Code Execution Vulnerability	2023-08-08	7.8	High
CVE-2023-36898	microsoft - multiple products	Tablet Windows User Interface Application Core Remote Code Execution Vulnerability	2023-08-08	7.8	High
CVE-2023-36900	microsoft - multiple products	Windows Common Log File System Driver Elevation of Privilege Vulnerability	2023-08-08	7.8	High

CVE-2023-36904	microsoft - multiple products	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2023-08-08	7.8	High
CVE-2023-38154	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-08-08	7.8	High
CVE-2023-38170	microsoft - hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability	2023-08-08	7.8	High
CVE-2023-38175	microsoft - windows_defender	Microsoft Windows Defender Elevation of Privilege Vulnerability	2023-08-08	7.8	High
CVE-2023-39211	zoom - multiple products	Improper privilege management in Zoom Desktop Client for Windows and Zoom Rooms for Windows before 5.15.5 may allow an authenticated user to enable an information disclosure via local access.	2023-08-08	7.8	High
CVE-2023-38211	adobe - dimension	Adobe Dimension version 3.4.9 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.	2023-08-09	7.8	High
CVE-2023-38212	adobe - dimension	Adobe Dimension version 3.4.9 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.	2023-08-09	7.8	High
CVE-2023-30679	samsung - multiple products	Improper access control in HDCP trustlet prior to SMR Aug-2023 Release 1 allows local attackers to execute arbitrary code.	2023-08-10	7.8	High
CVE-2023-30680	samsung - multiple products	Improper privilege management vulnerability in MMIGroup prior to SMR Aug-2023 Release 1 allows code execution with privilege.	2023-08-10	7.8	High
CVE-2023-30681	samsung - multiple products	An improper input validation vulnerability within initialize function in HAL VaultKeeper prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write.	2023-08-10	7.8	High
CVE-2023-30686	samsung - multiple products	Out-of-bounds Write in ReqDataRaw of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	2023-08-10	7.8	High
CVE-2023-30687	samsung - multiple products	Out-of-bounds Write in RmtUimApdu of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	2023-08-10	7.8	High
CVE-2023-30688	samsung - multiple products	Out-of-bounds Write in MakeUiccAuthForOem of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	2023-08-10	7.8	High
CVE-2023-30689	samsung - multiple products	Out-of-bounds Write in BuildOemEmbmsGetSigStrengthResponse of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	2023-08-10	7.8	High
CVE-2023-30691	samsung - multiple products	Parcel mismatch in AuthenticationConfig prior to SMR Aug-2023 Release 1 allows local attacker to privilege escalation.	2023-08-10	7.8	High
CVE-2023-30693	samsung - multiple products	Out-of-bounds Write in DoOemFactorySendFactoryBypassCommand of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	2023-08-10	7.8	High
CVE-2023-30694	samsung - multiple products	Out-of-bounds Write in IpcTxPcscTransmitApdu of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	2023-08-10	7.8	High
CVE-2023-30695	samsung - galaxy_book_go_firmware	Out-of-bounds Write vulnerability in SSHDCPAPP TA prior to "SAMSUNG ELECTONICS, CO, LTD. - System Hardware Update - 7/13/2023" in Windows Update for Galaxy book Go, Galaxy book Go 5G, Galaxy book2 Go and Galaxy book2 Pro 360 allows local attacker to execute arbitrary code.	2023-08-10	7.8	High
CVE-2023-30696	samsung - multiple products	An improper input validation in IpcTxGetVerifyAkey in libsec-ril prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write.	2023-08-10	7.8	High
CVE-2023-30697	samsung - multiple products	An improper input validation in IpcTxCfgSetSimlockPayload in libsec-ril prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-bounds write.	2023-08-10	7.8	High
CVE-2023-30702	samsung - galaxy_book_go_firmware	Stack overflow vulnerability in SSHDCPAPP TA prior to "SAMSUNG ELECTONICS, CO, LTD. - System Hardware Update - 7/13/2023" in Windows Update for Galaxy book Go, Galaxy book Go 5G, Galaxy book2 Go and Galaxy book2 Pro 360 allows local attacker to execute arbitrary code.	2023-08-10	7.8	High
CVE-2023-29320	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Violation of Secure Design Principles vulnerability that could result in arbitrary code execution in the context of the current user by bypassing the API blacklisting feature. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	7.8	High
CVE-2023-38222	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	2023-08-10	7.8	High
CVE-2023-38223	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer that could result in arbitrary code execution in the context of the current user. Exploitation of this issue	2023-08-10	7.8	High

		requires user interaction in that a victim must open a malicious file.			
