

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 Please note that this notification/advisory has been tagged as TLP خلال القنوات العامة.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني للمساعدة في حماية الفضاء السيبراني protecting national interests, NCA provides the weekly summary of the National الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للشغرات المسجلة من قبل published vulnerabilities by the National Institute of Standards and Institute of Standards and Technology (NIST) National Technology (NIST) National Vulnerability Database (NVD) for the للأسبوع من 3 ديسمبر إلى 9 ديسمبر إلى 9 ديسمبر إلى 9 ديسمبر الله علماً أنه week from 3rd of December to 9th of December. Vulnerabilities are Common Vulnerability Scoring يتم تصنيف هذه الثغراتُ باستخدام معيار 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

System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

عالى جدًا: النتيجة الأساسية لـ10.0-CVSS 9.0-10.0

عالى: النتيجة الأساسية لـ2.8-7.0 CVSS

متوسط: النتيجة الأساسية لـ6.9-CVSS 4.0

منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

CVE ID &				CVS	
Source	Vendor - Product	Description	Publish Date	S	Severity
				Score	
		Dell DM5500 5.14.0.0 and prior contain an improper			
	dell -	authentication vulnerability. A remote unauthenticated attacker			
	powerprotect_data	could potentially exploit this vulnerability to gain access of			
	_manager_dm5500	resources or functionality that could possibly lead to execute			
CVE-2023-44302	_firmware	arbitrary code.	2023-12-04	9.8	Critical
		Dell DM5500 5.14.0.0, contains a Stack-based Buffer Overflow			
		Vulnerability in PPOE. An unauthenticated remote attacker may			
	dell -	exploit this vulnerability to crash the affected process or execute			
CVE-2023-44305	dm5500_firmware	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
		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			
CVE-2023-40078	google - android	privileges needed. User interaction is not needed for exploitation.	2023-12-04	9.8	Critical
CVL 2023 40070	googie unaroid	In modify_for_next_stage of fdt.rs, there is a possible way to	2023 12 04	3.0	Critical
		render KASLR ineffective due to improperly used crypto. This could			
		lead to remote escalation of privilege with no additional execution			
CVE-2023-40082	google - android	privileges needed. User interaction is not needed for exploitation.	2023-12-04	9.8	Critical
	<u> </u>	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			
	microsoft -	RTOS v6.2.1 and below. The fixes have been included in NetX Duo			
	azure_rtos_netx_d	release 6.3.0. Users are advised to upgrade. There are no known			
CVE-2023-48315	uo	workarounds for this vulnerability.	2023-12-05	9.8	Critical
		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			
	microsoft -	overflow vulnerabilities in Azure RTOS NETX Duo. The affected			
	azure_rtos_netx_d	components include processes/functions related to snmp, smtp,			_
CVE-2023-48316	uo	ftp and dtls in RTOS v6.2.1 and below. The fixes have been	2023-12-05	9.8	Critical

	<u> </u>	included in NetX Duo release 6.3.0. Users are advised to upgrade.			
		There are no known workarounds for this vulnerability.			
		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			
	microsoft -	v6.2.1 and below. The fix has been included in NetX Duo release			
	azure_rtos_netx_d	6.3.0. Users are advised to upgrade. There are no known			
CVE-2023-48691	uo	workarounds for this vulnerability.	2023-12-05	9.8	Critical
		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,			
	microsoft -	snmp, dhcp, nat and ftp in RTOS v6.2.1 and below. The fixes have			
CVE 2022 49C02	azure_rtos_netx_d	been included in NetX Duo release 6.3.0. Users are advised to	2022 12 05	0.0	Cuitinal
CVE-2023-48692	uo	upgrade. There are no known workarounds for this vulnerability. Azure RTOS ThreadX is an advanced real-time operating system	2023-12-05	9.8	Critical
		(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			
	microsoft -	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			
CVE-2023-48693	azure_rtos_threadx	known workarounds for this vulnerability.	2023-12-05	9.8	Critical
		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			
C) /F 2022 40C04	microsoft -	to upgrade. There are no known workarounds for this	2022 42 05	0.0	Californi
CVE-2023-48694	azure_rtos_usbx	vulnerability. Azure RTOS USBX is a USB host, device, and on-the-go (OTG)	2023-12-05	9.8	Critical
		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			
	microsoft -	advised to upgrade. There are no known workarounds for this			
CVE-2023-48695	azure_rtos_usbx	vulnerability.	2023-12-05	9.8	Critical
		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			
0)/5 2022 :::::	microsoft -	in USBX release 6.3.0. Users are advised to upgrade. There are no	2020 15 5=		.
CVE-2023-48696	azure_rtos_usbx	known workarounds for this vulnerability.	2023-12-05	9.8	Critical
		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			
	microsoft -	USBX release 6.3.0. Users are advised to upgrade. There are no			
CVE-2023-48697	azure_rtos_usbx	known workarounds for this vulnerability.	2023-12-05	9.8	Critical
	_ _	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			
01/5 2022 1255	microsoft -	release 6.3.0. Users are advised to upgrade. There are no known	2020 15 5=	. .	.
CVE-2023-48698	azure_rtos_usbx	workarounds for this vulnerability. Mamory corruption while conding an Assoc Request having RTM	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
<u> </u>	qualcomm -	Memory corruption in WLAN Host while processing RRM beacon	2020 12 00	5.0	Sittlean
CVE-2023-33083	ar8035_firmware	on the AP.	2023-12-05	9.8	Critical
		Improper URL validation from MCSLaunch deeplink in Galaxy Store			
CVE 2022 42500	samsung -	prior to version 4.5.64.4 allows attackers to execute JavaScript API	2022 42 05	0.0	Cutation
CVE-2023-42580	galaxy_store	to install APK from Galaxy Store.	2023-12-05	9.8	Critical

		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.			
CVE-2023-49070	apache - ofbiz	Users are recommended to upgrade to version 18.12.10 Improper input validation vulnerability in Samsung Open Source	2023-12-05	9.8	Critical
	samsung - multiple	Escargot allows stack overflow and segmentation fault. This issue			
CVE-2023-41268	products	affects Escargot: from 3.0.0 through 4.0.0. Certain versions of the Atlassian Companion App for MacOS were	2023-12-06	9.8	Critical
		affected by a remote code execution vulnerability. An attacker			
CVE 2022 22524	atlassian -	could utilize WebSockets to bypass Atlassian Companion's blocklist	2022 42 06	0.0	California
CVE-2023-22524	companion	and MacOS Gatekeeper to allow execution of code. Permission management vulnerability in the PMS module.	2023-12-06	9.8	Critical
		Successful exploitation of this vulnerability may cause privilege			
CVE-2023-46773	huawei - emui	escalation. An attacker can manipulate file upload params to enable paths	2023-12-06	9.8	Critical
		traversal and under some circumstances this can lead to uploading			
		a malicious file which can be used to perform Remote Code Execution.			
	apache - multiple	Users are recommended to upgrade to versions Struts 2.5.33 or			
CVE-2023-50164	products	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
<u> </u>	151750_IIIIIIWale	In dhcp4_SetPDNAddress of dhcp4_Main.c, there is a possible out	2023 12 00	5.0	Circical
		of bounds write due to a missing bounds check. This could lead to			
CVE-2023-48423	google - android	remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	9.8	Critical
	8.00	An OS Command Injection in the CLI interface on DrayTek Vigor167			
	draytek -	version 5.2.2, allows remote attackers to execute arbitrary system commands and escalate privileges via any account created within			
CVE-2023-47254	vigor167_firmware	the web interface.	2023-12-09	9.8	Critical
	microsoft -	Microsoft Edge (Chromium-based) Elevation of Privilege			
CVE-2023-35618	edge_chromium qualcomm -	Vulnerability	2023-12-07	9.6	Critical
	315_5g_iot_mode	Cryptographic issue in GPS HLOS Driver while downloading			
CVE-2023-33054	m_firmware	Qualcomm GNSS assistance data.	2023-12-05	9.1	Critical
		Dell DM5500 contains a privilege escalation vulnerability in PPOE			
		Component. A remote attacker with low privileges could			
CVE 2022 44204	dell - dm5500 firmware	potentially exploit this vulnerability to escape the restricted shell	2023-12-04	8.8	Lligh
CVE-2023-44304	diff5500_fifffiware	and gain root access to the appliance. In transcodeQ*ToFloat of btif avrcp audio track.cc, there is a	2023-12-04	0.0	High
		possible out of bounds write due to a missing bounds check. This			
	google - multiple	could lead to paired device escalation of privilege with no additional execution privileges needed. User interaction is not			
CVE-2023-40087	products	needed for exploitation.	2023-12-04	8.8	High
		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			
CVE-2023-40088	google - multiple products	additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	8.8	High
<u> </u>	qualcomm -	necessarion exploitation.	2020 12 04	0.0	111811
OVE 2022 20525	315_5g_iot_mode	Management and the landing of the la	2022 42 25	0.0	11:-1-
CVE-2023-28585	m_firmware	Memory corruption while loading an ELF segment in TEE Kernel. Improper authentication in the SMA100 SSL-VPN virtual office	2023-12-05	8.8	High
		portal allows a remote authenticated attacker to create an			
CVE-2023-5970	sonicwall - sma_200_firmware	identical external domain user using accent characters, resulting in an MFA bypass.	2023-12-05	8.8	High
CVL-2023-33/U	Sina_200_illiliwale	Use after free in Media Stream in Google Chrome prior to	7072-17-02	0.0	ııığıı
		120.0.6099.62 allowed a remote attacker to potentially exploit			
CVE-2023-6508	google - chrome	heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-12-06	8.8	High
	55-2 Smorrie	Use after free in Side Panel Search in Google Chrome prior to		3.5	
		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:			
CVE-2023-6509	google - chrome	High)	2023-12-06	8.8	High
		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			
OVE 2022 ST 12		corruption via specific UI interaction. (Chromium security severity:	2022 42 25		
CVE-2023-6510	google - chrome	Medium) This Template Injection vulnerability allows an authenticated	2023-12-06	8.8	High
		attacker, including one with anonymous access, to inject unsafe			
	atlaccian multiple	user input into a Confluence page. Using this approach, an			
CVE-2023-22522	atlassian - multiple products	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
J. L LULU LLULL	p. 00000		5_5 _2 50		ייסייי ו

		Server versions as listed below are at risk and require immediate attention. See the advisory for additional details			
	atlassian - multiple	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. 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			
CVE-2023-22523	products	Discovery) and the Assets Discovery agent.	2023-12-06	8.8	High
		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.			
CVE-2023-6514	huawei - ajmd- 370s_firmware	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. 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:	2023-12-08	8.8	High
CVE-2023-47565	qnap - qvr_firmware	QVR Firmware 5.0.0 and later	2023-12-08	8.8	High
CVE-2023-47363	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.	2023-12-08	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. In ion service, there is a possible missing permission check. This	2023-12-05	8.1	High
CVE-2023-42681	google - multiple products	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 In wifi service, there is a possible missing permission check. This	2023-12-04	7.8	High
CVE-2023-42686	google - android	could lead to local escalation of privilege with no additional execution privileges needed In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional	2023-12-04	7.8	High
CVE-2023-42687	google - android	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 In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional	2023-12-04	7.8	High
CVE-2023-42690	google - android	could lead to local escalation of privilege with no additional execution privileges needed In wifi service, there is a possible missing permission check. This	2023-12-04	7.8	High
CVE-2023-42691	google - multiple products	could lead to local escalation of privilege with no additional execution privileges needed	2023-12-04	7.8	High
		In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional			
CVE-2023-42692	google - android	execution privileges needed In wifi service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional	2023-12-04	7.8	High
CVE-2023-42693	google - android	execution privileges needed In wifi service, there is a possible missing permission check. This	2023-12-04	7.8	High
CVE-2023-42694	google - android	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 In telecom service, there is a possible way to write permission	2023-12-04	7.8	High
CVE-2023-42740	google - multiple products	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 In camera service, there is a possible missing permission check.	2023-12-04	7.8	High
CVE-2023-42747	google - multiple products	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 google - multiple	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. 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:	2023-12-04	7.8	High
CVE-2023-32850	products	ALPS08016659. 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	2023-12-04	7.8	High
CVE-2023-32851	google - multiple products	needed for exploitation. Patch ID: ALPS08016652; Issue ID: ALPS08016652. 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	2023-12-04	7.8	High
CVE-2023-40079	google - android google - multiple	execution privileges needed. User interaction is not needed for exploitation. 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	2023-12-04	7.8	High
CVE-2023-40080	products google - multiple	needed. User interaction is not needed for exploitation. 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	2023-12-04	7.8	High
CVE-2023-40084	products	needed. User interaction is not needed for exploitation. 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	2023-12-04	7.8	High
CVE-2023-40089	google - android	interaction is not needed for exploitation. In onTransact of IncidentService.cpp, there is a possible out of	2023-12-04	7.8	High
CVE-2023-40091	google - multiple products	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. 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	2023-12-04	7.8	High
CVE-2023-40094	google - multiple products	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

