الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

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

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

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 3rd of December to 9th of December. 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**

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 3 ديسمبر إلى 9 ديسمبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-44302	dell - powerprotect_data_manager_dm5500_firmware	Dell DM5500 5.14.0.0 and prior contain an improper authentication vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability to gain access of resources or functionality that could possibly lead to execute arbitrary code.	2023-12-04	9.8	Critical
CVE-2023-44305	dell - dm5500_firmware	Dell DM5500 5.14.0.0, contains a Stack-based Buffer Overflow Vulnerability in PPOE. An unauthenticated remote attacker may exploit this vulnerability to crash the affected process or execute arbitrary code on the system by sending specially crafted input dat	2023-12-04	9.8	Critical
CVE-2023-21162	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-21163	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-21164	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-21166	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-21215	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-21216	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-21217	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-21218	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-21228	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-21263	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-21401	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-21402	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-21403	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-35690	google - android	There is elevation of privilege.	2023-12-04	9.8	Critical
CVE-2023-40078	google - android	In a2dp_vendor_opus_decoder_decode_packet of a2dp_vendor_opus_decoder.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to paired device escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	9.8	Critical
CVE-2023-40082	google - android	In modify_for_next_stage of fdt.rs, there is a possible way to render KASLR ineffective due to improperly used crypto. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	9.8	Critical
CVE-2023-48315	microsoft - azure_rtos_netx_duo	Azure RTOS NetX Duo is a TCP/IP network stack designed specifically for deeply embedded real-time and IoT applications. An attacker can cause remote code execution due to memory overflow vulnerabilities in Azure RTOS NETX Duo. The affected components include processes/functions related to ftp and sntp in RTOS v6.2.1 and below. The fixes have been included in NetX Duo release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-12-05	9.8	Critical
CVE-2023-48316	microsoft - azure_rtos_netx_duo	Azure RTOS NetX Duo is a TCP/IP network stack designed specifically for deeply embedded real-time and IoT applications. An attacker can cause remote code execution due to memory overflow vulnerabilities in Azure RTOS NETX Duo. The affected components include processes/functions related to snmp, smtp, ftp and dtls in RTOS v6.2.1 and below. The fixes have been	2023-12-05	9.8	Critical

		included in NetX Duo release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.			
CVE-2023-48691	microsoft - azure_rtos_netx_duo	Azure RTOS NetX Duo is a TCP/IP network stack designed specifically for deeply embedded real-time and IoT applications. An attacker can cause an out-of-bounds write in Azure RTOS NETX Duo, that could lead to remote code execution. The affected components include process related to IGMP protocol in RTOS v6.2.1 and below. The fix has been included in NetX Duo release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-12-05	9.8	Critical
CVE-2023-48692	microsoft - azure_rtos_netx_duo	Azure RTOS NetX Duo is a TCP/IP network stack designed specifically for deeply embedded real-time and IoT applications. An attacker can cause remote code execution due to memory overflow vulnerabilities in Azure RTOS NETX Duo. The affected components include processes/functions related to icmp, tcp, snmp, dhcp, nat and ftp in RTOS v6.2.1 and below. The fixes have been included in NetX Duo release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-12-05	9.8	Critical
CVE-2023-48693	microsoft - azure_rtos_threadx	Azure RTOS ThreadX is an advanced real-time operating system (RTOS) designed specifically for deeply embedded applications. An attacker can cause arbitrary read and write due to vulnerability in parameter checking mechanism in Azure RTOS ThreadX, which may lead to privilege escalation. The affected components include RTOS ThreadX v6.2.1 and below. The fixes have been included in ThreadX release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-12-05	9.8	Critical
CVE-2023-48694	microsoft - azure_rtos_usbx	Azure RTOS USBX is a USB host, device, and on-the-go (OTG) embedded stack, that is fully integrated with Azure RTOS ThreadX. An attacker can cause remote code execution due to expired pointer dereference and type confusion vulnerabilities in Azure RTOS USBX. The affected components include functions/processes in host stack and host class, related to device linked classes, ASIX, Prolific, SWAR, audio, CDC ECM in RTOS v6.2.1 and below. The fixes have been included in USBX release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-12-05	9.8	Critical
CVE-2023-48695	microsoft - azure_rtos_usbx	Azure RTOS USBX is a USB host, device, and on-the-go (OTG) embedded stack, that is fully integrated with Azure RTOS ThreadX. An attacker can cause remote code execution due to out of bounds write vulnerabilities in Azure RTOS USBX. The affected components include functions/processes in host and device classes, related to CDC ECM and RNDIS in RTOS v6.2.1 and below. The fixes have been included in USBX release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-12-05	9.8	Critical
CVE-2023-48696	microsoft - azure_rtos_usbx	Azure RTOS USBX is a USB host, device, and on-the-go (OTG) embedded stack, that is fully integrated with Azure RTOS ThreadX. An attacker can cause remote code execution due to expired pointer dereference vulnerabilities in Azure RTOS USBX. The affected components include components in host class, related to CDC ACM in RTOS v6.2.1 and below. The fixes have been included in USBX release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-12-05	9.8	Critical
CVE-2023-48697	microsoft - azure_rtos_usbx	Azure RTOS USBX is a USB host, device, and on-the-go (OTG) embedded stack, that is fully integrated with Azure RTOS ThreadX. An attacker can cause remote code execution due to memory buffer and pointer vulnerabilities in Azure RTOS USBX. The affected components include functions/processes in pictbridge and host class, related to PIMA, storage, CDC ACM, ECM, audio, hub in RTOS v6.2.1 and below. The fixes have been included in USBX release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-12-05	9.8	Critical
CVE-2023-48698	microsoft - azure_rtos_usbx	Azure RTOS USBX is a USB host, device, and on-the-go (OTG) embedded stack, that is fully integrated with Azure RTOS ThreadX. An attacker can cause remote code execution due to expired pointer dereference vulnerabilities in Azure RTOS USBX. The affected components include functions/processes in host stack and host classes, related to device linked classes, GSER and HID in RTOS v6.2.1 and below. The fixes have been included in USBX release 6.3.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-12-05	9.8	Critical
CVE-2023-33082	qualcomm - ar8035_firmware	Memory corruption while sending an Assoc Request having BTM Query or BTM Response containing MBO IE.	2023-12-05	9.8	Critical
CVE-2023-33083	qualcomm - ar8035_firmware	Memory corruption in WLAN Host while processing RRM beacon on the AP.	2023-12-05	9.8	Critical
CVE-2023-42580	samsung - galaxy_store	Improper URL validation from MCSLaunch deeplink in Galaxy Store prior to version 4.5.64.4 allows attackers to execute JavaScript API to install APK from Galaxy Store.	2023-12-05	9.8	Critical