CVE-2023-38224	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	2023-08-10	7.8	High
CVE-2023-38225	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	2023-08-10	7.8	High
CVE-2023-38226	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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.	2023-08-10	7.8	High
CVE-2023-38227	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	2023-08-10	7.8	High
CVE-2023-38228	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	2023-08-10	7.8	High
CVE-2023-38231	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	7.8	High
CVE-2023-38233	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	7.8	High
CVE-2023-38234	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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.	2023-08-10	7.8	High
CVE-2023-38246	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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.	2023-08-10	7.8	High
CVE-2023-4128	linux - multiple products	A use-after-free flaw was found in net/sched/cls_fw.c in classifiers (cls_fw, cls_u32, and cls_route) in the Linux Kernel. This flaw allows a local attacker to perform a local privilege escalation due to incorrect handling of the existing filter, leading to a kernel information leak issue.	2023-08-10	7.8	High
CVE-2023-28129	ivanti - multiple products	Desktop & Server Management (DSM) may have a possible execution of arbitrary commands.	2023-08-10	7.8	High
CVE-2022-25864	intel - oneapi_math_kernel_library	Uncontrolled search path in some Intel(R) oneMKL software before version 2022.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2022-29470	intel - dynamic_tuning_technology	Improper access control in the Intel DTT Software before version 8.7.10400.15482 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2022-38076	intel - multiple products	Improper input validation in some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi software may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2022-43456	intel - multiple products	Uncontrolled search path in some Intel(R) RST software before versions 16.8.5.1014.5, 17.11.3.1010.2, 18.7.6.1011.2 and 19.5.2.1049.5 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-25182	intel - unite	Uncontrolled search path element in the Intel(R) Unite(R) Client software for Mac before version 4.2.11 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-25773	intel - unite	Improper access control in the Intel(R) Unite(R) Hub software installer for Windows before version 4.2.34962 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High

CVE-2023-25944	intel - vcust_tool	Uncontrolled search path element in some Intel(R) VCUST Tool software downloaded before February 3nd 2023 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-26587	intel - easy_streaming_wizard	Improper input validation for the Intel(R) Easy Streaming Wizard software may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-27505	intel - advanced_link_analyzer	Incorrect default permissions in some Intel(R) Advanced Link Analyzer Standard Edition software installers before version 22.1 .1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-27506	intel - optimization_for_tensorflow	Improper buffer restrictions in the Intel(R) Optimization for Tensorflow software before version 2.12 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-27509	intel - ispc_software_installer	Improper access control in some Intel(R) ISPC software installers before version 1.19.0 may allow an authenticated user to potentially enable escalation of privileges via local access.	2023-08-11	7.8	High
CVE-2023-28405	intel - openvino	Uncontrolled search path in the Intel(R) Distribution of OpenVINO(TM) Toolkit before version 2022.3.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-28658	intel - oneapi_math_kernel_library	Insecure inherited permissions in some Intel(R) oneMKL software before version 2022.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-32543	intel - intelligent_test_system	Incorrect default permissions in the Intel(R) ITS sofware before version 3.1 may allow authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-32656	intel - realsense_450_fa_firmware	Improper buffer restrictions in some Intel(R) RealSense(TM) ID software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-32663	intel - realsense_software_development_kit	Incorrect default permissions in some Intel(R) RealSense(TM) SDKs in version 0.25.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-33867	intel - realsense_450_fa_firmware	Improper buffer restrictions in some Intel(R) RealSense(TM) ID software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-33877	intel - realsense_450_fa_firmware	Out-of-bounds write in some Intel(R) RealSense(TM) ID software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-34427	intel - realsense_450_fa_firmware	Protection mechanism failure in some Intel(R) RealSense(TM) ID software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-34438	intel - nuc_rugged_kit_nuc8cchb_firmware	Race condition in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2023-32783	zohocorp - manageengine_adaudit_plus	The event analysis component in Zoho ManageEngine ADAudit Plus 7.1.1 allows an attacker to bypass audit detection by creating or renaming user accounts with a "$" symbol suffix.	2023-08-07	7.5	High
CVE-2023-33993	sap - business_one	B1i module of SAP Business One - version 10.0, application allows an authenticated user with deep knowledge to send crafted queries over the network to read or modify the SQL data. On successful exploitation, the attacker can cause high impact on confidentiality, integrity and availability of the application.	2023-08-08	7.5	High
CVE-2023-37486	sap - multiple products	Under certain conditions SAP Commerce (OCC API) - versions HY_COM 2105, HY_COM 2205, COM_CLOUD 2211, endpoints allow an attacker to access information which would otherwise be restricted. On successful exploitation there could be a high impact on confidentiality with no impact on integrity and availability of the application.	2023-08-08	7.5	High