	T				
		In createDontSendToRestrictedAppsBundle of			
		PendingIntentUtils.java, there is a possible background activity			
	1 11	launch due to a missing check. This could lead to local escalation of			
CVE 2022 4000E	google - multiple	privilege with no additional execution privileges needed. User	2022 42 04	7.0	112.1.
CVE-2023-40095	products	interaction is not needed for exploitation.	2023-12-04	7.8	High
		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			
CVE 2022 40006	google - multiple	with User execution privileges needed. User interaction is not	2022 12 04	7.0	Hiah
CVE-2023-40096	products	needed for exploitation.	2023-12-04	7.8	High
		In hasPermissionForActivity of PackageManagerHelper.java, there			
		is a possible URI grant due to improper input validation. This could			
0.45 2022 40007	google - multiple	lead to local escalation of privilege with no additional execution	2022 42 04	7.0	
CVE-2023-40097	products	privileges needed. User interaction is needed for exploitation.	2023-12-04	7.8	High
		In multiple locations, there is a possible way to corrupt memory			
		due to a double free. This could lead to local escalation of privilege			
0) /5 2022 40402		with no additional execution privileges needed. User interaction is	2022 42 04	7.0	
CVE-2023-40103	google - android	not needed for exploitation.	2023-12-04	7.8	High
		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			
	google - multiple	local escalation of privilege with User execution privileges needed.			
CVE-2023-45773	products	User interaction is not needed for exploitation.	2023-12-04	7.8	High
		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			
	google - multiple	additional execution privileges needed. User interaction is not			
CVE-2023-45774	products	needed for exploitation.	2023-12-04	7.8	High
		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			
CVE-2023-45775	google - android	needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
		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			
CVE-2023-45776	google - android	needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
		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			
	google - multiple	execution privileges needed. User interaction is not needed for			
CVE-2023-45777	products	exploitation.	2023-12-04	7.8	High
		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			
CVE-2023-45779	google - android	needed. User interaction is not needed for exploitation.	2023-12-04	7.8	High
	qualcomm -	Memory Corruption in Radio Interface Layer while sending an SMS			
CVE-2023-21634	aqt1000_firmware	or writing an SMS to SIM.	2023-12-05	7.8	High
	qualcomm -	Memory Corruption in camera while installing a fd for a particular			
CVE-2023-22383	aqt1000_firmware	DMA buffer.	2023-12-05	7.8	High
	qualcomm -	Memory Corruption in Audio while invoking IOCTLs calls from the			
CVE-2023-22668	aqt1000_firmware	user-space.	2023-12-05		High
	qualcomm -	·		7.8	111611
	•			7.8	111811
	315 5g iot mode	Memory Corruption in SPS Application while exporting public key		7.8	111611
CVE-2023-28546	315_5g_iot_mode m firmware	Memory Corruption in SPS Application while exporting public key in sorter TA.	2023-12-05		
CVE-2023-28546	m_firmware	Memory Corruption in SPS Application while exporting public key in sorter TA.	2023-12-05	7.8	High
CVE-2023-28546	m_firmware qualcomm -	in sorter TA.	2023-12-05		
	m_firmware qualcomm - 315_5g_iot_mode	in sorter TA. Memory corruption in MPP performance while accessing DSM		7.8	High
	m_firmware qualcomm - 315_5g_iot_mode m_firmware	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address.	2023-12-05		
	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm -	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory		7.8	High
CVE-2023-28550	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input	2023-12-05	7.8	High High
CVE-2023-28550	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory		7.8	High
CVE-2023-28550	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm -	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments.	2023-12-05	7.8	High High
CVE-2023-28550 CVE-2023-28551	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input	2023-12-05 2023-12-05	7.8 7.8 7.8	High High High
CVE-2023-28550 CVE-2023-28551	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length.	2023-12-05	7.8	High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm -	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in	2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8	High High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - qualcomm - ar8035_firmware	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length.	2023-12-05 2023-12-05	7.8 7.8 7.8	High High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - ar8035_firmware qualcomm -	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache.	2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8	High High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579 CVE-2023-28580	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - ar8035_firmware qualcomm - ar8035_firmware	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache. Memory corruption in BT controller while parsing debug	2023-12-05 2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8 7.8	High High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579 CVE-2023-28580	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - ar8035_firmware qualcomm - 315_5g_iot_mode m_firmware	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache.	2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8	High High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579 CVE-2023-28580	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - ar8035_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm -	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache. Memory corruption in BT controller while parsing debug commands with specific sub-opcodes at HCI interface level.	2023-12-05 2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8 7.8	High High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579 CVE-2023-28580 CVE-2023-28587	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - ar8035_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm -	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache. Memory corruption in BT controller while parsing debug commands with specific sub-opcodes at HCI interface level. Memory corruption in Boot while running a ListVars test in UEFI	2023-12-05 2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8 7.8 7.8	High High High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579 CVE-2023-28580 CVE-2023-28587	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - ar8035_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache. Memory corruption in BT controller while parsing debug commands with specific sub-opcodes at HCI interface level.	2023-12-05 2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8 7.8	High High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579 CVE-2023-28580 CVE-2023-28587	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - ar8035_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm -	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache. Memory corruption in BT controller while parsing debug commands with specific sub-opcodes at HCI interface level. Memory corruption in Boot while running a ListVars test in UEFI Menu during boot.	2023-12-05 2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8 7.8 7.8	High High High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579 CVE-2023-28580 CVE-2023-28587 CVE-2023-33017	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - ar8035_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm -	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache. Memory corruption in BT controller while parsing debug commands with specific sub-opcodes at HCI interface level. Memory corruption in Boot while running a ListVars test in UEFI Menu during boot. Memory corruption while using the UIM diag command to get the	2023-12-05 2023-12-05 2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8 7.8 7.8 7.8 7.8	High High High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579 CVE-2023-28580 CVE-2023-28587 CVE-2023-33017	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - ar8035_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm -	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache. Memory corruption in BT controller while parsing debug commands with specific sub-opcodes at HCI interface level. Memory corruption in Boot while running a ListVars test in UEFI Menu during boot.	2023-12-05 2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8 7.8 7.8	High High High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579 CVE-2023-28580 CVE-2023-28587 CVE-2023-33017	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - ar8035_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - qualcomm -	Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache. Memory corruption in BT controller while parsing debug commands with specific sub-opcodes at HCI interface level. Memory corruption in Boot while running a ListVars test in UEFI Menu during boot. Memory corruption while using the UIM diag command to get the operators name.	2023-12-05 2023-12-05 2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8 7.8 7.8 7.8 7.8	High High High High
CVE-2023-28587 CVE-2023-33017 CVE-2023-33018	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - ar8035_firmware qualcomm - 315_5g_iot_mode m_firmware	in sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache. Memory corruption in BT controller while parsing debug commands with specific sub-opcodes at HCI interface level. Memory corruption in Boot while running a ListVars test in UEFI Menu during boot. Memory corruption while using the UIM diag command to get the	2023-12-05 2023-12-05 2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8 7.8 7.8 7.8 7.8	High High High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579 CVE-2023-28580 CVE-2023-28587 CVE-2023-33017	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - ar8035_firmware qualcomm - 315_5g_iot_mode m_firmware	Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache. Memory corruption in BT controller while parsing debug commands with specific sub-opcodes at HCI interface level. Memory corruption in Boot while running a ListVars test in UEFI Menu during boot. Memory corruption while using the UIM diag command to get the operators name.	2023-12-05 2023-12-05 2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8 7.8 7.8 7.8 7.8	High High High High
CVE-2023-28550 CVE-2023-28551 CVE-2023-28579 CVE-2023-28580 CVE-2023-28587 CVE-2023-33017 CVE-2023-33018	m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - 315_5g_iot_mode m_firmware qualcomm - fastconnect_6900_f irmware qualcomm - ar8035_firmware qualcomm - 315_5g_iot_mode m_firmware	In sorter TA. Memory corruption in MPP performance while accessing DSM watermark using external memory address. Memory corruption in UTILS when modem processes memory specific Diag commands having arbitrary address values as input arguments. Memory Corruption in WLAN Host while deserializing the input PMK bytes without checking the input PMK length. Memory corruption in WLAN Host while setting the PMK length in PMK length in internal cache. Memory corruption in BT controller while parsing debug commands with specific sub-opcodes at HCI interface level. Memory corruption in Boot while running a ListVars test in UEFI Menu during boot. Memory corruption while using the UIM diag command to get the operators name. Memory corruption in HLOS while invoking IOCTL calls from user-	2023-12-05 2023-12-05 2023-12-05 2023-12-05 2023-12-05 2023-12-05	7.8 7.8 7.8 7.8 7.8 7.8 7.8 7.8	High High High High High High