CVE-2023-49070	apache - ofbiz	Pre-auth RCE in Apache Ofbiz 18.12.09. It's due to XML-RPC no longer maintained still present. This issue affects Apache OFBiz: before 18.12.10. Users are recommended to upgrade to version 18.12.10	2023-12-05	9.8	Critical
CVE-2023-41268	samsung - multiple products	Improper input validation vulnerability in Samsung Open Source Escargot allows stack overflow and segmentation fault. This issue affects Escargot: from 3.0.0 through 4.0.0.	2023-12-06	9.8	Critical
CVE-2023-22524	atlassian - companion	Certain versions of the Atlassian Companion App for MacOS were affected by a remote code execution vulnerability. An attacker could utilize WebSockets to bypass Atlassian Companion's blocklist and MacOS Gatekeeper to allow execution of code.	2023-12-06	9.8	Critical
CVE-2023-46773	huawei - emui	Permission management vulnerability in the PMS module. Successful exploitation of this vulnerability may cause privilege escalation.	2023-12-06	9.8	Critical
CVE-2023-50164	apache - multiple products	An attacker can manipulate file upload params to enable paths traversal and under some circumstances this can lead to uploading a malicious file which can be used to perform Remote Code Execution. Users are recommended to upgrade to versions Struts 2.5.33 or Struts 6.3.0.2 or greater to fix this issue.	2023-12-07	9.8	Critical
CVE-2023-49007	netgear - rbr750_firmware	In Netgear Orbi RBR750 firmware before V7.2.6.21, there is a stack-based buffer overflow in /usr/sbin/httpd.	2023-12-08	9.8	Critical
CVE-2023-48423	google - android	In dhcp4_SetPDNAddress of dhcp4_Main.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	9.8	Critical
CVE-2023-47254	draytek - vigor167_firmware	An OS Command Injection in the CLI interface on DrayTek Vigor167 version 5.2.2, allows remote attackers to execute arbitrary system commands and escalate privileges via any account created within the web interface.	2023-12-09	9.8	Critical
CVE-2023-35618	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-12-07	9.6	Critical
CVE-2023-33054	qualcomm - 315_5g_iot_modem_firmware	Cryptographic issue in GPS HLOS Driver while downloading Qualcomm GNSS assistance data.	2023-12-05	9.1	Critical
CVE-2023-44304	dell - dm5500_firmware	Dell DM5500 contains a privilege escalation vulnerability in PPOE Component. A remote attacker with low privileges could potentially exploit this vulnerability to escape the restricted shell and gain root access to the appliance.	2023-12-04	8.8	High
CVE-2023-40087	google - multiple products	In transcodeQ*ToFloat of btif_avrcp_audio_track.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to paired device escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	8.8	High
CVE-2023-40088	google - multiple products	In callback_thread_event of com_android_bluetooth_btservice_AdapterService.cpp, there is a possible memory corruption due to a use after free. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	8.8	High
CVE-2023-28585	qualcomm - 315_5g_iot_modem_firmware	Memory corruption while loading an ELF segment in TEE Kernel.	2023-12-05	8.8	High
CVE-2023-5970	sonicwall - sma_200_firmware	Improper authentication in the SMA100 SSL-VPN virtual office portal allows a remote authenticated attacker to create an identical external domain user using accent characters, resulting in an MFA bypass.	2023-12-05	8.8	High
CVE-2023-6508	google - chrome	Use after free in Media Stream in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-12-06	8.8	High
CVE-2023-6509	google - chrome	Use after free in Side Panel Search in Google Chrome prior to 120.0.6099.62 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: High)	2023-12-06	8.8	High
CVE-2023-6510	google - chrome	Use after free in Media Capture in Google Chrome prior to 120.0.6099.62 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium)	2023-12-06	8.8	High
CVE-2023-22522	atlassian - multiple products	This Template Injection vulnerability allows an authenticated attacker, including one with anonymous access, to inject unsafe user input into a Confluence page. Using this approach, an attacker is able to achieve Remote Code Execution (RCE) on an affected instance. Publicly accessible Confluence Data Center and	2023-12-06	8.8	High

		Server versions as listed below are at risk and require immediate attention. See the advisory for additional details Atlassian Cloud sites are not affected by this vulnerability. If your Confluence site is accessed via an atlassian.net domain, it is hosted by Atlassian and is not vulnerable to this issue.			
CVE-2023-22523	atlassian - multiple products	This vulnerability, if exploited, allows an attacker to perform privileged RCE (Remote Code Execution) on machines with the Assets Discovery agent installed. The vulnerability exists between the Assets Discovery application (formerly known as Insight Discovery) and the Assets Discovery agent.	2023-12-06	8.8	High
CVE-2023-6514	huawei - ajmd-370s_firmware	The Bluetooth module of some Huawei Smart Screen products has an identity authentication bypass vulnerability. Successful exploitation of this vulnerability may allow attackers to access restricted functions. Successful exploitation of this vulnerability may allow attackers to access restricted functions.	2023-12-06	8.8	High
CVE-2023-45866	google - android	Bluetooth HID Hosts in BlueZ may permit an unauthenticated Peripheral role HID Device to initiate and establish an encrypted connection, and accept HID keyboard reports, potentially permitting injection of HID messages when no user interaction has occurred in the Central role to authorize such access. An example affected package is bluez 5.64-0ubuntu1 in Ubuntu 22.04LTS. NOTE: in some cases, a CVE-2020-0556 mitigation would have already addressed this Bluetooth HID Hosts issue.	2023-12-08	8.8	High
CVE-2023-47565	qnap - qvr_firmware	An OS command injection vulnerability has been found to affect legacy QNAP VioStor NVR models running QVR Firmware 4.x. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QVR Firmware 5.0.0 and later	2023-12-08	8.8	High
CVE-2023-40077	google - multiple products	In multiple functions of MetaDataBase.cpp, there is a possible UAF write due to a race condition. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	8.1	High
CVE-2023-44295	dell - powerscale_onefs	Dell PowerScale OneFS versions 8.2.2.x through 9.6.0.x contains an improper control of a resource through its lifetime vulnerability. A low privilege attacker could potentially exploit this vulnerability, leading to loss of information, and information disclosure.	2023-12-05	8.1	High
CVE-2023-42681	google - multiple products	In ion service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42685	google - android	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42686	google - android	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42687	google - android	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42688	google - android	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42689	google - android	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42690	google - android	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42691	google - multiple products	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42692	google - android	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42693	google - android	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42694	google - android	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High