CVE-2023-21625	qualcomm - apq8009_firmware	Information disclosure in Network Services due to buffer over-read while the device receives DNS response.	2023-08-08	7.5	High
CVE-2023-28555	qualcomm - ar8035_firmware	Transient DOS in Audio while remapping channel buffer in media codec decoding.	2023-08-08	7.5	High
CVE-2023-37373	siemens - ruggedcom_crossbow	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.4). The affected applications accept unauthenticated file write messages. An unauthenticated remote attacker could write arbitrary files to the affected application's file system.	2023-08-08	7.5	High
CVE-2023-39269	siemens - ruggedcom_ros	A vulnerability has been identified in RUGGEDCOM i800, RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC, RUGGEDCOM i802, RUGGEDCOM i802NC, RUGGEDCOM i803, RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM M2100F, RUGGEDCOM M2100NC, RUGGEDCOM M2200, RUGGEDCOM M2200F, RUGGEDCOM M2200NC, RUGGEDCOM M969, RUGGEDCOM M969F, RUGGEDCOM M969NC,	2023-08-08	7.5	High

		RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC, RUGGEDCOM RS400, RUGGEDCOM RS400F, RUGGEDCOM RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC, RUGGEDCOM RS416, RUGGEDCOM RS416F, RUGGEDCOM RS416NC, RUGGEDCOM RS416NC v2, RUGGEDCOM RS416P, RUGGEDCOM RS416PF, RUGGEDCOM RS416PNC, RUGGEDCOM RS416PNC v2, RUGGEDCOM RS416Pv2, RUGGEDCOM RS416v2, RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC, RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900F, RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GF, RUGGEDCOM RS900GNC, RUGGEDCOM RS900GNC(32M) V4.X, RUGGEDCOM RS900GNC(32M) V5.X, RUGGEDCOM RS900GP, RUGGEDCOM RS900GPF, RUGGEDCOM RS900GPNC, RUGGEDCOM RS900L, RUGGEDCOM RS900LNC, RUGGEDCOM RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-GETS-XX, RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM RS900MNC-STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM RS900NC(32M) V4.X, RUGGEDCOM RS900NC(32M) V5.X, RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GF, RUGGEDCOM RS940GNC, RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100F, RUGGEDCOM RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PF, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200F, RUGGEDCOM RSG2200NC, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300F, RUGGEDCOM RSG2300NC V4.X, RUGGEDCOM RSG2300NC V5.X, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM RSG2300P V5.X, RUGGEDCOM RSG2300PF, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488F, RUGGEDCOM RSG2488NC V4.X, RUGGEDCOM RSG2488NC V5.X, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C, RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM RSL910, RUGGEDCOM RSL910NC, RUGGEDCOM RST2228, RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM RST916P. The web server of the affected devices contains a vulnerability that may lead to a denial of service condition. An attacker may cause total loss of availability of the web server, which might recover after the attack is over.			
CVE-2023-35383	microsoft - multiple products	Microsoft Message Queuing Information Disclosure Vulnerability	2023-08-08	7.5	High
CVE-2023-36532	zoom - multiple products	Buffer overflow in Zoom Clients before 5.14.5 may allow an unauthenticated user to enable a denial of service via network access.	2023-08-08	7.5	High
CVE-2023-36533	zoom - multiple products	Uncontrolled resource consumption in Zoom SDKs before 5.14.7 may allow an unauthenticated user to enable a denial of service via network access.	2023-08-08	7.5	High
CVE-2023-36905	microsoft - multiple products	Windows Wireless Wide Area Network Service (WwanSvc) Information Disclosure Vulnerability	2023-08-08	7.5	High
CVE-2023-36906	microsoft - multiple products	Windows Cryptographic Services Information Disclosure Vulnerability	2023-08-08	7.5	High
CVE-2023-36907	microsoft - multiple products	Windows Cryptographic Services Information Disclosure Vulnerability	2023-08-08	7.5	High
CVE-2023-36912	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-08-08	7.5	High
CVE-2023-36913	microsoft - multiple products	Microsoft Message Queuing Information Disclosure Vulnerability	2023-08-08	7.5	High

CVE-2023-38172	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-08-08	7.5	High
CVE-2023-38178	microsoft - multiple products	.NET Core and Visual Studio Denial of Service Vulnerability	2023-08-08	7.5	High
CVE-2023-38184	microsoft - multiple products	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	2023-08-08	7.5	High
CVE-2023-39217	zoom - multiple products	Improper input validation in Zoom SDK's before 5.14.10 may allow an unauthenticated user to enable a denial of service via network access.	2023-08-08	7.5	High
CVE-2023-35391	microsoft - multiple products	ASP.NET Core SignalR and Visual Studio Information Disclosure Vulnerability	2023-08-08	7.5	High
CVE-2023-38180	microsoft - multiple products	.NET and Visual Studio Denial of Service Vulnerability	2023-08-08	7.5	High
CVE-2022-47185	apache - multiple products	Improper input validation vulnerability on the range header in Apache Software Foundation Apache Traffic Server.This issue affects Apache Traffic Server: through 9.2.1.	2023-08-09	7.5	High
CVE-2023-38207	adobe - multiple products	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by a XML Injection (aka Blind XPath Injection) vulnerability that could lead in minor arbitrary file system read. Exploitation of this issue does not require user interaction.	2023-08-09	7.5	High
CVE-2023-37543	cacti - cacti	Cacti before 1.2.6 allows IDOR (Insecure Direct Object Reference) for accessing any graph via a modified local_graph_id parameter to graph_xport.php. This is a different vulnerability than CVE-2019-16723.	2023-08-10	7.5	High
CVE-2023-32561	ivanti - avalanche	A previously generated artifact by an administrator could be accessed by an attacker. The contents of this artifact could lead to authentication bypass. Fixed in version 6.4.1.	2023-08-10	7.5	High