				 	
CVE-2023-33053	qualcomm - csr8811_firmware qualcomm -	Memory corruption in Kernel while parsing metadata.	2023-12-05	7.8	High
CVE-2023-33063	315_5g_iot_mode m_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
	qualcomm - 315_5g_iot_mode	Memory corruption when processing cmd parameters while			
CVE-2023-33088 CVE-2023-33092	m_firmware qualcomm - aqt1000_firmware	parsing vdev. 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 7.8	High 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
	qualcomm -			- 10	6
CVE-2023-33107	315_5g_iot_mode m_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. Integer overflow vulnerability in	2023-12-05	7.8	High
CVE-2023-42562	samsung - multiple products	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
0) (5, 2022, 42567	samsung - multiple	Improper size check vulnerability in softsimd prior to SMR Dec-	2022 42 05	7.0	
CVE-2023-42567	products samsung -	2023 Release 1 allows stack-based buffer overflow. Improper access control vulnerablility in GameHomeCN prior to version 4.2.60.2 allows local attackers to launch arbitrary activity	2023-12-05	7.8	High
CVE-2023-42574	gamehomecn	in GameHomeCN.	2023-12-05	7.8	High
	dell -	Dell PowerEdge BIOS contains an improper privilege management			
CVE 2022 22460	poweredge_r660_fi	security vulnerability. An unauthenticated local attacker could	2022 42 00	7.0	11: -1-
CVE-2023-32460	rmware	potentially exploit this vulnerability, leading to privilege escalation. In ppcfw_enable of ppcfw.c, there is a possible EoP due to a missing permission check. This could lead to local escalation of	2023-12-08	7.8	High
CVE-2023-48402	google - android	privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	7.8	High
<u> </u>	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	2023-12-08	7.8	Tilgii
CVE-2023-48407	google - android	privilege with no additional execution privileges needed. User interaction is not needed for exploitation. In gpu_pixel_handle_buffer_liveness_update_ioctl of	2023-12-08	7.8	High
		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			
CVE-2023-48409	google - android	privileges needed. User interaction is not needed for exploitation. In gpu pixel handle buffer liveness update ioctl of	2023-12-08	7.8	High
		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.			
CVE-2023-48421	google - android	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
	ibm - multiple	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.			
CVE-2023-28523	products	IBM X-Force ID: 250753. IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect	2023-12-09	7.8	High
CVE-2023-45178	ibm - multiple products	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
01/5 0055 155	ibm - multiple	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, 11.5 is vulnerable to denial of service under	0005 1		
CVE-2023-40692	products	extreme stress conditions. IBM X-Force ID: 264807. In telephony service, there is a possible missing permission check.	2023-12-04	7.5	High
CVE-2023-42716	google - multiple products	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
		IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect			
CVE-2023-46167	ibm - db2	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
	ibm - multiple	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			
CVE-2023-47701	products	specially crafted query. IBM X-Force ID: 266166.	2023-12-04	7.5	High
		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			
CVE-2023-29258	ibm - multiple products	specially crafted federated query on specific federation objects. IBM X-Force ID: 252048.	2023-12-04	7.5	High
011 1010 13100		IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect		7.13	
CVE-2023-38727	ibm - multiple products	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
		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			
	ibm - multiple	specially crafted RUNSTATS command on an 8TB table. IBM X-			
CVE-2023-40687 CVE-2023-21227	products google - android	Force ID: 264809. There is information disclosure.	2023-12-04 2023-12-04	7.5 7.5	High High
	qualcomm -				
CVE-2023-28588	apq8017_firmware qualcomm -	Transient DOS in Bluetooth Host while rfc slot allocation. Under certain scenarios the WLAN Firmware will reach an	2023-12-05	7.5	High
CVE-2023-33041	ar8035_firmware	assertion due to state confusion while looking up peer ids.	2023-12-05	7.5	High
	qualcomm - 315_5g_iot_mode				
CVE-2023-33042	m_firmware qualcomm -	Transient DOS in Modem after RRC Setup message is received. Transient DOS in Modem when a Beam switch request is made	2023-12-05	7.5	High
CVE-2023-33043	ar8035_firmware	with a non-configured BWP.	2023-12-05	7.5	High
	qualcomm - 315_5g_iot_mode	Transient DOS in Data modem while handling TLB control			
CVE-2023-33044	m_firmware	messages from the Network.	2023-12-05	7.5	High
	qualcomm - 315_5g_iot_mode	Transient DOS while parsing a vender specific IE (Information			
CVE-2023-33080	m_firmware	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
	qualcomm - 315_5g_iot_mode	Transient DOS when processing a NULL buffer while parsing WLAN			
CVE-2023-33089	m_firmware	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
	qualcomm - 315_5g_iot_mode	Transient DOS while parsing WPA IES, when it is passed with			
CVE-2023-33098	m_firmware	length more than expected size.	2023-12-05	7.5	High
		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			
CVE-2023-42578	samsung - cloud	permission. Improper URL validation from InstantPlay deeplink in Galaxy Store	2023-12-05	7.5	High
CVE-2023-42581	samsung - galaxy_store	prior to version 4.5.64.4 allows attackers to execute JavaScript API to access data.	2023-12-05	7.5	High
CVL-2023-42361	galaxy_store		2023-12-03	7.5	- I ligii
		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			
	dell -	severity vulnerability as it allows an attacker to cause an outage of network. Dell recommends customers to upgrade at the earliest			
CVE-2023-39248	networking_os10	opportunity.	2023-12-05	7.5	High
		Dell PowerScale OneFS, 8.2.2.x through 9.6.0.x, contains an			
	dell -	improper control of a resource through its lifetime vulnerability. An unauthenticated network attacker could potentially exploit this			
CVE-2023-44288	powerscale_onefs	vulnerability, leading to denial of service.	2023-12-05	7.5	High
		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.			
CVE-2023-41835	apache - multiple products	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
	·	Vulnerability of data verification errors in the kernel module.			
CVE-2023-44099	huawei - emui	Successful exploitation of this vulnerability may cause WLAN interruption.	2023-12-06	7.5	High
		Vulnerability of missing permission verification for APIs in the Designed for Reliability (DFR) module. Successful exploitation of			
CVE-2023-44113	huawei - emui	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. An issue was discovered in Zimbra Collaboration (ZCS) before	2023-12-06	7.5	High
CVE-2023-41106	zimbra - multiple products	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
		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			
CVE-2023-48398	google - android	required. User interaction is not needed for exploitation. 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	2023-12-08	7.5	High
CVE-2023-48403	google - android	needed for exploitation. In ProtocolMiscCarrierConfigSimInfoIndAdapter of protocolmiscadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote	2023-12-08	7.5	High
CVE-2023-48404	google - android	information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. In cd_ParseMsg of cd_codec.c, there is a possible out of bounds	2023-12-08	7.5	High
CVE-2023-48410	google - android	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. In multiple locations, there is a possible null dereference due to a	2023-12-08	7.5	High
CVE-2023-48416	google - android	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
	dell - powerprotect_data manager_dm5500	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			
CVE-2023-44291	firmware	to a system take over by an attacker. Improper neutralization of special elements in the SMA100 SSL-VPN management interface allows a remote authenticated	2023-12-04	7.2	High
VE-2023-44221	sonicwall - sma_200_firmware	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
N/E 2022 2222		Exposure of Proxy Administrator Credentials An authenticated administrator equivalent Filr user can access the	2022 12 22	7.0	
CVE-2023-32268	microfocus - filr	credentials of proxy administrators. A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If	2023-12-06	7.2	High
CVE-2023-32968	qnap - multiple products	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			
		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			
	anon multiple	QTS 5.1.2.2533 build 20230926 and later QuTS hero h5.0.1.2515 build 20230907 and later			
CVE-2023-32975	qnap - multiple products	QuTS hero h5.1.2.2534 build 20230927 and later	2023-12-08	7.2	High
<u>CVL 2023 32373</u>	products	An out-of-bounds read vulnerability was found in smbCalcSize in	2023 12 00	7.2	111611
		fs/smb/client/netmisc.c in the Linux Kernel. This issue could allow			
		a local attacker to crash the system or leak internal kernel			
CVE-2023-6606	linux - linux_kernel	information.	2023-12-08	7.1	High
		An out-of-bounds read vulnerability was found in			
		smb2_dump_detail in fs/smb/client/smb2ops.c in the Linux			
CVE 2022 CC10	limono limono lommal	Kernel. This issue could allow a local attacker to crash the system	2022 12 00	7.1	Hiah
CVE-2023-6610	linux - linux_kernel	or leak internal kernel information. Heap out-of-bounds write vulnerability in bootloader prior to SMR	2023-12-08	7.1	High
	samsung - multiple	Dec-2023 Release 1 allows a physical attacker to execute arbitrary			
CVE-2023-42561	products	code.	2023-12-05	6.8	Medium
<u> </u>	products	Abuse of remote unlock in Find My Mobile prior to version	2023 12 03	0.0	Wiediaiii
		7.3.13.4 allows physical attacker to unlock the device remotely by			
	samsung -	resetting the Samsung Account password with SMS verification			
CVE-2023-42571	find_my_mobile	when user lost the device.	2023-12-05	6.8	Medium
		Improper Authentication vulnerability in Samsung Pass prior to			
		version 4.3.00.17 allows physical attackers to bypass			
CVE-2023-42575	samsung - pass	authentication due to invalid flag setting.	2023-12-05	6.8	Medium
		Improper Authentication vulnerability in Samsung Pass prior to			
CVE-2023-42576	samsung - pass	version 4.3.00.17 allows physical attackers to bypass authentication due to invalid exception handler.	2023-12-05	6.8	Medium
CVL-2023-42370	Sattisutig - pass	authentication due to invalid exception handler.	2023-12-03	0.8	Mediaiii
		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			
	dell -	potentially exploit this vulnerability, leading to information			
	poweredge_r660_fi	disclosure, information tampering, code execution, denial of			
CVE-2023-44297	rmware	service.	2023-12-05	6.8	Medium
		Dell PowerEdge platforms 16G Intel E5 BIOS and Dell Precision			
		BIOS, version 1.4.4, contain active debug code security			
	dell -	vulnerability. An unauthenticated physical attacker could			
	poweredge_r660_fi	potentially exploit this vulnerability, leading to information			
CVE-2023-44298	rmware	tampering, code execution, denial of service.	2023-12-05	6.8	Medium
		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			
CVE-2023-42722	google - android	execution privileges needed	2023-12-04	6.7	Medium
		In vdec, there is a possible out of bounds write due to type			
		confusion. This could lead to local escalation of privilege with			
	googlo multiple	System execution privileges needed. User interaction is not			
CVE-2023-32848	google - multiple products	needed for exploitation. Patch ID: ALPS08163896; Issue ID: ALPS08163896.	2023-12-04	6.7	Medium
CVL 2023 32040	products	In cmdq, there is a possible out of bounds write due to type	2023 12 04	0.7	Wicalam
		confusion. This could lead to local escalation of privilege with			
		System execution privileges needed. User interaction is not			
	google - multiple	needed for exploitation. Patch ID: ALPS08161758; Issue ID:			
CVE-2023-32849	products	ALPS08161758.	2023-12-04	6.7	Medium
		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			
	l let l	System execution privileges needed. User interaction is not			
CVE 2022 220E2	google - multiple	needed for exploitation. Patch ID: ALPS07648764; Issue ID:	2022 12 04	6.7	Madium
CVE-2023-32853	products	ALPS07648764. In ril, there is a possible out of bounds write due to a missing	2023-12-04	6.7	Medium
		bounds check. This could lead to local escalation of privilege with			
				l	
		System execution privileges needed. User interaction is not		1	
	google - multiple	System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08240132; Issue ID:			
CVE-2023-32854	google - multiple products	'	2023-12-04	6.7	Medium
CVE-2023-32854	• • • •	needed for exploitation. Patch ID: ALPS08240132; Issue ID: ALPS08240132. In meta, there is a possible classic buffer overflow due to a missing	2023-12-04	6.7	Medium
CVE-2023-32854	• • • •	needed for exploitation. Patch ID: ALPS08240132; Issue ID: ALPS08240132. In meta, there is a possible classic buffer overflow due to a missing bounds check. This could lead to local escalation of privilege with	2023-12-04	6.7	Medium
CVE-2023-32854	products	needed for exploitation. Patch ID: ALPS08240132; Issue ID: ALPS08240132. 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	2023-12-04	6.7	Medium
CVE-2023-32854 CVE-2023-32859	• • • •	needed for exploitation. Patch ID: ALPS08240132; Issue ID: ALPS08240132. In meta, there is a possible classic buffer overflow due to a missing bounds check. This could lead to local escalation of privilege with	2023-12-04	6.7	Medium Medium

		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			
CVE 2022 228C0	google - multiple	interaction is not needed for exploitation. Patch ID:	2022 12 04	6.7	N/Lo alicens
CVE-2023-32860	products	ALPS07929788; Issue ID: ALPS07929788. In display, there is a possible out of bounds read due to an	2023-12-04	6.7	Medium
		incorrect bounds check. This could lead to local escalation of			
		privilege with System execution privileges needed. User			
CVE-2023-32861	google - multiple products	interaction is not needed for exploitation. Patch ID: ALPS08059081; Issue ID: ALPS08059081.	2023-12-04	6.7	Medium
CVL-2023-32801	products	In display, there is a possible out of bounds read due to an	2023-12-04	0.7	Mediaiii
		incorrect bounds check. This could lead to local escalation of			
		privilege with System execution privileges needed. User			
CVE-2023-32862	google - multiple products	interaction is not needed for exploitation. Patch ID: ALPS07388762; Issue ID: ALPS07388762.	2023-12-04	6.7	Medium
311 2010 02002	p. caucio	In display drm, there is a possible out of bounds read due to a		<u> </u>	
		missing bounds check. This could lead to local escalation of			
	google - multiple	privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:			
CVE-2023-32863	products	ALPS07326314; Issue ID: ALPS07326314.	2023-12-04	6.7	Medium
	·	In display drm, there is a possible out of bounds write due to an			
		incorrect bounds check. This could lead to local escalation of			
	google - multiple	privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:			
CVE-2023-32864	products	ALPS07292187; Issue ID: ALPS07292187.	2023-12-04	6.7	Medium
		In display drm, there is a possible out of bounds write due to an			
		incorrect bounds check. This could lead to local escalation of			
	google - multiple	privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:			
CVE-2023-32865	products	ALPS07363456; Issue ID: ALPS07363456.	2023-12-04	6.7	Medium
		In mmp, there is a possible memory corruption due to an incorrect			
		bounds check. This could lead to local escalation of privilege with			
	google - multiple	System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07342152; Issue ID:			
CVE-2023-32866	products	ALPS07342152.	2023-12-04	6.7	Medium
		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			
	google - multiple	interaction is not needed for exploitation. Patch ID:			
CVE-2023-32867	products	ALPS07560793; Issue ID: ALPS07560793.	2023-12-04	6.7	Medium
		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			
	google - multiple	interaction is not needed for exploitation. Patch ID:			
CVE-2023-32868	products	ALPS07363632; Issue ID: ALPS07363632.	2023-12-04	6.7	Medium
		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			
	google - multiple	interaction is not needed for exploitation. Patch ID:			
CVE-2023-32869	products	ALPS07363632; Issue ID: ALPS07363689.	2023-12-04	6.7	Medium
		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			
	google - multiple	interaction is not needed for exploitation. Patch ID:			
CVE-2023-32870	products	ALPS07363740; Issue ID: ALPS07363740.	2023-12-04	6.7	Medium
		Out-of-bound write vulnerability in libIfaaCa prior to SMR Dec-			
CVE-2023-42557	samsung - multiple products	2023 Release 1 allows local system attackers to execute arbitrary code.	2023-12-05	6.7	Medium
<u> </u>	p. 5 a. a. 5 t.	Improper input validation vulnerability in Smart Clip prior to SMR		0.7	
		Improper input validation valificiability in Smart clip prior to Sivik			
	samsung - multiple	Dec-2023 Release 1 allows local attackers with shell privilege to			
CVE-2023-42565	samsung - multiple products	Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code.	2023-12-05	6.7	Medium
CVE-2023-42565		Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code. there is a possible way for the secure world to write to NS memory	2023-12-05	6.7	Medium
CVE-2023-42565		Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code.	2023-12-05	6.7	Medium
CVE-2023-42565 CVE-2023-48405		Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code. 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.	2023-12-05	6.7	Medium Medium
	products	Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code. 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. there is a possible permanent DoS or way for the modem to boot			
	products	Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code. 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. 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			
	products	Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code. 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. there is a possible permanent DoS or way for the modem to boot			
CVE-2023-48405	products google - android	Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code. 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. 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. In the Pixel Camera Driver, there is a possible use after free due to	2023-12-08	6.7	Medium
CVE-2023-48405	products google - android	Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code. 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. 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. 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	2023-12-08	6.7	Medium
CVE-2023-48405 CVE-2023-48406	google - android google - android	Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code. 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. 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. 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	2023-12-08	6.7	Medium
CVE-2023-48405	products google - android	Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code. 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. 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. 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	2023-12-08	6.7	Medium
CVE-2023-48405 CVE-2023-48406	google - android google - android	Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code. 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. 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. 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. Dell DM5500 contains a path traversal vulnerability in PPOE	2023-12-08	6.7	Medium
CVE-2023-48405 CVE-2023-48406	google - android google - android	Dec-2023 Release 1 allows local attackers with shell privilege to execute arbitrary code. 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. 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. 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