CVE-2023-42695	google - android	In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42696	google - multiple products	In telecom service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42736	google - multiple products	In telecom service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42738	google - multiple products	In telocom service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42739	google - multiple products	In engineermode service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42740	google - multiple products	In telecom service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42743	google - multiple products	In telecom service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42745	google - multiple products	In telecom service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42746	google - multiple products	In power manager, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42747	google - multiple products	In camera service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-42748	google - multiple products	In telecom service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
CVE-2023-32847	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 no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08241940; Issue ID: ALPS08241940.	2023-12-04	7.8	High
CVE-2023-32850	google - multiple products	In decoder, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08016659; Issue ID: ALPS08016659.	2023-12-04	7.8	High
CVE-2023-32851	google - multiple products	In decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08016652; Issue ID: ALPS08016652.	2023-12-04	7.8	High
CVE-2023-40079	google - android	In injectSendIntentSender of ShortcutService.java, there is a possible background activity launch due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-40080	google - multiple products	In multiple functions of btm_ble_gap.cc, there is a possible out of bounds write due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-40084	google - multiple products	In run of MDnsSdListener.cpp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-40089	google - android	In getCredentialManagerPolicy of DevicePolicyManagerService.java, there is a possible method for users to select credential managers without permission due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-40091	google - multiple products	In onTransact of IncidentService.cpp, there is a possible out of bounds write due to memory corruption. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-40094	google - multiple products	In keyguardGoingAway of ActivityTaskManagerService.java, there is a possible lock screen bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High

CVE-2023-40095	google - multiple products	In createDontSendToRestrictedAppsBundle of PendingIntentUtils.java, there is a possible background activity launch due to a missing check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-40096	google - multiple products	In OpRecordAudioMonitor::onFirstRef of AudioRecordClient.cpp, there is a possible way to record audio from the background due to a missing flag. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-40097	google - multiple products	In hasPermissionForActivity of PackageManagerHelper.java, there is a possible URI grant due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2023-12-04	7.8	High
CVE-2023-40103	google - android	In multiple locations, there is a possible way to corrupt memory due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-45773	google - multiple products	In multiple functions of btm_ble_gap.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-45774	google - multiple products	In fixUpIncomingShortcutInfo of ShortcutService.java, there is a possible way to view another user's image due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-45775	google - android	In CreateAudioBroadcast of broadcaster.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-45776	google - android	In CreateAudioBroadcast of broadcaster.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-45777	google - multiple products	In checkKeyIntentParceledCorrectly of AccountManagerService.java, there is a possible way to launch arbitrary activities using system privileges due to Parcel Mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-45779	google - android	In TBD of TBD, there is a possible malicious update to platform components due to improperly used crypto. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
CVE-2023-21634	qualcomm - aqt1000_firmware	Memory Corruption in Radio Interface Layer while sending an SMS or writing an SMS to SIM.	2023-12-05	7.8	High
CVE-2023-22383	qualcomm - aqt1000_firmware	Memory Corruption in camera while installing a fd for a particular DMA buffer.	2023-12-05	7.8	High
CVE-2023-22668	qualcomm - aqt1000_firmware	Memory Corruption in Audio while invoking IOCTLs calls from the user-space.	2023-12-05	7.8	High
CVE-2023-28546	qualcomm - 315_5g_iot_modem_firmware	Memory Corruption in SPS Application while exporting public key in sorter TA.	2023-12-05	7.8	High
CVE-2023-28550	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in MPP performance while accessing DSM watermark using external memory address.	2023-12-05	7.8	High
CVE-2023-28551	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments.	2023-12-05	7.8	High
CVE-2023-28579	qualcomm - fastconnect_6900_firmware	Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length.	2023-12-05	7.8	High
CVE-2023-28580	qualcomm - ar8035_firmware	Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache.	2023-12-05	7.8	High
CVE-2023-28587	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in BT controller while parsing debug commands with specific sub-opcodes at HCI interface level.	2023-12-05	7.8	High
CVE-2023-33017	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in Boot while running a ListVars test in UEFI Menu during boot.	2023-12-05	7.8	High
CVE-2023-33018	qualcomm - 315_5g_iot_modem_firmware	Memory corruption while using the UIM diag command to get the operators name.	2023-12-05	7.8	High
CVE-2023-33022	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in HLOS while invoking IOCTL calls from user-space.	2023-12-05	7.8	High
CVE-2023-33024	qualcomm - aqt1000_firmware	Memory corruption while sending SMS from AP firmware.	2023-12-05	7.8	High

CVE-2023-33053	qualcomm - csr8811_firmware	Memory corruption in Kernel while parsing metadata.	2023-12-05	7.8	High
CVE-2023-33063	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in DSP Services during a remote call from HLOS to DSP.	2023-12-05	7.8	High
CVE-2023-33071	qualcomm - qca6574_firmware	Memory corruption in Automotive OS whenever untrusted apps try to access HAb for graphics functionalities.	2023-12-05	7.8	High
CVE-2023-33079	qualcomm - ar8035_firmware	Memory corruption in Audio while running invalid audio recording from ADSP.	2023-12-05	7.8	High
CVE-2023-33087	qualcomm - ar8035_firmware	Memory corruption in Core while processing RX intent request.	2023-12-05	7.8	High
CVE-2023-33088	qualcomm - 315_5g_iot_modem_firmware	Memory corruption when processing cmd parameters while parsing vdev.	2023-12-05	7.8	High
CVE-2023-33092	qualcomm - aqt1000_firmware	Memory corruption while processing pin reply in Bluetooth, when pin code received from APP layer is greater than expected size.	2023-12-05	7.8	High
CVE-2023-33106	qualcomm - ar8035_firmware	Memory corruption while submitting a large list of sync points in an AUX command to the IOCTL_KGSL_GPU_AUX_COMMAND.	2023-12-05	7.8	High
CVE-2023-33107	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in Graphics Linux while assigning shared virtual memory region during IOCTL call.	2023-12-05	7.8	High
CVE-2023-42558	samsung - multiple products	Out of bounds write vulnerability in HDCP in HAL prior to SMR Dec-2023 Release 1 allows attacker to perform code execution.	2023-12-05	7.8	High
CVE-2023-42560	samsung - multiple products	Heap out-of-bounds write vulnerability in dec_mono_audb of libsavsac.so prior to SMR Dec-2023 Release 1 allows an attacker to execute arbitrary code.	2023-12-05	7.8	High
CVE-2023-42562	samsung - multiple products	Integer overflow vulnerability in detectionFindFaceSupportMultiInstance of libFacePreProcessingjni.camera.samsung.so prior to SMR Dec-2023 Release 1 allows attacker to trigger heap overflow.	2023-12-05	7.8	High
CVE-2023-42563	samsung - multiple products	Integer overflow vulnerability in landmarkCopyImageToNative of libFacePreProcessingjni.camera.samsung.so prior to SMR Dec-2023 Release 1 allows attacker to trigger heap overflow.	2023-12-05	7.8	High
CVE-2023-42566	samsung - multiple products	Out-of-bound write vulnerability in libsavsvc prior to SMR Dec-2023 Release 1 allows local attackers to execute arbitrary code.	2023-12-05	7.8	High
CVE-2023-42567	samsung - multiple products	Improper size check vulnerability in softsimd prior to SMR Dec-2023 Release 1 allows stack-based buffer overflow.	2023-12-05	7.8	High
CVE-2023-42574	samsung - gamehomecn	Improper access control vulnerablility in GameHomeCN prior to version 4.2.60.2 allows local attackers to launch arbitrary activity in GameHomeCN.	2023-12-05	7.8	High
CVE-2023-32460	dell - poweredge_r660_firmware	Dell PowerEdge BIOS contains an improper privilege management security vulnerability. An unauthenticated local attacker could potentially exploit this vulnerability, leading to privilege escalation.	2023-12-08	7.8	High
CVE-2023-48402	google - android	In ppcfw_enable of ppcfw.c, there is a possible EoP due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	7.8	High
CVE-2023-48407	google - android	there is a possible DCK won't be deleted after factory reset due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	7.8	High
CVE-2023-48409	google - android	In gpu_pixel_handle_buffer_liveness_update_ioctl of private/google-modules/gpu/mali_kbase/mali_kbase_core_linux.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	7.8	High
CVE-2023-48421	google - android	In gpu_pixel_handle_buffer_liveness_update_ioctl of private/google-modules/gpu/mali_kbase/platform/pixel/pixel_gpu_slc.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	7.8	High
CVE-2023-28523	ibm - multiple products	IBM Informix Dynamic Server 12.10 and 14.10 onsmsync is vulnerable to a heap buffer overflow, caused by improper bounds checking which could allow an attacker to execute arbitrary code. IBM X-Force ID: 250753.	2023-12-09	7.8	High
CVE-2023-45178	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 CLI is vulnerable to a denial of service when a specially crafted request is used. IBM X-Force ID: 268073.	2023-12-03	7.5	High
CVE-2023-40692	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, 11.5 is vulnerable to denial of service under extreme stress conditions. IBM X-Force ID: 264807.	2023-12-04	7.5	High
CVE-2023-42716	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to remote information disclosure no additional execution privileges needed	2023-12-04	7.5	High