CVE-2023-24016	intel - multiple products	Uncontrolled search path element in some Intel(R) Quartus(R) Prime Pro and Standard edition software for linux may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.3	High
CVE-2023-28823	intel - multiple products	Uncontrolled search path in some Intel(R) oneAPI Toolkit and component software installers before version 4.3.1.493 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.3	High
CVE-2023-33913	google - multiple products	In DRM/oemcrypto, there is a possible out of bounds write due to an incorrect calculation of buffer size.This could lead to remote escalation of privilege with System execution privileges needed	2023-08-07	7.2	High
CVE-2023-4009	mongodb - multiple products	In MongoDB Ops Manager v5.0 prior to 5.0.22 and v6.0 prior to 6.0.17 it is possible for an authenticated user with project owner or project user admin access to generate an API key with the privileges of org owner resulting in privilege escalation.	2023-08-08	7.2	High
CVE-2023-38167	microsoft - dynamics_365_business_central	Microsoft Dynamics Business Central Elevation Of Privilege Vulnerability	2023-08-08	7.2	High
CVE-2023-38208	adobe - multiple products	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead to arbitrary code execution by an admin-privilege authenticated attacker. Exploitation of this issue does not require user interaction.	2023-08-09	7.2	High
CVE-2023-35179	solarwinds - serv-u	A vulnerability has been identified within Serv-U 15.4 that, if exploited, allows an actor to bypass multi-factor/two-factor authentication. The actor must have administrator-level access to Serv-U to perform this action.	2023-08-11	7.2	High
CVE-2023-25757	intel - unison	Improper access control in some Intel(R) Unison(TM) software before version 10.12 may allow a privileged user to potentially enable escalation of privilege via network access.	2023-08-11	7.2	High
CVE-2023-21626	qualcomm - apq8009_firmware	Cryptographic issue in HLOS due to improper authentication while performing key velocity checks using more than one key.	2023-08-08	7.1	High
CVE-2023-21652	qualcomm - aqt1000_firmware	Cryptographic issue in HLOS as derived keys used to encrypt/decrypt information is present on stack after use.	2023-08-08	7.1	High
CVE-2023-36876	microsoft - windows_server_2008	Reliability Analysis Metrics Calculation (RacTask) Elevation of Privilege Vulnerability	2023-08-08	7.1	High
CVE-2023-28576	qualcomm - fastconnect_6800_firmware	The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues.	2023-08-08	7	High
CVE-2023-35378	microsoft - multiple products	Windows Projected File System Elevation of Privilege Vulnerability	2023-08-08	7	High
CVE-2023-38176	microsoft - azure_arc-enabled_servers	Azure Arc-Enabled Servers Elevation of Privilege Vulnerability	2023-08-08	7	High

CVE-2023-20783	google - multiple products	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826905; Issue ID: ALPS07826905.	2023-08-07	6.7	Medium
CVE-2023-20784	google - multiple products	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07826989; Issue ID: ALPS07826989.	2023-08-07	6.7	Medium
CVE-2023-20786	google - multiple products	In gps, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767811; Issue ID: ALPS07767811.	2023-08-07	6.7	Medium
CVE-2023-20795	google - multiple products	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07864900.	2023-08-07	6.7	Medium
CVE-2023-20797	google - multiple products	In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629582; Issue ID: ALPS07629582.	2023-08-07	6.7	Medium
CVE-2023-20806	google - multiple products	In hcp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07340433; Issue ID: ALPS07537437.	2023-08-07	6.7	Medium
CVE-2023-20807	google - multiple products	In dpe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608433; Issue ID: ALPS07608433.	2023-08-07	6.7	Medium
CVE-2023-20808	google - android	In OPTEE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: DTV03645895.	2023-08-07	6.7	Medium
CVE-2023-20809	google - multiple products	In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198.	2023-08-07	6.7	Medium
CVE-2023-20811	google - multiple products	In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061.	2023-08-07	6.7	Medium
CVE-2023-20814	google - multiple products	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560.	2023-08-07	6.7	Medium
CVE-2023-20815	google - multiple products	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587.	2023-08-07	6.7	Medium
CVE-2023-20816	google - multiple products	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589.	2023-08-07	6.7	Medium
CVE-2023-20817	google - multiple products	In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600.	2023-08-07	6.7	Medium
CVE-2023-4273	linux - multiple products	A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged attacker could use this flaw to overflow the kernel stack.	2023-08-09	6.7	Medium

CVE-2022-27635	intel - multiple products	Improper access control for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi software may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.7	Medium
CVE-2022-36372	intel - nuc_8_compute_element_cm8i3cb4n_firmware	Improper buffer restrictions in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.7	Medium
CVE-2022-37336	intel - nuc_10_performance_kit_nuc10i7fnhn_firmware	Improper input validation in BIOS firmware for some Intel(R) NUC may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.7	Medium
CVE-2022-37343	intel - atom_c3338r_firmware	Improper access control in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.7	Medium
CVE-2022-40964	intel - multiple products	Improper access control for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi software may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.7	Medium
CVE-2022-41804	debian - multiple products	Unauthorized error injection in Intel(R) SGX or Intel(R) TDX for some Intel(R) Xeon(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.7	Medium