		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			
CVE-2023-40090	google - multiple products	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_mode m_firmware	Information disclosure when the trusted application metadata symbol addresses are accessed while loading an ELF in TEE. Inappropriate implementation in Web Browser UI in Google Chrome prior to 120.0.6099.62 allowed a remote attacker to	2023-12-05	6.5	Medium
CVE-2023-6512	google - chrome	potentially spoof the contents of an iframe dialog context menu via a crafted HTML page. (Chromium security severity: Low) there is a possible use after free due to a race condition. This could	2023-12-06	6.5	Medium
CVE-2023-48420	google - android	lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. An issue was discovered in Zimbra Collaboration (ZCS) before	2023-12-08	6.4	Medium
CVE-2023-43102	zimbra - multiple products zimbra - multiple	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. An XSS issue was discovered in a web endpoint in Zimbra Collaboration (ZCS) before 10.0.4 via an unsanitized parameter.	2023-12-07	6.1	Medium
CVE-2023-43103	products	This is also fixed in 8.8.15 Patch 43 and 9.0.0 Patch 36.	2023-12-07	6.1	Medium
		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			
CVE-2023-23372	qnap - multiple products	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 In wifi service, there is a possible out of bounds write due to a	2023-12-04	5.5	Medium
CVE-2022-48463	google - android	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
	google - multiple	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			
CVE-2023-42672	products	In imsservice, there is a possible way to write permission usage	2023-12-04	5.5	Medium
CVE-2023-42673	google - multiple products	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 In imsservice, there is a possible way to write permission usage	2023-12-04	5.5	Medium
CVE-2023-42676	google - multiple products	records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed In imsservice, there is a possible way to write permission usage	2023-12-04	5.5	Medium
CVE-2023-42677	google - multiple products	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
	google - multiple	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			
CVE-2023-42678	products google - multiple	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	2023-12-04	5.5	Medium
CVE-2023-42697	products	privileges needed	2023-12-04	5.5	Medium

	google - multiple	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			
CVE-2023-42698	products	privileges needed	2023-12-04	5.5	Medium
		In omacp service, there is a possible way to write permission usage			
	1 100 1	records of an app due to a missing permission check. This could			
CVE 2022 42C00	google - multiple	lead to local information disclosure with no additional execution	2022 42 04		NA - divor-
CVE-2023-42699	products	privileges needed	2023-12-04	5.5	Medium
		In firewall service, there is a possible way to write permission			
	googlo multiplo	usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional			
CVE-2023-42700	google - multiple products	execution privileges needed	2023-12-04	5.5	Medium
CVE-2023-42700	products	In firewall service, there is a possible way to write permission	2025-12-04	5.5	Medium
		usage records of an app due to a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-42701	products	execution privileges needed	2023-12-04	5.5	Medium
<u>CVL 2023 12701</u>	products	In firewall service, there is a possible way to write permission	2023 12 01	3.3	Wicaram
		usage records of an app due to a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-42702	products	execution privileges needed	2023-12-04	5.5	Medium
012 2020 12702	products	In firewall service, there is a possible way to write permission	2020 12 0 1	3.3	Wiediaiii
		usage records of an app due to a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-42703	products	execution privileges needed	2023-12-04	5.5	Medium
<u> </u>	p. ou u ou	In imsservice, there is a possible way to write permission usage		0.0	
		records of an app due to a missing permission check. This could			
	google - multiple	lead to local information disclosure with no additional execution			
CVE-2023-42704	products	privileges needed	2023-12-04	5.5	Medium
		In imsservice, there is a possible way to write permission usage			
		records of an app due to a missing permission check. This could			
	google - multiple	lead to local information disclosure with no additional execution			
CVE-2023-42705	products	privileges needed	2023-12-04	5.5	Medium
	·	In firewall service, there is a possible way to write permission			
		usage records of an app due to a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-42706	products	execution privileges needed	2023-12-04	5.5	Medium
	·	In firewall service, there is a possible way to write permission			
		usage records of an app due to a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-42707	products	execution privileges needed	2023-12-04	5.5	Medium
		In firewall service, there is a possible way to write permission			
		usage records of an app due to a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-42708	products	execution privileges needed	2023-12-04	5.5	Medium
	•	In firewall service, there is a possible way to write permission			
		usage records of an app due to a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-42709	products	execution privileges needed	2023-12-04	5.5	Medium
	·	In firewall service, there is a possible way to write permission			
		usage records of an app due to a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-42710	products	execution privileges needed	2023-12-04	5.5	Medium
		In firewall service, there is a possible way to write permission			
		usage records of an app due to a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-42711	products	execution privileges needed	2023-12-04	5.5	Medium
		In firewall service, there is a possible way to write permission			
		usage records of an app due to a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-42712	products	execution privileges needed	2023-12-04	5.5	Medium
		In firewall service, there is a possible way to write permission			
		usage records of an app due to a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-42713	products	execution privileges needed	2023-12-04	5.5	Medium
		In firewall service, there is a possible way to write permission			
		usage records of an app due to a missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-42714	products	execution privileges needed	2023-12-04	5.5	Medium
		In telephony service, there is a possible missing permission check.			
	google - multiple	This could lead to local information disclosure with no additional			
CVE-2023-42715	products	execution privileges needed	2023-12-04	5.5	Medium
		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			
	google - multiple	local information disclosure with no additional execution privileges			
CVE-2023-42718	products	needed	2023-12-04	5.5	Medium
		In video service, there is a possible out of bounds read due to a			
					Ī
		incorrect bounds check. This could lead to local denial of service			