CVE-2023-42717	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to remote information disclosure no additional execution privileges needed	2023-12-04	7.5	High
CVE-2023-46167	ibm - db2	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 federated server is vulnerable to a denial of service when a specially crafted cursor is used. IBM X-Force ID: 269367.	2023-12-04	7.5	High
CVE-2023-47701	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 266166.	2023-12-04	7.5	High
CVE-2023-29258	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1, and 11.5 is vulnerable to a denial of service through a specially crafted federated query on specific federation objects. IBM X-Force ID: 252048.	2023-12-04	7.5	High
CVE-2023-38727	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted SQL statement. IBM X-Force ID: 262257.	2023-12-04	7.5	High
CVE-2023-40687	ibm - multiple products	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted RUNSTATS command on an 8TB table. IBM X-Force ID: 264809.	2023-12-04	7.5	High
CVE-2023-21227	google - android	There is information disclosure.	2023-12-04	7.5	High
CVE-2023-28588	qualcomm - apq8017_firmware	Transient DOS in Bluetooth Host while rfc slot allocation.	2023-12-05	7.5	High
CVE-2023-33041	qualcomm - ar8035_firmware	Under certain scenarios the WLAN Firmware will reach an assertion due to state confusion while looking up peer ids.	2023-12-05	7.5	High
CVE-2023-33042	qualcomm - 315_5g_iot_modem_firmware	Transient DOS in Modem after RRC Setup message is received.	2023-12-05	7.5	High
CVE-2023-33043	qualcomm - ar8035_firmware	Transient DOS in Modem when a Beam switch request is made with a non-configured BWP.	2023-12-05	7.5	High
CVE-2023-33044	qualcomm - 315_5g_iot_modem_firmware	Transient DOS in Data modem while handling TLB control messages from the Network.	2023-12-05	7.5	High
CVE-2023-33080	qualcomm - 315_5g_iot_modem_firmware	Transient DOS while parsing a vender specific IE (Information Element) of reassociation response management frame.	2023-12-05	7.5	High
CVE-2023-33081	qualcomm - aqt1000_firmware	Transient DOS while converting TWT (Target Wake Time) frame parameters in the OTA broadcast.	2023-12-05	7.5	High
CVE-2023-33089	qualcomm - 315_5g_iot_modem_firmware	Transient DOS when processing a NULL buffer while parsing WLAN vdev.	2023-12-05	7.5	High
CVE-2023-33097	qualcomm - ar8035_firmware	Transient DOS in WLAN Firmware while processing a FTMR frame.	2023-12-05	7.5	High
CVE-2023-33098	qualcomm - 315_5g_iot_modem_firmware	Transient DOS while parsing WPA IES, when it is passed with length more than expected size.	2023-12-05	7.5	High
CVE-2023-42578	samsung - cloud	Improper handling of insufficient permissions or privileges vulnerability in Samsung Data Store prior to version 5.2.00.7 allows remote attackers to access location information without permission.	2023-12-05	7.5	High
CVE-2023-42581	samsung - galaxy_store	Improper URL validation from InstantPlay deeplink in Galaxy Store prior to version 4.5.64.4 allows attackers to execute JavaScript API to access data.	2023-12-05	7.5	High
CVE-2023-39248	dell - networking_os10	Dell OS10 Networking Switches running 10.5.2.x and above contain an Uncontrolled Resource Consumption (Denial of Service) vulnerability, when switches are configured with VLT and VRRP. A remote unauthenticated user can cause the network to be flooded leading to Denial of Service for actual network users. This is a high severity vulnerability as it allows an attacker to cause an outage of network. Dell recommends customers to upgrade at the earliest opportunity.	2023-12-05	7.5	High
CVE-2023-44288	dell - powerscale_onefs	Dell PowerScale OneFS, 8.2.2.x through 9.6.0.x, contains an improper control of a resource through its lifetime vulnerability. An unauthenticated network attacker could potentially exploit this vulnerability, leading to denial of service.	2023-12-05	7.5	High
CVE-2023-41835	apache - multiple products	When a Multipart request is performed but some of the fields exceed the maxStringLength limit, the upload files will remain in struts.multipart.saveDir even if the request has been denied. Users are recommended to upgrade to versions Struts 2.5.32 or 6.1.2.2 or Struts 6.3.0.1 or greater, which fixe this issue.	2023-12-05	7.5	High
CVE-2023-44099	huawei - emui	Vulnerability of data verification errors in the kernel module. Successful exploitation of this vulnerability may cause WLAN interruption.	2023-12-06	7.5	High
CVE-2023-44113	huawei - emui	Vulnerability of missing permission verification for APIs in the Designed for Reliability (DFR) module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-12-06	7.5	High