CVE-2022-46329	intel - multiple products	Protection mechanism failure for some Intel(R) PROSet/Wireless WiFi software may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.7	Medium
CVE-2023-22449	intel - nuc_13_extreme_compute_element_nuc13sbbi5_firmware	Improper input validation in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.7	Medium
CVE-2023-27391	intel - multiple products	Improper access control in some Intel(R) oneAPI Toolkit and component software installers before version 4.3.1.493 may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.7	Medium
CVE-2023-28385	intel - next_unit_of_computing_firmware	Improper authorization in the Intel(R) NUC Pro Software Suite for Windows before version 2.0.0.9 may allow a privileged user to potentially enable escalation of privilage via local access.	2023-08-11	6.7	Medium
CVE-2023-29494	intel - nuc_11_pro_kit_nuc11tnhi70z_firmware	Improper input validation in BIOS firmware for some Intel(R) NUCs may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.7	Medium
CVE-2023-32617	intel - nuc_kit_nuc7i7bnhx1_firmware	Improper input validation in some Intel(R) NUC Rugged Kit, Intel(R) NUC Kit and Intel(R) Compute Element BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.7	Medium
CVE-2023-34086	intel - nuc_rugged_kit_nuc8cchb_firmware	Improper input validation in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.7	Medium
CVE-2023-38157	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2023-08-07	6.5	Medium
CVE-2023-38924	netgear - dgn3500_firmware	Netgear DGN3500 1.1.00.37 was discovered to contain a buffer overflow via the http_password parameter at setup.cgi.	2023-08-07	6.5	Medium
CVE-2023-37492	sap - multiple products	SAP NetWeaver Application Server ABAP and ABAP Platform - versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This could allow an attacker to read sensitive information which can be used in a subsequent serious attack.	2023-08-08	6.5	Medium
CVE-2023-21647	qualcomm - qca6390_firmware	Information disclosure in Bluetooth when an GATT packet is received due to improper input validation.	2023-08-08	6.5	Medium
CVE-2023-35376	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-08-08	6.5	Medium
CVE-2023-35377	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-08-08	6.5	Medium
CVE-2023-35384	microsoft - multiple products	Windows HTML Platforms Security Feature Bypass Vulnerability	2023-08-08	6.5	Medium
CVE-2023-35389	microsoft - multiple products	Microsoft Dynamics 365 On-Premises Remote Code Execution Vulnerability	2023-08-08	6.5	Medium
CVE-2023-36535	zoom - multiple products	Client-side enforcement of server-side security in Zoom clients before 5.14.10 may allow an authenticated user to enable information disclosure via network access.	2023-08-08	6.5	Medium
CVE-2023-36890	microsoft - multiple products	Microsoft SharePoint Server Information Disclosure Vulnerability	2023-08-08	6.5	Medium
CVE-2023-36893	microsoft - multiple products	Microsoft Outlook Spoofing Vulnerability	2023-08-08	6.5	Medium
CVE-2023-36894	microsoft - multiple products	Microsoft SharePoint Server Information Disclosure Vulnerability	2023-08-08	6.5	Medium

CVE-2023-36897	microsoft - multiple products	Visual Studio Tools for Office Runtime Spoofing Vulnerability	2023-08-08	6.5	Medium
CVE-2023-36908	microsoft - multiple products	Windows Hyper-V Information Disclosure Vulnerability	2023-08-08	6.5	Medium
CVE-2023-36909	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-08-08	6.5	Medium
CVE-2023-38254	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-08-08	6.5	Medium
CVE-2023-39209	zoom - zoom	Improper input validation in Zoom Desktop Client for Windows before 5.15.5 may allow an authenticated user to enable an information disclosure via network access.	2023-08-08	6.5	Medium
CVE-2023-38209	adobe - multiple products	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and earlier) and 2.4.4-p4 (and earlier) are affected by an Incorrect Authorization vulnerability that could lead to a Security feature bypass. A low-privileged attacker could leverage this vulnerability to access other user's data. Exploitation of this issue does not require user interaction.	2023-08-09	6.5	Medium
CVE-2022-36351	intel - multiple products	Improper input validation in some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi software may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2023-08-11	6.5	Medium
CVE-2022-40982	redhat - multiple products	Information exposure through microarchitectural state after transient execution in certain vector execution units for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	2023-08-11	6.5	Medium
CVE-2023-20785	google - multiple products	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID: ALPS07628524.	2023-08-07	6.4	Medium
CVE-2023-20787	google - android	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648734.	2023-08-07	6.4	Medium
CVE-2023-20788	google - android	In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID: ALPS07648735.	2023-08-07	6.4	Medium
CVE-2023-34349	intel - nuc_performance_kit_and_mini_pc_nuc10i3fnh_firmware	Race condition in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.4	Medium
CVE-2023-36869	microsoft - multiple products	Azure DevOps Server Spoofing Vulnerability	2023-08-08	6.3	Medium
CVE-2023-37488	sap - netweaver_process_integration	In SAP NetWeaver Process Integration - versions SAP_XIESR 7.50, SAP_XITOOL 7.50, SAP_XIAF 7.50, user-controlled inputs, if not sufficiently encoded, could result in Cross-Site Scripting (XSS) attack. On successful exploitation the attacker can cause limited impact on confidentiality and integrity of the system.	2023-08-08	6.1	Medium
CVE-2023-38333	zohocorp - multiple products	Zoho ManageEngine Applications Manager through 16530 allows reflected XSS while logged in.	2023-08-10	6.1	Medium
CVE-2020-27449	zohocorp - manageengine_password_manager_pro	Cross Site Scripting (XSS) vulnerability in Query Report feature in Zoho ManageEngine Password Manager Pro version 11001, allows remote attackers to execute arbitrary code and steal cookies via crafted JavaScript payload.	2023-08-11	6.1	Medium