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
	00	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			
CVE-2023-42723	google - android	with no additional execution privileges needed In phasecheckserver, there is a possible out of bounds read due to	2023-12-04	5.5	Medium
CVE-2023-42728	google - multiple products	a missing bounds check. This could lead to local denial of service with no additional execution privileges needed In IMS service, there is a possible way to write permission usage	2023-12-04	5.5	Medium
	google - multiple	records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution			
CVE-2023-42730	products	privileges needed In telephony service, there is a possible missing permission check.	2023-12-04	5.5	Medium
CVE-2023-42732	google - multiple products	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
	google - multiple	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			
CVE-2023-42737	products	execution privileges needed In telecom service, there is a possible way to write permission	2023-12-04	5.5	Medium
CVE-2023-42741	google - multiple products	usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed In sysui, there is a possible missing permission check. This could	2023-12-04	5.5	Medium
CVE-2023-42742	google - multiple products	lead to local denial of service with no additional execution privileges needed	2023-12-04	5.5	Mediun
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	Mediun
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 thissettings 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
	google - multiple	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			
CVE-2023-35668	products	privileges needed. User interaction is not needed for exploitation. In visitUris of Notification.java, there is a possible cross-user media read due to Confused Deputy. This could lead to local information	2023-12-04	5.5	Mediun
CVE-2023-40073	google - multiple products	disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. In saveToXml of PersistableBundle.java, invalid data could lead to	2023-12-04	5.5	Mediun
CVE-2023-40074	google - multiple products	local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-12-04	5.5	Mediun
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. 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	2023-12-04	5.5	Medium
CVE-2023-40076	google - android	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 mode analysis of security in products of the process of the products of t		I	with no additional eventtion privileges needed. Hear interaction is			1
In parse, gap, datu of utilises, there is a possible out of bounds goggle - multiple products and the image products and the image products of the image products and the image of the products of the image products of the image of the products of the image products of the image of the o			with no additional execution privileges needed. User interaction is			
cVI-2023-4038 poogle - multiple products which makes the company of the company			•			
products products information disclosure with User execution privileges needed. products in verifySprotrustinic Package of StructurService jaws, there is a google - multiple products in verifySprotrustinic Package of StructurService jaws, there is a google - multiple products in meaning the products in the secure to California of the secure to California of the products in the produ			· · · · · · · · · · · · · · · · · · ·			
the verify@fortcuttinfoPackage of ShortcutService_java, there is a possible way to see another user's image due to a comised objective. This could lead to local information in control additional execution privileges needed. User interaction in cot needed for exploitation. In windower of NortcataconConversationInt part there is a minute of the products of the produ		google - multiple	<u> </u>			
possible way to see another user's image due to a confused epopty. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. products in monitorial execution privileges needed. User interaction is not needed for exploitation. products products in monitorial products in monitorial products of the country of	CVE-2023-40083	products	User interaction is not needed for exploitation.	2023-12-04	5.5	Mediur
deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction in not needed for eaglotation. UNE-2023-40988 products products products products on the products of			· · · · · · · · · · · · · · · · · · ·			
documents docu			,			
CVE-2023-49392 products needed for exploitation. a constitution of the possible way to access app notification data of another user due to possible way to access app notification data of another user due to be possible way to access app notification data of another user due to be possible way to access app notification data of another user due to be possible way to access app notification data of another user due to be possible user due to be possibl						
ImmonDrone of Notification ConversationInfo].asy, there is a possible way to access app norification data of another served to a logic error in the code. This could lead to local information disclosure with an additional execution privileges needed. User interaction is not needed for exploitation.			, -			
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 in a not needed for exploitation. In parse, gap, data of trilis cr, 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 missing bounds check. This could lead to local information disclosure with user execution privileges needed. VEZ 2023 427581 products VEZ 2023 427561 products VEZ 2023 427561 products VEZ 2023 427561 products VEZ 2023 427562 products VEZ 2023 427562 products VEZ 2023 427562 products VEZ 2023 427563 products VEZ 2023 427564 products VEZ 2023 427565 products VEZ 2023 427565 products VEZ 2023 427566 products VEZ 2023 427567 products VEZ 2023 42757 products VEZ 2023 42757 products VEZ 2023 42757 products VEZ	CVE-2023-40092	products		2023-12-04	5.5	Mediur
a logogle - multiple products products interaction is not needed for exploitation. In parse, gap, clark of wilds, city here 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. CVF-2023-43781 google - multiple products qualiform and products qualiform and products qualiform and products qualiform. Transvent DSD as use to improper underflictation or Transvent DSD in Automorbive DS due to improper underflictation. CVF-2023-43551 growth products products are supplied to the products products. Products products are supplied products. Products products are products. Products products are products. Products products are products. Prod			•			
google - multiple disclosure with no additional execution privileges needed. User products inferenction is not needed for exploitation. 1023-12-04 5.5 Medium 1022-127-128 products						
CVE 2023-45781 products Interaction is not needed for exploitation. 2023-12-04 5.5 Medium Products Google - multiple Google - multip						
In passe_gap_date of stutksct. There is a possible out of bounds read due to a missing bounds facet. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation. Ver. 2023 42936 User interaction is not needed for exploitation. Ver. 2023 42936 Ver. 202			, -			
cyt. 2023-45781 google - multiple gualcomm - groducts and gualcomm - groducts gualcomm - groducts gualcomm - groducts gualcomm - groducts g	CVE-2023-40098	products		2023-12-04	5.5	Mediur
CVE-2023-45781 google - multiple products User interaction is not needed for exploitation. 2023-12-04 5.5 Medium CVE-2023-45781 google - android Protocolinascipherophysis CVE-2023-48410 google - android GVE-2023-48412 google - android GVE-2023-48412 google - android CVE-2023-48412 google - android CVE-2023-48422 google - android CVE-2023-248422 google - android CVE			· · · · · · · · · · · · · · · · · · ·			
CVE-2023-45781 products outside products of the secure ID calls. CVE-2023-4256 products of the secure ID calls. CVE-2023-4257 products of the secure ID calls o			<u> </u>			
CVE-2023-4256 amsung - multiple products amsung			. •			
CVE-2023-42560 products 2023-12-05 5.5 Medium 2023-12-05 5.5 Medium 2023-12-05 5.5 Medium 2023-12-05 2023-12-05 5.5 Medium 2023-12-05	CVE-2023-45781	•	'	2023-12-04	5.5	Mediur
Samsung - multiple products 2023 Release 1 allows attacker to get sensitive information. 2023-12-05 5.5 Medium products 2023 Release 1 allows attacker to get sensitive information. 2023-12-05 5.5 Medium privilege. 2023 Release 1 allows attacker to send broadcast with system privilege. 2023 Release 1 allows attacker to send broadcast with system privilege. 2023-12-05 5.5 Medium privilege. 2023-12-05 2023 Release 1 allows attacker to get sensitive information. 2023-12-05 5.5 Medium privilege. 2023-12-05						
CVE-2023-42556 products 2023 Release 1 allows attacker to get sensitive information. 2023-12-05 5.5 Medium Improper access control in knoxususus mervice prior to SMP. Decade products as missing account, web, soft ware, development with the control of the contro	CVE-2023-33070			2023-12-05	5.5	Mediur
minute products privales and products are products and products are products and products and products are producted and products are producted and products are producted and products are producted and products and products are producted and products and products are producted and products are producted and products are producted and products are producted and products and products are producted and products are pro			, , , , , , , , , , , , , , , , , , , ,			
samsung anutiple products provilege. 2023-14564 products provilege. 3023-14565 products provilege. 3023-14565 products provilege. 3023-14572 samsung account, web, soft ware, development like to be products provilege. 3023-14572 samsung account, web, soft ware, development like to be products provilege. 3023-14572 samsung account, web, soft ware, development like to be products products products and the products products of the products	CVE-2023-42556	products		2023-12-05	5.5	Mediur
CVE-2023-42564 products privilege. 2023-12-05 5.5 Mediur prior to version 1.5.24 allows attacker to get sensitive information. 2023-12-05 5.5 Mediur prior to version 1.5.24 allows attacker to get sensitive information. 2023-12-05 5.5 Mediur prior to version 1.5.24 allows attacker to get sensitive information. 2023-12-05 5.5 Mediur version 3.4 in China models allows local attackers to access data 2023-12-05 5.5 Mediur Vinerability of unauthorized file access. in the Settings app. Successful exploitation of this vulnerability may cause unauthorized file access. in ProtocolMiscARCommandAdapter:sinit() 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. CVE-2023-48401 google - android in ProtocolNetSimpleInfoAdapter() of protocolnetsdapter.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with baseband firmware compromise required. User interaction is not needed for exploitation. CVE-2023-48403 google - android in ProtocolNetSimpleInfoAdapter() of protocolnetsdapter.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with baseband firmware compromise required. User interaction is not needed for exploitation. CVE-2023-48408 google - android in SignalStrength() of protocolnetsdapter.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. CVE-2023-48412 google - android in private particles of the protocolnetsdapter.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 on ended. User interaction is not needed for exploi						
amsung account, web, soft ware development Let account, web, soft ware development Let account, web, soft ware development Let account web soft ware development Let account web soft ware development was allowed to exploit the were well was accounted by the web accounted with the web accounted was accounted by the web accounted was allowed to get accounted with the web accounted was allowed to account web soft was accounted with the web accounted was accounted with the web accounted was accounted with a web accounted was accounted was accounted with a web accounted was accounted was accounted with a web accounted was acc	OVE 2022 12==:			2022 12 ==		
account_web_soft ware_development ware_development ware_development ware_development Lit ware_development ware_development Lit samsung - samsung - samsung - samsung - version 3.4 in China models allows local attackers to get sensitive information. VE-2023-42573 samsung - version 3.4 in China models allows local attackers to access data. Vulicerability of unauthorized file access in the Settings app. Successful exploitation of this vulnerability may cause unauthorized file access. In ProtocolMiscATCommandAdapter:initity of protocolMiscATCommandAdapter:initity of protocolMiscATCommandAdapter:initity of protocolMiscATCommandAdapter:initity of protocolMiscATCommandAdapter:initity of protocolMiscATCommandAdapter:initity of protocolMiscATCommandAdapter:pt, 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. 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. In ProtocolNetSimileinfoAdapter() of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds there was not a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. In ProtocolNetSimileinfoAdapter::FiliGsmSignalStrength() 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. In privileges needed. User interaction is not needed for exploitation. In privileges needed. User interaction is not needed for exploitation. In linit of protocolembandapter.cpp, there is a possible	CVE-2023-42564		privilege.	2023-12-05	5.5	Mediur
ware development kit prior to version 1.5.24 allows attacker to get sensitive information. 2023-12-05 5.5 Medium prior to version 1.5.24 allows attacker to get sensitive information. 2023-12-05 5.5 Medium prior to version 1.5.24 allows attackers to access data. 2023-12-05 5.5 Medium prior to version 1.5.24 allows attackers to access data. 2023-12-05 5.5 Medium version 3.4 in China models allows local attackers to access data. 2023-12-05 5.5 Medium version 3.4 in China models allows local attackers to access data. 2023-12-06 5.5 Medium version 3.4 in China models allows local attackers to access data. 2023-12-06 5.5 Medium version 3.4 in China models allows local attackers to access data. 2023-12-06 5.5 Medium version 3.4 in China models allows local attackers to access data. 2023-12-06 5.5 Medium version 3.4 in China models allows local attackers to access data. 2023-12-06 5.5 Medium version 3.4 in China models and version 3.4 in China models a		_				
Price to version 1.5.24 allows attacker to get sensitive information. 2023-12-05 S.5 Medium			Insuliate intent bile alies and a sacisfic to Control of the Contr			
Samsung search, widget version 3.4 in China models allows local attackers to access data. 2023-12-05 5.5 Mediur Volnerability of unauthorized file access in the Settings app. Successful exploitation of this vulnerability may cause unauthorized file access. 1 In ProtocolMiscal CommandAdapter: init(1) 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. In SetSizeOffeniBadapter: inition 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 naseband firmware compromise required. User interaction is not needed for exploitation. In SetSizeOffeniBecords 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 no additional execution privileges needed. User interaction is not needed for exploitation. In SignalStrengthAdapter:FillGsmSignalStrength() of protocolmetadapter.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. 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. In Interaction	CVE 2022 42572			2022 42 05		0.4 = =1:
version 3.4 in China models allows local attackers to access data. 2023-12-05 5.5 Medium Vulnerability of unauthorized file access in the Settings app. 2023-12-06 5.5 Medium Vulnerability of unauthorized file access. 2023-12-06 5.5 Medium Vulnerability of unauthorized file access. 2023-12-06 5.5 Medium Vulnerability of protocolmiscadapter cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information Vulnerability of protocolmiscadapter cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information Vulnerability of protocoladapter cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information Vulnerability of protocoladapter cpp, there is a possible out of bounds read due to a misor protocoladapter cpp, there is a possible out of bounds read due to a misor protocoladapter cpp, there is a possible out of bounds read due to a misor protocoladapter cpp, there is a possible out of bounds read due to a misor protocoladapter cpp, there is a possible out of bounds read due to a misor protocoladapter 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. CVE-2023-48408 google - android In private_handle_tof mail_gralloc_buffer.hthere is a possible information leak due to a logic error in the code. This could lead to local information leak due to a logic error in the code. This could lead to local information leak due to a logic error in the code. This could lead to local information leak due to a logic error in the code. This could lead to local 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. CVE-2023-48412 google - andr	CVE-2023-42572	_		2023-12-05	5.5	Mediur
Vulnerability of unauthorized file access in the Settings app.	0/5 2022 42572	_	, , , , , , , , , , , , , , , , , , , ,	2022 42 05		N 41"
huawei - multiple products DrotocolMiscATCommandAdapter::Init() of protocolMiscATCommandAdapter::Init() of protocolMiscAGDCOMMISCAGD	CVE-2023-425/3	searcn_widget		2023-12-05	5.5	Mediur
UE-2023-49248 products unauthorized file access. 2023-12-06 5.5 Mediur			,			
In ProtocolMisca/Tommand/Agapter::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. CVE-2023-48401 google - android exploitation in protocolmistation devecution privileges needed. User interaction is not needed for exploitation. CVF-2023-48401 google - android exploitation in protocolmistation devecution privileges needed. User interaction is not needed for exploitation. CVF-2023-48408 google - android exploitation. CVF-2023-48408 google - android exploitation. CVF-2023-48408 google - android exploitation. In SignalStrengthAdapter: FilliGsmSignalStrength() of protocolmistadapter.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. In SignalStrengthAdapter: FilliGsmSignalStrength() 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. CVF-2023-48411 google - android interaction is not needed for exploitation. In private_handle_t of mail_grailoc_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. In linit of protocolembinsadapter.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. In linit of protocolembinsadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosur	CVE 2022 40240	· ·	· · · · · · · · · · · · · · · · · · ·	2022 12 06		Madium
protocolmiscadapter.cop., 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. In Gestizeo(TeeniBecords 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. CVE-2023-48401 google - android execution privileges needed. User interaction is not needed for exploitation. CVE-2023-48408 google - android baseband firmware compromise required. User interaction is not needed for exploitation. CVE-2023-48408 google - android in Signal StrengthAdapter: FillCismSignalStrength() 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. CVE-2023-48411 google - android in Signal Strength() 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. In private handle; to final grallop. buffer, 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. In init of protocolembmasadpter.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. In linit of protocolnetadpter.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 exec	CVE-2023-49248	products		2023-12-06	5.5	Mediur
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. In GetSizeoffeniRecords 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. CVE-2023-48401 google - android protocolnetsim: In Interaction: In			, , , , , , , , , , , , , , , , , , , ,			
disclosure with baseband firmware compromise required. User interaction is not needed for exploitation. CVE-2023-48401 google - android googl						