CVE-2023-49239	huawei - multiple products	Unauthorized access vulnerability in the card management module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-12-06	7.5	High
CVE-2023-49240	huawei - multiple products	Unauthorized access vulnerability in the launcher module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-12-06	7.5	High
CVE-2023-49241	huawei - multiple products	API permission control vulnerability in the network management module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-12-06	7.5	High
CVE-2023-49242	huawei - multiple products	Free broadcast vulnerability in the running management module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-12-06	7.5	High
CVE-2023-49243	huawei - multiple products	Vulnerability of unauthorized access to email attachments in the email module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-12-06	7.5	High
CVE-2023-49244	huawei - emui	Permission management vulnerability in the multi-user module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-12-06	7.5	High
CVE-2023-49245	huawei - multiple products	Unauthorized access vulnerability in the Huawei Share module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-12-06	7.5	High
CVE-2023-49246	huawei - multiple products	Unauthorized access vulnerability in the card management module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-12-06	7.5	High
CVE-2023-49247	huawei - multiple products	Permission verification vulnerability in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality.	2023-12-06	7.5	High
CVE-2023-41106	zimbra - multiple products	An issue was discovered in Zimbra Collaboration (ZCS) before 10.0.3. An attacker can gain access to a Zimbra account. This is also fixed in 9.0.0 Patch 35 and 8.8.15 Patch 42.	2023-12-07	7.5	High
CVE-2023-48398	google - android	In ProtocolNetAcBarringInfo::ProtocolNetAcBarringInfo() of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with baseband firmware compromise required. User interaction is not needed for exploitation.	2023-12-08	7.5	High
CVE-2023-48403	google - android	In sms_DecodeCodedTpMsg of sms_PduCodec.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure if the attacker is able to observe the behavior of the subsequent switch conditional with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	7.5	High
CVE-2023-48404	google - android	In ProtocolMiscCarrierConfigSimInfoIndAdapter of protocolmiscadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	7.5	High
CVE-2023-48410	google - android	In cd_ParseMsg of cd_codec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	7.5	High
CVE-2023-48416	google - android	In multiple locations, there is a possible null dereference due to a missing null check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	7.5	High
CVE-2023-38003	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow a user with DATAACCESS privileges to execute routines that they should not have access to. IBM X-Force ID: 260214.	2023-12-04	7.2	High
CVE-2023-44291	dell - powerprotect_data_manager_dm5500_firmware	Dell DM5500 5.14.0.0 contains an OS command injection vulnerability in PPOE component. A remote attacker with high privileges could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker.	2023-12-04	7.2	High
CVE-2023-44221	sonicwall - sma_200_firmware	Improper neutralization of special elements in the SMA100 SSL-VPN management interface allows a remote authenticated attacker with administrative privilege to inject arbitrary commands as a 'nobody' user, potentially leading to OS Command Injection Vulnerability.	2023-12-05	7.2	High
CVE-2023-32268	microfocus - filr	Exposure of Proxy Administrator Credentials An authenticated administrator equivalent Filr user can access the credentials of proxy administrators.	2023-12-06	7.2	High
CVE-2023-32968	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network.	2023-12-08	7.2	High

		We have already fixed the vulnerability in the following versions: QTS 5.0.1.2514 build 20230906 and later QTS 5.1.2.2533 build 20230926 and later QuTS hero h5.0.1.2515 build 20230907 and later QuTS hero h5.1.2.2534 build 20230927 and later			
CVE-2023-32975	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2514 build 20230906 and later QTS 5.1.2.2533 build 20230926 and later QuTS hero h5.0.1.2515 build 20230907 and later QuTS hero h5.1.2.2534 build 20230927 and later	2023-12-08	7.2	High
CVE-2023-6606	linux - linux_kernel	An out-of-bounds read vulnerability was found in smbCalcSize in fs/smb/client/netmisc.c in the Linux Kernel. This issue could allow a local attacker to crash the system or leak internal kernel information.	2023-12-08	7.1	High
CVE-2023-6610	linux - linux_kernel	An out-of-bounds read vulnerability was found in smb2_dump_detail in fs/smb/client/smb2ops.c in the Linux Kernel. This issue could allow a local attacker to crash the system or leak internal kernel information.	2023-12-08	7.1	High
CVE-2023-42561	samsung - multiple products	Heap out-of-bounds write vulnerability in bootloader prior to SMR Dec-2023 Release 1 allows a physical attacker to execute arbitrary code.	2023-12-05	6.8	Medium
CVE-2023-42571	samsung - find_my_mobile	Abuse of remote unlock in Find My Mobile prior to version 7.3.13.4 allows physical attacker to unlock the device remotely by resetting the Samsung Account password with SMS verification when user lost the device.	2023-12-05	6.8	Medium
CVE-2023-42575	samsung - pass	Improper Authentication vulnerability in Samsung Pass prior to version 4.3.00.17 allows physical attackers to bypass authentication due to invalid flag setting.	2023-12-05	6.8	Medium
CVE-2023-42576	samsung - pass	Improper Authentication vulnerability in Samsung Pass prior to version 4.3.00.17 allows physical attackers to bypass authentication due to invalid exception handler.	2023-12-05	6.8	Medium
CVE-2023-44297	dell - poweredge_r660_firmware	Dell PowerEdge platforms 16G Intel E5 BIOS and Dell Precision BIOS, version 1.4.4, contain active debug code security vulnerability. An unauthenticated physical attacker could potentially exploit this vulnerability, leading to information disclosure, information tampering, code execution, denial of service.	2023-12-05	6.8	Medium
CVE-2023-44298	dell - poweredge_r660_firmware	Dell PowerEdge platforms 16G Intel E5 BIOS and Dell Precision BIOS, version 1.4.4, contain active debug code security vulnerability. An unauthenticated physical attacker could potentially exploit this vulnerability, leading to information tampering, code execution, denial of service.	2023-12-05	6.8	Medium
CVE-2023-42722	google - android	In camera service, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with System execution privileges needed	2023-12-04	6.7	Medium
CVE-2023-32848	google - multiple products	In vdec, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08163896; Issue ID: ALPS08163896.	2023-12-04	6.7	Medium
CVE-2023-32849	google - multiple products	In cmdq, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08161758; Issue ID: ALPS08161758.	2023-12-04	6.7	Medium
CVE-2023-32853	google - multiple products	In rpmb, 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: ALPS07648764; Issue ID: ALPS07648764.	2023-12-04	6.7	Medium
CVE-2023-32854	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: ALPS08240132; Issue ID: ALPS08240132.	2023-12-04	6.7	Medium
CVE-2023-32859	google - multiple products	In meta, there is a possible classic buffer overflow 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: ALPS08000473; Issue ID: ALPS08000473.	2023-12-04	6.7	Medium