CVE-2023-36873	microsoft - .net_framework	.NET Framework Spoofing Vulnerability	2023-08-08	5.9	Medium
CVE-2023-39436	sap - multiple products	SAP Supplier Relationship Management -versions 600, 602, 603, 604, 605, 606, 616, 617, allows an unauthorized attacker to discover information relating to SRM within Vendor Master Data for Business Partners replication functionality.This information could be used to allow the attacker to specialize their attacks against SRM.	2023-08-08	5.8	Medium
CVE-2023-33906	google - multiple products	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-08-07	5.5	Medium
CVE-2023-33907	google - multiple products	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	2023-08-07	5.5	Medium
CVE-2023-33908	google - multiple products	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	2023-08-07	5.5	Medium
CVE-2023-33909	google - multiple products	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-08-07	5.5	Medium

CVE-2023-33910	google - multiple products	In Contacts Service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-08-07	5.5	Medium
CVE-2023-33911	google - multiple products	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-08-07	5.5	Medium
CVE-2023-33912	google - multiple products	In Contacts service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-08-07	5.5	Medium
CVE-2023-4194	linux - multiple products	A flaw was found in the Linux kernel's TUN/TAP functionality. This issue could allow a local user to bypass network filters and gain unauthorized access to some resources. The original patches fixing CVE-2023-1076 are incorrect or incomplete. The problem is that the following upstream commits - a096ccca6e50 ("tun: tun_chr_open(): correctly initialize socket uid"), - 66b2c338adce ("tap: tap_open(): correctly initialize socket uid"), pass "inode->i_uid" to sock_init_data_uid() as the last parameter and that turns out to not be accurate.	2023-08-07	5.5	Medium
CVE-2023-38532	siemens - multiple products	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected application contains a stack exhaustion vulnerability while parsing a specially crafted X_T file. This could allow an attacker to cause denial of service condition.	2023-08-08	5.5	Medium
CVE-2023-36889	microsoft - multiple products	Windows Group Policy Security Feature Bypass Vulnerability	2023-08-08	5.5	Medium
CVE-2023-36914	microsoft - multiple products	Windows Smart Card Resource Management Server Security Feature Bypass Vulnerability	2023-08-08	5.5	Medium
CVE-2023-39210	zoom - meeting_software_development_kit	Cleartext storage of sensitive information in Zoom Client SDK for Windows before 5.15.0 may allow an authenticated user to enable an information disclosure via local access.	2023-08-08	5.5	Medium
CVE-2023-39212	zoom - rooms	Untrusted search path in Zoom Rooms for Windows before version 5.15.5 may allow an authenticated user to enable a denial of service via local access.	2023-08-08	5.5	Medium
CVE-2023-38213	adobe - dimension	Adobe Dimension version 3.4.9 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.	2023-08-09	5.5	Medium
CVE-2023-30654	samsung - multiple products	Improper access control vulnerability in SLocationService prior to SMR Aug-2023 Release 1 allows local attacker to update fake location.	2023-08-10	5.5	Medium
CVE-2023-30698	samsung - multiple products	Improper access control vulnerability in TelephonyUI prior to SMR Aug-2023 Release 1 allows local attacker to connect BLE without privilege.	2023-08-10	5.5	Medium
CVE-2023-30701	samsung - multiple products	PendingIntent hijacking in WifiGeofenceManager prior to SMR Aug-2023 Release 1 allows local attacker to arbitrary file access.	2023-08-10	5.5	Medium
CVE-2023-30705	samsung - galaxy_store	Improper sanitization of incoming intent in Galaxy Store prior to version 4.5.56.6?allows local attackers to access privileged content providers as Galaxy Store permission.	2023-08-10	5.5	Medium
CVE-2023-29303	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use After Free 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.	2023-08-10	5.5	Medium
CVE-2023-38210	adobe - xmp_toolkit_software_development_kit	Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	5.5	Medium
CVE-2023-38229	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	5.5	Medium
CVE-2023-38230	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free 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.	2023-08-10	5.5	Medium
CVE-2023-38232	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read	2023-08-10	5.5	Medium

		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.			
CVE-2023-38235	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	5.5	Medium
CVE-2023-38236	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	5.5	Medium
CVE-2023-38237	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	5.5	Medium
CVE-2023-38238	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free 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.	2023-08-10	5.5	Medium
CVE-2023-38239	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	5.5	Medium
CVE-2023-38240	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	5.5	Medium
CVE-2023-38241	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	5.5	Medium
CVE-2023-38242	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	5.5	Medium
CVE-2023-38243	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free 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.	2023-08-10	5.5	Medium
CVE-2023-38244	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	5.5	Medium
CVE-2023-38245	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted Microsoft Office file, or visit an attacker controlled web page.	2023-08-10	5.5	Medium
CVE-2023-38247	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	5.5	Medium
CVE-2023-38248	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read	2023-08-10	5.5	Medium

		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.			