CVE-2023-48409 google - android interaction is not needed for exploitation. 2023-12-08 5.5 Mediur In GetSizeOffeenlRecords 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. 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. In SignalStrengthAdapter:.FillGsmSignalStrength() 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. In SignalStrengthAdapter:.pp, 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 Mediur In private handle, to fmail gralloc, buffer h, there is a possible information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. 2023-12-08 5.5 Mediur In lint of protocolnetmbandapter 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 Mediur In lint of protocolnetmbandapter 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 Mediur In lint of protocolnetadapter.cpp, there is a						
In GetSizeOfEenIRecords 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. CVE-2023-48401 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. CVE-2023-48408 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. CVE-2023-48411 google - android In private_handle_t of mail_gralloc_buffer.h, there is a possible information leak due to a logic error in the code. This could lead to local 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. CVE-2023-48412 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. 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. 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 exploit			· · · · · · · · · · · · · · · · · · ·			
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. 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. 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. CVE-2023-48411 google - android interaction is not needed for exploitation. In private_handle_tof 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. CVE-2023-48412 google - android privileges needed. User interaction is not needed for exploitation. In lnit 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. CVE-2023-48415 google - android needed. User interaction is not needed for exploitation. In lnit of protocolembadapter.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. CVE-2023-48412 google - android needed. User interaction is not needed for exploitation. A null pointer dereference vulnerability was found in nft_dynset. in nft_dynset. in nft_ables in the timux kernel. This issue may allow a local attack	CVE-2023-48399	google - android	, ,	2023-12-08	5.5	Mediur
could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. 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. 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. 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. CVE-2023-48412 google - android privileges needed. User interaction is not needed for exploitation. 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. 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. In Init of protocolembadapter.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. In Init of protocolembadapter.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			, , , , , , , , , , , , , , , , , , , ,			
execution privileges needed. User interaction is not needed for exploitation. 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. In SignalStrengthAdapter::FillGsmSignalStrength() of protocolnetadapter due to a missing 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. CVE-2023-48411 google - android In private_handle_t of mail_gralloc_buffer.h, 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. CVE-2023-48412 google - android In private_handle_t of mail_gralloc_buffer.h, there is a possible out of local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. CVE-2023-48415 google - android privileges needed. User interaction is not needed for exploitation. CVE-2023-48415 google - android needed. User interaction is not needed for exploitation. In Init of protocolembnsadapter.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. CVE-2023-48415 google - android needed. User interaction is not needed for exploitation. 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. A null pointer dereference vulnerability was found in float prival prival prival prival prival prival prival pri			'·			
CVE-2023-48401 google - android exploitation. 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. CVE-2023-48408 google - android needed for exploitation. 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. 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. CVE-2023-48412 google - android privaleges needed. User interaction is not needed for exploitation. In Init of protocolnembmsadapter.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. CVE-2023-48415 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. CVE-2023-48412 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. CVE-2023-48422 google - android Init not 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 ad						
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. 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. 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. CVE-2023-48412 google - android privileges needed. User interaction is not needed for exploitation. 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. CVE-2023-48415 google - android in 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. 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. A null pointer dereference vulnerability was found in fit_dynset_init() in net/nerability was found in fit_dynset_init() in net/nerability was found in fit_dynset_init() in net/nerability was found in the io_uring SQ/CQ rings functionality in the Linux kernel. This issue could allow a local star for unultiple products In mu			, -			
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. 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. 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. CVE-2023-48412 google - android privileges needed. User interaction is not needed for exploitation. 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. CVE-2023-48415 google - android In Init of protocolentadapter.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. In Init of protocolentadapter.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. A null pointer dereference vulnerability was found in fit_dynst_c in fit_dables in the Linux kernel. This issue may allow a local attacker with CVE-2023-6622 products An out-of-bounds memory access flaw was found in the io_uring SQ/CQ rings functionality in the Linux kernel. This issue	CVE-2023-48401	google - android	'	2023-12-08	5.5	Mediur
check. This could lead to local information disclosure with baseband firmware compromise required. User interaction is not needed for exploitation. 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. CVE-2023-48411 google - android inprivate_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. CVE-2023-48412 google - android 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. 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. 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. 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 CVE-2023-6622 products CAP_NET_ADMIN user privilege to trigger a denial of service. 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 surface of the products of the pro			1 11 11 11 11 11 11 11 11 11 11 11 11 1			
baseband firmware compromise required. User interaction is not needed for exploitation. 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. [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 information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. [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. [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. [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. [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. [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. [In Init of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to lo			· ·			
CVE-2023-48408 google - android needed for exploitation. 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. CVE-2023-48411 google - android interaction leak due to a logic error in the code. This could lead to local information leak due to a logic error in the code. This could lead to local 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. 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. 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. In Init of protocolmetadapter.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. A null pointer dereference vulnerability was found in nft_dynset_init() in net/netfilter/nft_dynset.c in nf_tables in the linux ernel. This issue may allow a local attacker with no additional execution privileges on the linux ernel. This issue could allow a local user to crash the system. In Init protocolombms adapter.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 to the possible out of bounds read due to a missing bounds check. This could						
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. CVE-2023-48411 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. CVE-2023-48412 google - android privileges needed. User interaction is not needed for exploitation. In lnit 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. In lnit 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. In lnit 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. A null pointer dereference vulnerability was found in mft_dynset_init() in net/netfilter/nft_dynset.c in nf_tables in the Linux kernel. This issue may allow a local attacker with CVE-2023-6622 products CVE-2023-6622 products In lnit 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 Mediur A null pointer dereference vulnerability was found in mft_dynset.c in nf_tables in the Linux kernel. Th						
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 compromiser required. User interaction is not needed for exploitation. 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 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. 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. 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. 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. CVE-2023-48422	CVE-2023-48408	google - android	•	2023-12-08	5.5	Mediur
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. CVE-2023-48412 google - android information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. CVE-2023-48412 google - android privileges needed. User interaction is not needed for exploitation. 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. CVE-2023-48415 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. CVE-2023-48415 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. CVE-2023-48422 google - android needed. User interaction is not needed for exploitation. A null pointer dereference vulnerability was found in nft_dynset_init() in net/netfilter/nft_dynset_c in nft_tables in the Linux kernel. This issue may allow a local attacker with CAP_NET_ADMIN user privilege to trigger a denial of service. 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. IBM Informix Dynamic Server 12.10 and 14.10 archecker is						
disclosure with baseband firmware compromise required. User interaction is not needed for exploitation. 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. In lnit 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. CVE-2023-48415 google - android ln lnit 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. In lnit 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. CVE-2023-48422 google - android needed. User interaction is not needed for exploitation. 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 CVE-2023-6622 products CAP_NET_ADMIN user privilege to trigger a denial of service. 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. IBM Informix Dynamic Server 12.10 and 14.10 archecker is						
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. CVE-2023-48412			_			
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. CVE-2023-48412 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. 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. CVE-2023-48412 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. A null pointer dereference vulnerability was found in inft_dynset_init() in net/netfilter/nft_dynset.c in nf_tables in the Linux kernel. This issue may allow a local attacker with CVE-2023-6622 products CAP_NET_ADMIN user privilege to trigger a denial of service. 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. IBM Informix Dynamic Server 12.10 and 14.10 archecker is	0.45 0.55	. , .	, ,			
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. CVE-2023-48412 google - android local information disclosure with no additional execution 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. 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. CVE-2023-48412 google - android linit 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. 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. CVE-2023-6502 products a local user to crash the system. IbM Informix Dynamic Server 12.10 and 14.10 archecker is	CVE-2023-48411	google - android	·	2023-12-08	5.5	Mediur
to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. In lnit 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. In lnit 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. CVE-2023-48412 google - android In lnit 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. 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. 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. IBM Informix Dynamic Server 12.10 and 14.10 archecker is						
CVE-2023-48412 google - android privileges needed. User interaction is not needed for exploitation. 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. 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 CVE-2023-48412 google - android needed. User interaction is not needed for exploitation. A null pointer dereference with no additional execution privileges needed. User interaction is not needed for exploitation. 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. 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. ibm - multiple lBM Informix Dynamic Server 12.10 and 14.10 archecker is						
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. 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. CVE-2023-48422 google - android google - android information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. A null pointer dereference vulnerability was found in inft_dynset_init() in net/netfilter/nft_dynset.c in nf_tables in the Linux kernel. This issue may allow a local attacker with CVE-2023-6622 products CAP_NET_ADMIN user privilege to trigger a denial of service. 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. ibm - multiple IBM Informix Dynamic Server 12.10 and 14.10 archecker is				_		
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. 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 google - android needed. User interaction is not needed for exploitation. A null pointer dereference vulnerability was found in nft_dynset_init() in net/netfilter/nft_dynset.c in nf_tables in the Linux - multiple Linux kernel. This issue may allow a local attacker with CVE-2023-6622 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. Description of the dead to local attacker is Medium 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.	CVE-2023-48412	google - android		2023-12-08	5.5	Mediur
local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. 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. 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 of the injury of the						
CVE-2023-48415 google - android needed. User interaction is not needed for exploitation. 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. A null pointer dereference vulnerability was found in nft_dynset_init() in net/netfilter/nft_dynset.c in nf_tables in the Linux - multiple products CAP_NET_ADMIN user privilege to trigger a denial of service. 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 attacker with CVE-2023-6560 ibm - multiple IBM Informix Dynamic Server 12.10 and 14.10 archecker is						
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. 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 CVE-2023-6622 products CAP_NET_ADMIN user privilege to trigger a denial of service. 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. Description of bounds bounds from the iouring standard for the			, -			
read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges google - android needed. User interaction is not needed for exploitation. 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 CVE-2023-6622 products CAP_NET_ADMIN user privilege to trigger a denial of service. 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. ibm - multiple IBM Informix Dynamic Server 12.10 and 14.10 archecker is	CVE-2023-48415	google - android	needed. User interaction is not needed for exploitation.	2023-12-08	5.5	Mediur
information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. A null pointer dereference vulnerability was found in nft_dynset_init() in net/netfilter/nft_dynset.c in nf_tables in the Linux - multiple products CAP_NET_ADMIN user privilege to trigger a denial of service. 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. SQ/CQ rings functionality in the Linux kernel allow a local attacker is IBM Informix Dynamic Server 12.10 and 14.10 archecker is						
CVE-2023-48422 google - android needed. User interaction is not needed for exploitation. 2023-12-08 5.5 Medium A null pointer dereference vulnerability was found in nft_dynset_init() in net/netfilter/nft_dynset.c in nf_tables in the Linux - multiple products CAP_NET_ADMIN user privilege to trigger a denial of service. 2023-12-08 5.5 Medium 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-2023-6560 ibm - multiple IBM Informix Dynamic Server 12.10 and 14.10 archecker is						
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 CVE-2023-6622 products CAP_NET_ADMIN user privilege to trigger a denial of service. 2023-12-08 5.5 Medium 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 ibm - multiple IBM Informix Dynamic Server 12.10 and 14.10 archecker is			information disclosure with no additional execution privileges			
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 CVE-2023-6622 products CAP_NET_ADMIN user privilege to trigger a denial of service. 2023-12-08 5.5 Medium 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 ibm - multiple IBM Informix Dynamic Server 12.10 and 14.10 archecker is	CVE-2023-48422	google - android	, -	2023-12-08	5.5	Mediur
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. 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. SQ-23-12-09 S.5 Mediur 2023-12-09 S.5 Mediur 1bm - multiple IBM Informix Dynamic Server 12.10 and 14.10 archecker is		_	·			
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-2023-6622 products CAP_NET_ADMIN user privilege to trigger a denial of service. 2023-12-08 5.5 Medium 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 ibm - multiple IBM Informix Dynamic Server 12.10 and 14.10 archecker is		linux - multiple				
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 ibm - multiple IBM Informix Dynamic Server 12.10 and 14.10 archecker is	CVE-2023-6622	· · · · · · · · · · · · · · · · · · ·	· ·	2023-12-08	5.5	Mediur
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		p. 00.000		<u> </u>	2.5	
CVE-2023-6560 products a local user to crash the system. 2023-12-09 5.5 Medium ibm - multiple IBM Informix Dynamic Server 12.10 and 14.10 archecker is		linux - multinla	·			
ibm - multiple IBM Informix Dynamic Server 12.10 and 14.10 archecker is	CVF-2023-6560	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	2023-12-09	55	Mediur
	OVE 2023-0300	ρισαάσιο	a rocal ager to crash the system.	∠∪∠J-1Z-UJ	ر.ر	iviculul
		ihm - multiple	IBM Informix Dynamic Server 12 10 and 14 10 archaeker is			
<u>CVL-2023-20320</u> products vullierable to a fleap buffer overflow, caused by improper bounds 2023-12-09 5.5 Mediur	C//E_2022 20526	•		2022 12 00	. .	Madium
	CVL-2UZ3-Z83Z8	products	value able to a neap butter overflow, caused by improper bounds	ZUZ3-1Z-UY	٥.٥	Iviediun