CVE-2023-32860	google - multiple products	In display, there is a possible classic buffer overflow 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: ALPS07929788; Issue ID: ALPS07929788.	2023-12-04	6.7	Medium
CVE-2023-32861	google - multiple products	In display, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08059081; Issue ID: ALPS08059081.	2023-12-04	6.7	Medium
CVE-2023-32862	google - multiple products	In display, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07388762; Issue ID: ALPS07388762.	2023-12-04	6.7	Medium
CVE-2023-32863	google - multiple products	In display drm, there is a possible out of bounds read 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: ALPS07326314; Issue ID: ALPS07326314.	2023-12-04	6.7	Medium
CVE-2023-32864	google - multiple products	In display drm, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292187; Issue ID: ALPS07292187.	2023-12-04	6.7	Medium
CVE-2023-32865	google - multiple products	In display drm, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363456; Issue ID: ALPS07363456.	2023-12-04	6.7	Medium
CVE-2023-32866	google - multiple products	In mmp, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342152; Issue ID: ALPS07342152.	2023-12-04	6.7	Medium
CVE-2023-32867	google - multiple products	In display drm, 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: ALPS07560793; Issue ID: ALPS07560793.	2023-12-04	6.7	Medium
CVE-2023-32868	google - multiple products	In display drm, 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: ALPS07363632; Issue ID: ALPS07363632.	2023-12-04	6.7	Medium
CVE-2023-32869	google - multiple products	In display drm, 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: ALPS07363632; Issue ID: ALPS07363689.	2023-12-04	6.7	Medium
CVE-2023-32870	google - multiple products	In display drm, there is a possible out of bounds read 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: ALPS07363740; Issue ID: ALPS07363740.	2023-12-04	6.7	Medium
CVE-2023-42557	samsung - multiple products	Out-of-bound write vulnerability in libIfaaCa prior to SMR Dec-2023 Release 1 allows local system attackers to execute arbitrary code.	2023-12-05	6.7	Medium
CVE-2023-42565	samsung - multiple products	Improper input validation vulnerability in Smart Clip prior to SMR Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code.	2023-12-05	6.7	Medium
CVE-2023-48405	google - android	there is a possible way for the secure world to write to NS memory due to a logic error in the code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	6.7	Medium
CVE-2023-48406	google - android	there is a possible permanent DoS or way for the modem to boot unverified firmware due to a logic error in the code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	6.7	Medium
CVE-2023-48414	google - android	In the Pixel Camera Driver, there is a possible use after free due to a logic error in the code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	6.7	Medium
CVE-2023-44306	dell - dm5500_firmware	Dell DM5500 contains a path traversal vulnerability in PPOE Component. A remote attacker with high privileges could potentially exploit this vulnerability to overwrite the files stored on the server filesystem.	2023-12-04	6.5	Medium

CVE-2023-40090	google - multiple products	In BTM_BleVerifySignature of btm_ble.cc, there is a possible way to bypass signature validation due to side channel information disclosure. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	6.5	Medium
CVE-2023-28586	qualcomm - 315_5g_iot_modem_firmware	Information disclosure when the trusted application metadata symbol addresses are accessed while loading an ELF in TEE.	2023-12-05	6.5	Medium
CVE-2023-6512	google - chrome	Inappropriate implementation in Web Browser UI in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to potentially spoof the contents of an iframe dialog context menu via a crafted HTML page. (Chromium security severity: Low)	2023-12-06	6.5	Medium
CVE-2023-48420	google - android	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.	2023-12-08	6.4	Medium
CVE-2023-43102	zimbra - multiple products	An issue was discovered in Zimbra Collaboration (ZCS) before 10.0.4. An XSS issue can be exploited to access the mailbox of an authenticated user. This is also fixed in 8.8.15 Patch 43 and 9.0.0 Patch 36.	2023-12-07	6.1	Medium
CVE-2023-43103	zimbra - multiple products	An XSS issue was discovered in a web endpoint in Zimbra Collaboration (ZCS) before 10.0.4 via an unsanitized parameter. This is also fixed in 8.8.15 Patch 43 and 9.0.0 Patch 36.	2023-12-07	6.1	Medium
CVE-2023-23372	qnap - multiple products	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to inject malicious code via a network. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2425 build 20230609 and later QTS 5.1.0.2444 build 20230629 and later QTS 4.5.4.2467 build 20230718 and later QuTS hero h5.1.0.2424 build 20230609 and later QuTS hero h5.0.1.2515 build 20230907 and later QuTS hero h4.5.4.2476 build 20230728 and later	2023-12-08	6.1	Medium
CVE-2022-48462	google - android	In wifi service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2022-48463	google - android	In wifi service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2022-48464	google - android	In wifi service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42671	google - multiple products	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42672	google - multiple products	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42673	google - multiple products	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42674	google - multiple products	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42675	google - multiple products	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42676	google - multiple products	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42677	google - multiple products	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42678	google - multiple products	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42697	google - multiple products	In omacp service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium

CVE-2023-42698	google - multiple products	In omacp service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42699	google - multiple products	In omacp service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42700	google - multiple products	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42701	google - multiple products	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42702	google - multiple products	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42703	google - multiple products	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42704	google - multiple products	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42705	google - multiple products	In imsservice, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42706	google - multiple products	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42707	google - multiple products	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42708	google - multiple products	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42709	google - multiple products	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42710	google - multiple products	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42711	google - multiple products	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42712	google - multiple products	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42713	google - multiple products	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42714	google - multiple products	In firewall service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42715	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42718	google - multiple products	In dialer, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42719	google - android	In video service, there is a possible out of bounds read due to a incorrect bounds check. This could lead to local denial of service with no additional execution privileges needed	2023-12-04	5.5	Medium