CVE-2022-44612	intel - unison	Use of hard-coded credentials in some Intel(R) Unison(TM) software before version 10.12 may allow an authenticated user user to potentially enable information disclosure via local access.	2023-08-11	5.5	Medium
CVE-2023-22338	intel - onevpl_gpu_runtime	Out-of-bounds read in some Intel(R) oneVPL GPU software before version 22.6.5 may allow an authenticated user to potentially enable information disclosure via local access.	2023-08-11	5.5	Medium
CVE-2023-22840	intel - onevpl_gpu_runtime	Improper neutralization in software for the Intel(R) oneVPL GPU software before version 22.6.5 may allow an authenticated user to potentially enable denial of service via local access.	2023-08-11	5.5	Medium
CVE-2023-28711	intel - hyperscan_library	Insufficient control flow management in the Hyperscan Library maintained by Intel(R) before version 5.4.1 may allow an authenticated user to potentially enable denial of service via local access.	2023-08-11	5.5	Medium
CVE-2023-30760	intel - realsense_450_fa_firmware	Out-of-bounds read in some Intel(R) RealSense(TM) ID software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow an authenticated user to potentially enable information disclosure via local access.	2023-08-11	5.5	Medium
CVE-2023-32609	intel - unite	Improper access control in the Intel Unite(R) android application before version 4.2.3504 may allow an authenticated user to potentially enable information disclosure via local access.	2023-08-11	5.5	Medium
CVE-2023-37581	apache - roller	Insufficient input validation and sanitation in Weblog Category name, Website About and File Upload features in all versions of Apache Roller on all platforms allows an authenticated user to perform an XSS attack. Mitigation: if you do not have Roller configured for untrusted users, then you need to do nothing because you trust your users to author raw HTML and other web content. If you are running with untrusted users then you should upgrade to Roller 6.1.2 and you should disable Roller's File Upload feature.?	2023-08-06	5.4	Medium
CVE-2023-39437	sap - business_one	SAP business One allows - version 10.0, allows an attacker to insert malicious code into the content of a web page or application and gets it delivered to the client, resulting to Cross-site scripting. This could lead to harmful action affecting the Confidentiality, Integrity and Availability of the application.	2023-08-08	5.4	Medium
CVE-2023-36926	sap - host_agent	Due to missing authentication check in SAP Host Agent - version 7.22, an unauthenticated attacker can set an undocumented parameter to a particular compatibility value and in turn call read functions. This allows the attacker to gather some non-sensitive information about the server. There is no impact on integrity or availability.	2023-08-08	5.3	Medium
CVE-2023-37484	sap - powerdesigner	SAP PowerDesigner - version 16.7, queries all password hashes in the backend database and compares it with the user provided one during login attempt, which might allow an attacker to access password hashes from the client's memory.	2023-08-08	5.3	Medium
CVE-2023-37487	sap - business_one	SAP Business One (Service Layer) - version 10.0, allows an authenticated attacker with deep knowledge perform certain operation to access unintended data over the network which could lead to high impact on confidentiality with no impact on integrity and availability of the application	2023-08-08	5.3	Medium
CVE-2023-3953	schneider-electric - pro-face_gp-pro_ex	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause memory corruption when an authenticated user opens a tampered log file from GP-Pro EX.	2023-08-09	5.3	Medium
CVE-2023-39218	zoom - multiple products	Client-side enforcement of server-side security in Zoom clients before 5.14.10 may allow a privileged user to enable information disclosure via network access.	2023-08-08	4.9	Medium
CVE-2023-29299	adobe - multiple products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Untrusted Search Path vulnerability that could lead to Application denial-of-service. An attacker could leverage this vulnerability if the default PowerShell Set-ExecutionPolicy is set to Unrestricted, making the attack complexity high. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	4.7	Medium
CVE-2023-35394	microsoft - azure_hdinsights	Azure HDInsight Jupyter Notebook Spoofing Vulnerability	2023-08-08	4.6	Medium
CVE-2023-30704	samsung - internet	Improper Authorization vulnerability in Samsung Internet prior to version 22.0.0.35 allows physical attacker access downloaded files in Secret Mode without user authentication.	2023-08-10	4.6	Medium

CVE-2023-35393	microsoft - azure_hdinsights	Azure Apache Hive Spoofing Vulnerability	2023-08-08	4.5	Medium
CVE-2023-36877	microsoft - azure_hdinsights	Azure Apache Oozie Spoofing Vulnerability	2023-08-08	4.5	Medium
CVE-2023-36881	microsoft - azure_hdinsights	Azure Apache Ambari Spoofing Vulnerability	2023-08-08	4.5	Medium
CVE-2023-38188	microsoft - azure_hdinsights	Azure Apache Hadoop Spoofing Vulnerability	2023-08-08	4.5	Medium
CVE-2022-47350	google - multiple products	In camera 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	2023-08-07	4.4	Medium
CVE-2022-47351	google - multiple products	In camera 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	2023-08-07	4.4	Medium
CVE-2023-20780	google - multiple products	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS08017756.	2023-08-07	4.4	Medium
CVE-2023-20781	google - multiple products	In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID: ALPS07905323.	2023-08-07	4.4	Medium
CVE-2023-20782	google - multiple products	In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550103.	2023-08-07	4.4	Medium
CVE-2023-20789	google - multiple products	In jpeg, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07693193; Issue ID: ALPS07693193.	2023-08-07	4.4	Medium