theising with could allow a local user to cause a segmentation air. MMX Farror 12:73104. IBM Informs Dynamic Sancer 2.13 and 14.10 cft is vulnerable to a heap halfer certifier, caused by immorph channels for a heap halfer certifier, caused by immorph channels for a heap halfer certifier, caused by immorph channels for the heap halfer certifier in the products. (NF 2023-1977) products Ibm - multiple products IbM AT Connect Y10.0.5.3 and Y10.0.6.0 stores user ordentials in Connect Y10.0.5.3 and Y10.0.6.0 stores user ordentials y10.0.5 and y10		<u> </u>	ah saling which savid allows to the control of the			
bith - multiple products Description						
Min		there are the t	a heap buffer overflow, caused by improper bounds checking			
BMAP Connect V10.0.5.3 and V10.0.6.0 stores user credentals in browser acade which can be read by a local user. IRM X-force ID 273912. Discover acade which can be read by a local user. IRM X-force ID 273912. Discover acade which can be read by a local user. IRM X-force ID 273912. Discover acade which can be read by a local user. IRM X-force ID 273912. Discover and ID 27	CVF-2023-28527			2023-12-09	5.5	Medium
CVE-2023-49329 products 271917. 271919 S.75 Medium divers/acce/habanadabs/scort/n banababs, socitic in the linux diversed by the society of the second potentials of a slew as information leak to user space because info-pago is not intribated. powerproted_data	<u> </u>	products		2020 12 03	3.3	Mediam
se_etst_info in directs/acts/habanabs/common/habanabs/joctLc in the Linux kernel directs/habanabs/common/habanabs/joctlc in the Linux kernel directs/habanabs/common/haba	CVE 2022 47722		,	2022 42 00		
Inux - Inux Lenux	CVE-2023-47722	products		2023-12-09	5.5	Medium
Del DMS500 5.14.0.0 and prior contrat a Reflected Cross-Sife Scripting Vulnerability. A network attacker with two privileges could potentially exploit this vulnerability, leading to the execution of malicious. HIMI. of avalority for oils in a victim unsers web provage of the province of malicious. HIMI. of avalority for oils in a victim unsers web provage of the country of malicious HIMI. of avalority for oils in a victim unsers web province of malicious. HIMI. of avalority for oils in a victim unsers web province oils a victim unsers web province of the country of the vulnerability could be remotely exploited from the country of the vulnerability country (victim). A patient of the vulnerability country (victim) of the vulnerability and been intended in Micro Foots. Arcsight Management Center. In wunnerability and be remotely exploited resulting in stored Cross Site Scripting MSS. VCF 2023 42579 victim of the vulnerability and the vulnerability and province of the vulnerability and victim of the vulnerability requires a microsification of the server to be present as of tending the vulnerability and victim of the vulnerability and the vulnerability and the vic						
Del DMS500 5.14.0.0 and prior contain a Reflected Cross Site Scripting Valnerability. A network attacker with low privileges could potentially specific this valnerability. Jeading to the execution of microsoft provinger description of microsoft and provinger description. The context of the vulnerability and the execution of microsoft and provinger description. The context of the vulnerability cannot be executed by the product of the voltage of the context of the vulnerability and the execution of microsoft and provinger description. The vulnerability could be remotely explored resulting an according in 2004 of the 2002 of the context of the vulnerability and the emotely explored resulting in 2004 of the 2002 of the 2	CVE 2002 F0424		,	2022 42 00		
Scripting Vulnerability. A network attacker with low privileges could potentially exploit this unkerability, leading to the execution of malidous FITML or savsScript code in a victim user's web powerprotect, data manager, dm5500 protects of malidous FITML or savsScript code in a victim user's web provision of malidous FITML or savsScript code in a victim user's web provision of malidous FITML or savsScript code in a victim user's web provision of malidous FITML or savsScript code in a victim user's web provision of malidous FITML or savsScript code in a victim user's web provision of malidous FITML or savsScript code in a victim user's web provision of malidous FITML or savsScripting M2S1. CVE-2023-43579 products and savs savs savs savs savs savs savs sav	CVE-2023-50431	linux - linux_kernel	because info->padU is not initialized.	2023-12-09	5.5	Medium
CVE 2023-4430 microsoft - multiple CVE 2023-42579 microsoft - multiple CVE 2023-42582 microsoft - multiple CVE 2023-42583 microsoft - graph A 2023-12584 microsoft - graph Microsoft - multiple CVE 2023-42583 microsoft - graph Microsoft - multiple CVE 2023-42583 m			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			
cive 2023-44390 firmware microfocus - arcsight, managem of a Aptential universability has been identified in Micro Focus arcsight, managem of Aptential universability has been identified in Micro Focus of Aptential universability and the service of Communication of Communicatio						
Arsight Management Center. The vulnerability could be remotely exploited residuling in store Gross Site Scripting RSS). Unproper usage of insecure protocol (i.e. HTPP) in SogouSDK of Chineses Samsung Reyboard off orto for versions \$3.70.1 in Android 12, and 5.6.00.52. Samsung - multiple products EVE-2023-42579 Arsian Site of Sit	CVE-2023-44301		client-side request forgery.	2023-12-04	5.4	Medium
ent_center exploited_resulting in stored_Cross_Site_Scripting_KSS). Ent_color			· ·			
Improper usage of Insecure protocol (Le. HTTP) in SogouSDK of Chineses Samsung Keyboard or for to versions \$3.70.1 in Android 12, and \$6.00.52. \$5.61.04.2, \$7.00.45 in Android 12, and \$6.00.52. \$5.61.04.2, \$7.00.45 in Android 12, and \$6.00.52. \$5.61.04.2, \$7.00.45 in Android 13 allows adjocent attackers to access keystroke data using Man-in-the-Middle attack. msgrah-skie-ph is the Microsoft Graph Interny for PIP. The Microsoft Graph PIP SDK published packages which contained test code that enabled the use of the phiprioff function from any application that could access and execute the file at vendor/microsoft/microsoft-paph/test/See/Pephinfor.php. The phipriof function exposes system information. The vulnerability affects the GetPhipling of pictor paph feet SpC SDK which contains a call to the phipriofig function. This vulnerability requires a misconfiguration of the server to be presents to it can be exploited. For example, making the PIP 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 phipriofig method. The attacker would then be able to get access to system information like configuration modules, and environment' vursibles and later on use the compromised secrets to access additional data. This problem has been patched in versions 1.109.1 and 2.0 erc. Si na immediate deployment with the updated vendor package is not available, you can perform the following temporal y workinorounstic effect the vendor/microsoft/mi	CVE-2020-25835		, ,	2023-12-09	5.4	Medium
samsung - multiple Solid 2, 5.00.05 is in Android 12, and 5.00.52 Somsung - multiple Solid 2, 5.00.04 is in Android 13 allows adjacent attackers to access keystroke data using Man-in-the-Middle attack. Migraph-Solid kph is the Microsoft Graph Itary for PIP. The Microsoft Graph PIP SDK published packages which contained test code that enabled the use of the phalnfol/ function from any application that could access and execute the file at vendor/microsoft/microsoft/microsoft/graph/test/GetPhplinC.php. The phplind function exposes system information like accessible. The combination of the eylinerability affects the GetPhplinfo, phy script of the PIP SDK which contains a call to the phplinfol/ function. This vulnerability requires a misconfiguration or the server to be present so it can be expolited. For example, making the PIP 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 phplinfol/ 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-RCS. If an immediate deployment with the updated vendor package is not available, you can perform the following temporary workarounds: delete the vendor/microsoff/microsoff-graph-tests/feethplinfo.php in file remove access to the invendor directory, or disable the phpinto function. Microsoft Graph beta PIP SDK published packages which contained test code that enabled the use of the phplinfol function from any application that could access and execute the file at vendor/microsoff/microsoff-graph-core to the phplinfol function. This vulnerability requires a misconfiguration would allow an attacker to craft an HTTP request that executes the phplinfol purched. The attacker would then be able to get access to system information like configuration, mo		_	Improper usage of insecure protocol (i.e. HTTP) in SogouSDK of			
samsung - multiple products S. 6.10.42, 5.70.04.5 in Android 13 allows adjacent attackers to access keytroke data using Mani-rith-re-Midle attack. See Seytroke data using Mani-rith-re-Midle attack.						
access keystroke data using Man-In-the-Middle attack. By access keystroke data using Man-In-the-Middle attack. By access keystroke data using Man-In-the-Middle attack. By access the Wicrosoft Graph PIP SDK published packages which contained test code that enabled the use of the phiprinfor function from any application that could access and execute the file at vendor/microsoft/microsoft/microsoft/press/GerPhiprinfo,php. The phiprinfo function exposes system information. The vulnerability affects the Gerphiprinfo,php script of the PIP SDK which contains a call to the phiprinfol function. This vulnerability requires a misconfiguration or of the server to be present so it can be expolited. For example, making the PIP application's yendor directory web accessible. The combination of the vulnerability and the server misconfiguration would allow an attacker to craft an HTTP request that executes the phiprinfol 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-RCS. If an immediate deployment with the updated vendor package is not available, you can perform the following temporary workarounds: delete the vendor/microsoft/microsoft/microsoft/microsoft/praph/tests/cettehpinfo.php if like remove access to the 'vendor' directory, or disable the phiprinfol function from any application that could access and execute the file at vendor/microsoft/microsoft/microsoft/praph/tests/cettehpinfo.php. The phiprinfo function exposes system information. The vulnerability affects the Gerbiphinfo.php price of the PIP SDK which contains a call to the phiprinfol function. This vulnerability affects the Gerbiphinfo.php price of the PIP SDK which contains a call to the phiprinfol function. This vulnerability affects the Gerbiphinfo.php call the problem and the server misconfiguration would allow an attacker to craft an HTTP request th		samsung - multiple				
Microsoft Graph PHP SDK published packages which contained test ode that enabled the use of the phiphifol function from any application that could access and execute the file at vendor/microsoft/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 phpinfol 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 phpinfol 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 2.00 PR.Cs. 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 Vendord' directory, or disable the phpinfol function from any application that could access and execute the file at 'vendor/microsoft/microsoft-graph-core/tests/GetPhpinfo.php'. 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 requires a misconfiguration of the server to be present so it can be exploited. For example, making the PHP split and the server misconfiguration would allow an attacker to craft an HTTP request that executes the phpinfol) 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 b	CVE-2023-42579		access keystroke data using Man-in-the-Middle attack.	2023-12-05	5.3	Medium
test code that enabled the use of the phiphifol function from any application that could access and execute the file at vendor/microsoft/microsoft-graph/tests/GetPhiphifo.php. The phiphifo function exposes system information. The vulnerability affects the GetPhiphifol, php script of the PPP SDK which contains a call to the phiphifol function. This vulnerability requires a misconfiguration of the server to be present so it can be exploited. For example, making the PPP 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 phiphifol (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 2.00 ARCS. If an immediate deployment with the updated vendor package is not available, you can perform the following temporary workarounds: delete the workor/microsoft-graph-core the Microsoft Graph beta phiphifol phip file, remove access to the /Vendor/indirectory, or disable the phiphifol function from any application that could access and execute the file at 'vendor/microsoft-graph-core the Microsoft Graph beta file at 'vendor/microsoft-graph-core developed by the phiphifol function from any application that could access and execute the file at 'vendor/microsoft/microsoft-graph-core/tests/GetPhiphifo.php. The phiphifol function and execute stemplands and execute stemplands and execute stemplands and the server misconfiguration of the server to be present so it can be exploited. For example, making the PPP 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 phiphifol method. The attacker would then be able to get access to system information like configuration, modules, and ev			1 - 1 - 1			
vendor/microsoft/microsoft/microsoft/microsoft/microsoft/microsoft/microsoft/microsoft/microsoft/microsoft/microsoft/microsoft/maps (high phinfo) function exposes system information. The vulnerability affects the GetPhinfo,php script of the PHP SDK which contains a call to the phinfo() function. This vulnerability requires a misconfiguration of the server to be presents oit 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 phinfo() 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-RCS. 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 the Microsoft Graph Library for PHP. The Microsoft Graph Beta PHP SDK published packages which contained test code that enabled the use of the phiprinfo() function from any application that could access and execute the file at 'vendor/microsoft/microsoft-graph-core/tests/GetPhinfo() function from any application that could access and execute the file at 'vendor/microsoft-graph-core/tests/GetPhinfo() function from any application that could access and execute the file at 'vendor/microsoft-graph-core/tests/GetPhinfo() function from any application that could access and execute the file at 'vendor/microsoft-graph-core/tests/GetPhinfo() function from any application out and access and execute the file at 'vendor/microsoft-graph-core/tests/GetPhinfo() function from any application out and access and execute the file at 'vendor/microsoft-graph-core/tests/GetPhinfo() function from any application out and access to the phinfo() method. The patched for exemple and the server micro			· · · · · · · · · · · · · · · · · · ·			
phplinfo function exposes system information. The vulnerability affects the GetPhplinfo phy script of the PIPL SDK which contains a call to the phplinfo) function. This vulnerability requires a misconfiguration would allow an attacker to raft an HTTP request that executes the phplinfo) function of the vulnerability and the server misconfiguration would allow an attacker to craft 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/GetPhplinfo,php' file, remove access to the 'vendor' directory, or disable the phpinfo from any application that could access and execute the file at 'vendor/microsoft/microsoft-graph-core/tests/GetPhplinfo,php'. The phplinfo function that could access and execute the file at 'vendor/microsoft/microsoft-graph-core/tests/GetPhplinfo,php'. The phplinfo function exposes system information. The vulnerability and the server misconfiguration would allow an attacker to craft an HTTP request that executes the phpinfo) function from any application that could access and execute the file at 'vendor/microsoft/microsoft-graph-core/tests/GetPhplinfo,php'. The phplinfo function exposes system information. The vulnerability and the server misconfiguration would allow an attacker to craft an HTTP request that executes the phpinfo) function file to explore that executes the phpinfo) function file to the vulnerability and the server misconfiguration would allow an attacker to craft an HTTP request that executes the phpinfo) function data. This problem has been patched in version 2.0.2. It 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/GetPhplinfo,php' file, remove access to the yendor directory, or disable the phpinfo function function. Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of			''			