CVE-2023-42720	google - android	In video service, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42721	google - android	In flv extractor, there is a possible missing verification incorrect input. This could lead to local denial of service with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42723	google - android	In camera service, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42728	google - multiple products	In phasecheckserver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42730	google - multiple products	In IMS service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42732	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42733	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42734	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42737	google - multiple products	In telecom service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42741	google - multiple products	In telecom service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42742	google - multiple products	In sysui, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42744	google - multiple products	In telecom service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42749	google - multiple products	In enginnermode service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-44300	dell - powerprotect_data_manager_dm5500_firmware	Dell DM5500 5.14.0.0, contain a Plain-text Password Storage Vulnerability in PPOE. A local attacker with privileges could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	2023-12-04	5.5	Medium
CVE-2023-6460	google - cloud_firestore	A potential logging of the firestore key via logging within nodejs-firestore exists - Developers who were logging objects through this._settings would be logging the firestore key as well potentially exposing it to anyone with logs read access. We recommend upgrading to version 6.1.0 to avoid this issue	2023-12-04	5.5	Medium
CVE-2023-35668	google - multiple products	In visitUris of Notification.java, there is a possible way to display images from another user due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	5.5	Medium
CVE-2023-40073	google - multiple products	In visitUris of Notification.java, there is a possible cross-user media read due to Confused Deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	5.5	Medium
CVE-2023-40074	google - multiple products	In saveToXml of PersistableBundle.java, invalid data could lead to local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	5.5	Medium
CVE-2023-40075	google - multiple products	In forceReplaceShortcutInner of ShortcutPackage.java, there is a possible way to register unlimited packages due to a missing bounds check. This could lead to local denial of service which results in a boot loop with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	5.5	Medium
CVE-2023-40076	google - android	In createPendingIntent of CredentialManagerUi.java, there is a possible way to access credentials from other users due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	5.5	Medium
CVE-2023-40081	google - multiple products	In loadMediaDataInBgForResumption of MediaDataManager.kt, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure	2023-12-04	5.5	Medium

		with no additional execution privileges needed. User interaction is not needed for exploitation.			
CVE-2023-40083	google - multiple products	In parse_gap_data of utils.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	5.5	Medium
CVE-2023-40092	google - multiple products	In verifyShortcutInfoPackage of ShortcutService.java, there is a possible way to see another user's image due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	5.5	Medium
CVE-2023-40098	google - multiple products	In mOnDone of NotificationConversationInfo.java, there is a possible way to access app notification data of another user due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	5.5	Medium
CVE-2023-45781	google - multiple products	In parse_gap_data of utils.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	5.5	Medium
CVE-2023-33070	qualcomm - aqt1000_firmware	Transient DOS in Automotive OS due to improper authentication to the secure IO calls.	2023-12-05	5.5	Medium
CVE-2023-42556	samsung - multiple products	Improper usage of implicit intent in Contacts prior to SMR Dec-2023 Release 1 allows attacker to get sensitive information.	2023-12-05	5.5	Medium
CVE-2023-42564	samsung - multiple products	Improper access control in knoxcustom service prior to SMR Dec-2023 Release 1 allows attacker to send broadcast with system privilege.	2023-12-05	5.5	Medium
CVE-2023-42572	samsung - account_web_software_development_kit	Implicit intent hijacking vulnerability in Samsung Account Web SDK prior to version 1.5.24 allows attacker to get sensitive information.	2023-12-05	5.5	Medium
CVE-2023-42573	samsung - search_widget	PendingIntent hijacking vulnerability in Search Widget prior to version 3.4 in China models allows local attackers to access data.	2023-12-05	5.5	Medium
CVE-2023-49248	huawei - multiple products	Vulnerability of unauthorized file access in the Settings app. Successful exploitation of this vulnerability may cause unauthorized file access.	2023-12-06	5.5	Medium
CVE-2023-48399	google - android	In ProtocolMiscATCommandAdapter::Init() of protocolmiscadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with baseband firmware compromise required. User interaction is not needed for exploitation.	2023-12-08	5.5	Medium
CVE-2023-48401	google - android	In GetSizeOfEenlRecords of protocoladapter.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	5.5	Medium
CVE-2023-48408	google - android	In ProtocolNetSimFileInfoAdapter() of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with baseband firmware compromise required. User interaction is not needed for exploitation.	2023-12-08	5.5	Medium
CVE-2023-48411	google - android	In SignalStrengthAdapter::FillGsmSignalStrength() of protocolmiscadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with baseband firmware compromise required. User interaction is not needed for exploitation.	2023-12-08	5.5	Medium
CVE-2023-48412	google - android	In private_handle_t of mali_gralloc_buffer.h, there is a possible information leak due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	5.5	Medium
CVE-2023-48415	google - android	In Init of protocolembmsadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	5.5	Medium
CVE-2023-48422	google - android	In Init of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	5.5	Medium
CVE-2023-6622	linux - multiple products	A null pointer dereference vulnerability was found in nft_dynset_init() in net/netfilter/nft_dynset.c in nf_tables in the Linux kernel. This issue may allow a local attacker with CAP_NET_ADMIN user privilege to trigger a denial of service.	2023-12-08	5.5	Medium
CVE-2023-6560	linux - multiple products	An out-of-bounds memory access flaw was found in the io_uring SQ/CQ rings functionality in the Linux kernel. This issue could allow a local user to crash the system.	2023-12-09	5.5	Medium
CVE-2023-28526	ibm - multiple products	IBM Informix Dynamic Server 12.10 and 14.10 archecker is vulnerable to a heap buffer overflow, caused by improper bounds	2023-12-09	5.5	Medium