CVE-2023-20793	google - multiple products	In apu, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767818; Issue ID: ALPS07767818.	2023-08-07	4.4	Medium
CVE-2023-20798	google - multiple products	In pda, there is a possible out of bounds read due to an incorrect calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07147572; Issue ID: ALPS07421076.	2023-08-07	4.4	Medium
CVE-2023-20810	google - multiple products	In IOMMU, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061.	2023-08-07	4.4	Medium
CVE-2023-20813	google - multiple products	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453549; Issue ID: ALPS07453549.	2023-08-07	4.4	Medium
CVE-2023-20818	google - multiple products	In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460540; Issue ID: ALPS07460540.	2023-08-07	4.4	Medium
CVE-2023-39440	sap - businessobjects_business_intelligence	In SAP BusinessObjects Business Intelligence - version 420, If a user logs in to a particular program, under certain specific conditions memory might not be cleared up properly, due to which attacker might be able to get access to user credentials. For a successful attack, the attacker needs to have local access to the system. There is no impact on availability and integrity.	2023-08-08	4.4	Medium
CVE-2022-27879	intel - pentium_j6426_firmware	Improper buffer restrictions in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	2023-08-11	4.4	Medium
CVE-2022-34657	intel - pcsd_bios	Improper input validation in firmware for some Intel(R) PCSD BIOS before version 02.01.0013 may allow a privileged user to potentially enable information disclosure via local access.	2023-08-11	4.4	Medium
CVE-2022-38083	intel - xeon_d-2745nx_firmware	Improper initialization in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	2023-08-11	4.4	Medium
CVE-2022-38102	intel - converged_security_management_engine_firmware	Improper Input validation in firmware for some Intel(R) Converged Security and Management Engine before versions 15.0.45, and 16.1.27 may allow a privileged user to potentially enable denial of service via local access.	2023-08-11	4.4	Medium

CVE-2022-43505	intel - pentium_j6426_firmware	Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable denial of service via local access.	2023-08-11	4.4	Medium
CVE-2023-22330	intel - nuc_11_performance_kit_nuc11pahi3_firmware	Use of uninitialized resource in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable information disclosure via local access.	2023-08-11	4.4	Medium
CVE-2023-22356	intel - nuc_7_enthusiast_nuc7i7bnkq_firmware	Improper initialization in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable information disclosure via local access.	2023-08-11	4.4	Medium
CVE-2023-22444	intel - nuc_13_extreme_compute_element_nuc13sbbi7f_firmware	Improper initialization in some Intel(R) NUC 13 Extreme Compute Element, Intel(R) NUC 13 Extreme Kit, Intel(R) NUC 11 Performance Kit, Intel(R) NUC 11 Performance Mini PC, Intel(R) NUC Compute Element, Intel(R) NUC Laptop Kit, Intel(R) NUC Pro Kit, Intel(R) NUC Pro Board and Intel(R) NUC Pro Mini PC BIOS firmware may allow a privileged user to potentially enable information disclosure via local access.	2023-08-11	4.4	Medium
CVE-2023-27392	intel - support	Incorrect default permissions in the Intel(R) Support android application before version v23.02.07 may allow a privileged user to potentially enable information disclosure via local access.	2023-08-11	4.4	Medium
CVE-2023-27887	intel - nuc_11_pro_kit_nuc11tnhi70z_firmware	Improper initialization in BIOS firmware for some Intel(R) NUCs may allow a privileged user to potentially enable information disclosure via local access.	2023-08-11	4.4	Medium
CVE-2023-29243	intel - realsense_450_fa_firmware	Unchecked return value in some Intel(R) RealSense(TM) ID software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow a priviledged user to potentially enable denial of service via local access.	2023-08-11	4.4	Medium
CVE-2023-29500	intel - nuc_11_performance_kit_nuc11pahi70z_firmware	Exposure of sensitive information to an unauthorized actor in BIOS firmware for some Intel(R) NUCs may allow a privilege user to potentially enable information disclosure via local access.	2023-08-11	4.4	Medium
CVE-2023-32285	intel - nuc_kit_nuc6cayh_firmware	Improper access control in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable denial of service via local access.	2023-08-11	4.4	Medium
CVE-2023-36482	samsung - s3nrn4v_firmware	An issue was discovered in Samsung NFC S3NRN4V, S3NSN4V, S3NSEN4, SEN82AB, and S3NRN82. A buffer copy without checking its input size can cause an NFC service restart.	2023-08-08	4.3	Medium
CVE-2023-30703	samsung - members	Improper URL validation vulnerability in Samsung Members prior to version 14.0.07.1 allows attackers to access sensitive information.	2023-08-10	4.3	Medium
CVE-2023-30682	samsung - multiple products	Improper access control in Telecom prior to SMR Aug-2023 Release 1 allows local attackers to call silenceRinger API without permission.	2023-08-10	3.3	Low
CVE-2023-30683	samsung - multiple products	Improper access control in Telecom prior to SMR Aug-2023 Release 1 allows local attackers to call endCall API without permission.	2023-08-10	3.3	Low
CVE-2023-30684	samsung - multiple products	Improper access control in Samsung Telecom prior to SMR Aug-2023 Release 1 allows local attackers to call acceptRingingCall API without permission.	2023-08-10	3.3	Low
CVE-2023-30685	samsung - multiple products	Improper access control vulnerability in Telecom prior to SMR Aug-2023 Release 1 allows local attakcers to change TTY mode.	2023-08-10	3.3	Low
CVE-2023-30700	samsung - multiple products	PendingIntent hijacking vulnerability in SemWifiApTimeOutImpl in framework prior to SMR Aug-2023 Release 1 allows local attackers to access ContentProvider without proper permission.	2023-08-10	3.3	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.