		checking which could allow a local user to cause a segmentation fault. IBM X-Force ID: 251204.			
CVE-2023-28527	ibm - multiple products	IBM Informix Dynamic Server 12.10 and 14.10 cdr is vulnerable to a heap buffer overflow, caused by improper bounds checking which could allow a local user to cause a segmentation fault. IBM X-Force ID: 251206.	2023-12-09	5.5	Medium
CVE-2023-47722	ibm - multiple products	IBM API Connect V10.0.5.3 and V10.0.6.0 stores user credentials in browser cache which can be read by a local user. IBM X-Force ID: 271912.	2023-12-09	5.5	Medium
CVE-2023-50431	linux - linux_kernel	sec_attest_info in drivers/accel/habanalabs/common/habanalabs_ioctl.c in the Linux kernel through 6.6.5 allows an information leak to user space because info->pad0 is not initialized.	2023-12-09	5.5	Medium
CVE-2023-44301	dell - powerprotect_data_manager_dm5500_firmware	Dell DM5500 5.14.0.0 and prior contain a Reflected Cross-Site Scripting Vulnerability. A network attacker with low privileges could potentially exploit this vulnerability, leading to the execution of malicious HTML or JavaScript code in a victim user's web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery.	2023-12-04	5.4	Medium
CVE-2020-25835	microfocus - arcsight_management_center	A potential vulnerability has been identified in Micro Focus ArcSight Management Center. The vulnerability could be remotely exploited resulting in stored Cross-Site Scripting (XSS).	2023-12-09	5.4	Medium
CVE-2023-42579	samsung - multiple products	Improper usage of insecure protocol (i.e. HTTP) in SogouSDK of Chinese Samsung Keyboard prior to versions 5.3.70.1 in Android 11, 5.4.60.49, 5.4.85.5, 5.5.00.58 in Android 12, and 5.6.00.52, 5.6.10.42, 5.7.00.45 in Android 13 allows adjacent attackers to access keystroke data using Man-in-the-Middle attack.	2023-12-05	5.3	Medium
CVE-2023-49282	microsoft - multiple products	msgraph-sdk-php is the Microsoft Graph Library for PHP. The Microsoft Graph PHP SDK published packages which contained test code that enabled the use of the phpInfo() function from any application that could access and execute the file at vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php. The phpInfo function exposes system information. The vulnerability affects the GetPhpInfo.php script of the PHP SDK which contains a call to the phpinfo() function. This vulnerability requires a misconfiguration of the server to be present so it can be exploited. For example, making the PHP application’s /vendor directory web accessible. The combination of the vulnerability and the server misconfiguration would allow an attacker to craft an HTTP request that executes the phpinfo() method. The attacker would then be able to get access to system information like configuration, modules, and environment variables and later on use the compromised secrets to access additional data. This problem has been patched in versions 1.109.1 and 2.0.0-RC5. If an immediate deployment with the updated vendor package is not available, you can perform the following temporary workarounds: delete the `vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php` file, remove access to the `/vendor` directory, or disable the phpinfo function.	2023-12-05	5.3	Medium
CVE-2023-49283	microsoft - graph	microsoft-graph-core the Microsoft Graph Library for PHP. The Microsoft Graph Beta PHP SDK published packages which contained test code that enabled the use of the phpInfo() function from any application that could access and execute the file at `vendor/microsoft/microsoft-graph-core/tests/GetPhpInfo.php`. The phpInfo function exposes system information. The vulnerability affects the GetPhpInfo.php script of the PHP SDK which contains a call to the phpinfo() function. This vulnerability requires a misconfiguration of the server to be present so it can be exploited. For example, making the PHP application’s /vendor directory web accessible. The combination of the vulnerability and the server misconfiguration would allow an attacker to craft an HTTP request that executes the phpinfo() method. The attacker would then be able to get access to system information like configuration, modules, and environment variables and later on use the compromised secrets to access additional data. This problem has been patched in version 2.0.2. If an immediate deployment with the updated vendor package is not available, you can perform the following temporary workarounds: delete the `vendor/microsoft/microsoft-graph-core/tests/GetPhpInfo.php` file, remove access to the /vendor directory, or disable the phpinfo function	2023-12-05	5.3	Medium
CVE-2023-6273	huawei - multiple products	Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally.	2023-12-06	5.3	Medium
CVE-2023-6393	redhat - build_of_quarkus	A flaw was found in the Quarkus Cache Runtime. When request processing utilizes a Uni cached using @CacheResult and the	2023-12-06	5.3	Medium

		cached Uni reuses the initial "completion" context, the processing switches to the cached Uni instead of the request context. This is a problem if the cached Uni context contains sensitive information, and could allow a malicious user to benefit from a POST request returning the response that is meant for another user, gaining access to sensitive data.			
CVE-2023-42559	samsung - multiple products	Improper exception management vulnerability in Knox Guard prior to SMR Dec-2023 Release 1 allows Knox Guard lock bypass via changing system time.	2023-12-05	5.2	Medium
CVE-2023-40053	solarwinds - multiple products	A vulnerability has been identified within Serv-U 15.4 that allows an authenticated actor to insert content on the file share function feature of Serv-U, which could be used maliciously.	2023-12-06	5	Medium
CVE-2023-48397	google - android	In Init of protocolcalladapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	4.9	Medium
CVE-2023-48413	google - android	In Init of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	4.9	Medium
CVE-2023-36880	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2023-12-07	4.8	Medium
CVE-2023-42679	google - android	In gpu driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-12-04	4.4	Medium
CVE-2023-42680	google - android	In gpu 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	2023-12-04	4.4	Medium
CVE-2023-42682	google - multiple products	In gsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-12-04	4.4	Medium
CVE-2023-42683	google - multiple products	In gsp 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	2023-12-04	4.4	Medium
CVE-2023-42684	google - multiple products	In gsp 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	2023-12-04	4.4	Medium
CVE-2023-42724	google - android	In gpu 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	2023-12-04	4.4	Medium
CVE-2023-42725	google - android	In gpu 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	2023-12-04	4.4	Medium
CVE-2023-42726	google - android	In TeleService, 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	2023-12-04	4.4	Medium
CVE-2023-42727	google - multiple products	In gpu driver, there is a possible out of bounds write due to a incorrect bounds check. This could lead to local denial of service with System execution privileges needed	2023-12-04	4.4	Medium
CVE-2023-42729	google - multiple products	In ril service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-12-04	4.4	Medium
CVE-2023-42731	google - multiple products	In Gnss service, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-12-04	4.4	Medium
CVE-2023-42735	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed	2023-12-04	4.4	Medium
CVE-2023-42751	google - multiple products	In gnss service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-12-04	4.4	Medium
CVE-2023-32852	google - multiple products	In cameraisp, 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: ALPS07670971; Issue ID: ALPS07670971.	2023-12-04	4.4	Medium
CVE-2023-32856	google - multiple products	In display, there is a possible out of bounds read due to an incorrect status check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07993705; Issue ID: ALPS07993705.	2023-12-04	4.4	Medium
CVE-2023-32857	google - multiple products	In display, there is a possible out of bounds read due to an incorrect status check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07993705; Issue ID: ALPS07993710.	2023-12-04	4.4	Medium
CVE-2023-32858	google - android	In GZ, there is a possible information disclosure due to a missing data erasing. This could lead to local information disclosure with System execution privileges needed. User interaction is not	2023-12-04	4.4	Medium

		needed for exploitation. Patch ID: ALPS07806008; Issue ID: ALPS07806008.			
CVE-2023-42568	samsung - multiple products	Improper access control vulnerability in SmartManagerCN prior to SMR Dec-2023 Release 1 allows local attackers to access arbitrary files with system privilege.	2023-12-05	4.4	Medium
CVE-2023-6511	google - chrome	Inappropriate implementation in Autofill in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to bypass Autofill restrictions via a crafted HTML page. (Chromium security severity: Low)	2023-12-06	4.3	Medium
CVE-2023-38174	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2023-12-07	4.3	Medium
CVE-2023-42569	samsung - multiple products	Improper authorization verification vulnerability in AR Emoji prior to SMR Dec-2023 Release 1 allows attackers to read sandbox data of AR Emoji.	2023-12-05	3.3	Low
CVE-2023-42570	samsung - multiple products	Improper access control vulnerability in KnoxCustomManagerService prior to SMR Dec-2023 Release 1 allows attacker to access device SIM PIN.	2023-12-05	3.3	Low
CVE-2023-42577	samsung - samsung_voice_recorder	Improper Access Control in Samsung Voice Recorder prior to versions 21.4.15.01 in Android 12 and Android 13, 21.4.50.17 in Android 14 allows physical attackers to access Voice Recorder information on the lock screen.	2023-12-05	2.4	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.