affects the GetPhpInfo php script of the PNP SDK which contains a call to the pohinfol function. This vulnerability requires a misconfiguration of the server to be present so it can be exploited. For example, making the PNP 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 phpinfol 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-RCS. If an immediate deployment with the updated vendor package is not available, you can perform the following temporary workarounds: delete the vendor/microsoft/microso						
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 phiphifol 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-RCS. 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/GetPhplinfo php file, remove access to the /vendor/ directory, or disable the phplinfo function. Wicrosoft Graph Beta PHP SDK published packages which contained test code that enabled the use of the phplinfol/ function from any application that could access and execute the file at vendor/microsoft/microsoft-graph-core/tests/GetPhplinfo.php. The phplinfol/ function in the vulnerability affects the GetPhplinfol, php. The phplinfol function in the vulnerability affects the GetPhplinfol, php. The phplinfol function in the vulnerability affects the GetPhplinfol, php. The phplinfol function in the vulnerability affects the GetPhplinfol, php. The phplinfol function in the 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 phplinfol/ 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 availab			1 ' '			
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 phpinfol 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-RCS. If an immediate deployment with the updated vendor package is not available, you can perform the following temporary workinounds: delete the 'vendor/microsoft/microsoft-graph/tests/GetPhplnfo.php' file, remove access to the 'vendor' directory, or disable the phpinfo function. Microsoft apph-core the Microsoft Graph Library for PHP. The 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 phpinfol 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 phpinfol function. This vulnerability and the server 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 phpinfol/ method. The attacker would then be able to get access to the vendor package is not available, you can perform the following temporary workarounds: delete the 'vendor/microsoft/microsoft-graph-core/tests/GetPhpinfo,php file, and the server to be 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 te						
accessible. The combination of the vulnerability and the server misconfiguration would allow an attacker to craft an HTTP request that executes the phipinfol 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 2.00-RCS. 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/GetPhipinfo.php file, remove access to the 'Vendor' directory, or disable the phipinfo function. The microsoft are the Microsoft Graph Library for PHP. The Microsoft Graph Beta PHP SDK published packages which contained test code that enabled the use of the phipinfol function from any application that could access and execute the file at 'vendor/microsoft/microsoft-graph-core/tests/GetPhpinfo.php'. The phipinfo function exposes system information. The 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 phipinfol function 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 phpinfol function or 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 followin			, , ,			
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 2.0.2.0-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. CVE-2023-49282 microsoft of span 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/GetPhplinfo,php" file, remove access to the /vendor directory, or disable the phpinfo function A flaw was found in the Quarkus Cache Runtime. When request			, , , , , , , , , , , , , , , , , , , ,			
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 1.109.1 and 2.0.0-RCS. 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. microsoft - multiple products 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.ph 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/grapah-core/tests/GetPhplinfo,php' file, remove access to the /vendor directory, or disable the phpinfo tunction A flaw was found in the Quarkus Cache Runtime. When request						
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-RCS. 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. microsoft a PHP SDK published packages which contained test code that enabled the use of the phplinfol) function contained test code that enabled the use of the phplinfol) function from any application that could access and execute the file at Vendor/microsoft/microsoft-graph-core/tests/GetPhplinfo.php. The phplinfo function exposes system information The vulnerability affects the GetPhplinfo.php script of the PHP SDK which contains a call to the phplinfol 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 phpinfol 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 2.02.1 fan 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/GetPhplinfo,php" file, remove access to the /vendor directory, or disable the phpinfo function Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. A flaw was found in the Quarkus Cache Runtime. When request						
been patched in versions 1.109.1 and 2.0.0=RCS. 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. 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 resposes 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. Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. A flaw was found in the Quarkus Cache Runtime. When request						
deployment with the updated vendor package is not available, you can perform the following temporary workarounds: delete the 'vendor/microsoft/microsoft/microsoft/graph/tests/GetPhplnfo,php' file, remove access to the 'vendor' directory, or disable the phpinfo function. Microsoft Graph Seta 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/GetPhplnfo,php'. The phplnfo function exposes system information. The vulnerability affects the GetPhplnfo,ph 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 phinfo() 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/GetPhplinfo.php' file, remove access to the /vendor directory, or disable the phpinfo function Permission management vulnerability in the module for disabling brushed the products cause features to perform abnormally. Permission management vulnerability in the module for disabling sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally.			•			
can perform the following temporary workarounds: delete the Vendor/microsoft/microsoft/microsoft/ergraph/tests/GetPhpInfo.php file, remove access to the 'vendor' directory, or disable the phpinfo function. 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 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 Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. OVE-2023-6273 products as found in the Quarkus Cache Runtime. When request			· ·			
vendor/microsoft-multiple products prod						
CVE-2023-49282 products function. 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 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 Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. A flaw was found in the Quarkus Cache Runtime. When request			`vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php` file,			
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 phplnfo() function from any application that could access and execute the file at 'vendor/microsoft/microsoft-graph-core/tests/GetPhplnfo.php'. The phplnfo function exposes system information. The vulnerability affects the GetPhplnfo.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/GetPhplnfo.php' file, remove access to the /vendor directory, or disable the phpinfo function 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 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 2022 40202	· ·		2022 42 05	F 3	\
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/microsoff/microsoff-graph-core/tests/GetPhpInfo.php' file, remove access to the /vendor directory, or disable the phpinfo function Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may 2023-12-06 5.3 Medium redhat - A flaw was found in the Quarkus Cache Runtime. When request	<u>CVE-2U23-49282</u>	products		2023-12-05	5.3	iviedium
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 Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cuse features to perform abnormally. 2023-12-06 5.3 Medium A flaw was found in the Quarkus Cache Runtime. When request						
`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 Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may redhat - A flaw was found in the Quarkus Cache Runtime. When request						
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 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 redhat - A flaw was found in the Quarkus Cache Runtime. When request						
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 CVE-2023-49283 microsoft - graph function Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. A flaw was found in the Quarkus Cache Runtime. When request			The phpInfo function exposes system information. The			
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 CVE-2023-49283 microsoft - graph 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 redhat - A flaw was found in the Quarkus Cache Runtime. When request						
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 CVE-2023-49283 microsoft - graph 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 redhat - A flaw was found in the Quarkus Cache Runtime. When request			, , , , ,			
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 CVE-2023-49283 microsoft - graph function Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. CVE-2023-6273 products A flaw was found in the Quarkus Cache Runtime. When request			exploited. For example, making the PHP application's /vendor			
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 Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. A flaw was found in the Quarkus Cache Runtime. When request						
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 CVE-2023-49283 microsoft - graph function Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. CVE-2023-6273 products A flaw was found in the Quarkus Cache Runtime. When request						
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 CVE-2023-49283 microsoft - graph function Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. CVE-2023-6273 products redhat - A flaw was found in the Quarkus Cache Runtime. When request			would then be able to get access to system information like			
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 CVE-2023-49283 microsoft - graph function Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. CVE-2023-6273 products redhat - A flaw was found in the Quarkus Cache Runtime. When request						
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 CVE-2023-49283 microsoft - graph function Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. CVE-2023-6273 products A flaw was found in the Quarkus Cache Runtime. When request			· ·			
CVE-2023-49283microsoft - graphfunction2023-12-055.3MediumCVE-2023-6273Permission management vulnerability in the module for disabling Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally.2023-12-065.3MediumCVE-2023-6273ProductsCause features to perform abnormally.2023-12-065.3Medium			deployment with the updated vendor package is not available, you			
file, remove access to the /vendor directory, or disable the phpinfo function Permission management vulnerability in the module for disabling huawei - multiple Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. A flaw was found in the Quarkus Cache Runtime. When request file, remove access to the /vendor directory, or disable the phpinfo 2023-12-05 5.3 Medium 2023-12-06 5.3 Medium			, , ,			
CVE-2023-49283microsoft - graphfunction2023-12-055.3MediumPermission management vulnerability in the module for disabling huawei - multiple productsSound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally.2023-12-065.3MediumCVE-2023-6273productsCause features to perform abnormally.2023-12-065.3Mediumredhat -A flaw was found in the Quarkus Cache Runtime. When request						
huawei - multiple products cause features to perform abnormally. Sound Booster. Successful exploitation of this vulnerability may cause features to perform abnormally. Tedhat - A flaw was found in the Quarkus Cache Runtime. When request	CVE-2023-49283	microsoft - graph	function	2023-12-05	5.3	Medium
CVE-2023-6273productscause features to perform abnormally.2023-12-065.3Mediumredhat -A flaw was found in the Quarkus Cache Runtime. When request5.3Medium		1	,			
redhat - A flaw was found in the Quarkus Cache Runtime. When request	CVF-2023-6273	·	, , , , , , , , , , , , , , , , , , , ,	2023-12-06	5 2	Medium
CVE-2023-6393 build_of_quarkus processing utilizes a Uni cached using @CacheResult and the 2023-12-06 5.3 Medium	<u> </u>			_02J 1Z-00	ر.ر	iricululli
	CVE-2023-6393	build_of_quarkus	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 2022 42550	samsung - multiple	Improper exception management vulnerability in Knox Guard prior to SMR Dec-2023 Release 1 allows Knox Guard lock bypass via	2022 42 05	5.2	
CVE-2023-42559	products	changing system time. A vulnerability has been identified within Serv-U 15.4 that allows	2023-12-05	5.2	Mediur
CVE-2023-40053	solarwinds - multiple products	an authenticated actor to insert content on the file share function feature of Serv-U, which could be used maliciously.	2023-12-06	5	Mediur
	, ,	In Init of protocolcalladapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote			
CVE-2023-48397	google - android	information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	4.9	Mediur
		In Init of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote			
CVE-2023-48413	google - android	information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2023-12-08	4.9	Mediur
CVE-2023-36880	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2023-12-07	4.8	Mediur
	<u> </u>	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			
CVE-2023-42679	google - android	with System execution privileges needed	2023-12-04	4.4	Mediur
		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			
CVE-2023-42680	google - android	with System execution privileges needed In gsp driver, there is a possible out of bounds write due to a	2023-12-04	4.4	Mediur
CVE 2022 42692	google - multiple	missing bounds check. This could lead to local denial of service	2022 12 04	4.4	Madium
CVE-2023-42682	products	with System execution privileges needed In gsp driver, there is a possible out of bounds read due to a	2023-12-04	4.4	Mediur
CVE-2023-42683	google - multiple products	missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-12-04	4.4	Mediur
	·	In gsp driver, there is a possible out of bounds read due to a			
CVE-2023-42684	google - multiple products	missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-12-04	4.4	Mediur
		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			
CVE-2023-42724	google - android	with System execution privileges needed	2023-12-04	4.4	Mediur
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	Mediur
<u> </u>	8008.0 0.10.010	In TeleService, there is a possible out of bounds read due to a			
CVE-2023-42726	google - android	missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-12-04	4.4	Mediur
	google - multiple	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			
CVE-2023-42727	products	with System execution privileges needed	2023-12-04	4.4	Mediur
	google - multiple	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			
CVE-2023-42729	products	with System execution privileges needed In Gnss service, there is a possible out of bounds read due to a	2023-12-04	4.4	Mediur
CVE-2023-42731	google - multiple products	missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-12-04	4.4	Mediur
CVE-2023-42731	·	In telephony service, there is a possible missing permission check.	2023-12-04	4.4	ivieului
CVE-2023-42735	google - multiple products	This could lead to local information disclosure with System execution privileges needed	2023-12-04	4.4	Mediur
	·	In gnss service, there is a possible out of bounds write due to a			
CVE-2023-42751	google - multiple products	missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-12-04	4.4	Mediur
		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			
CVE-2023-32852	google - multiple products	interaction is not needed for exploitation. Patch ID: ALPS07670971; Issue ID: ALPS07670971.	2023-12-04	4.4	Mediur
		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			
CVE-2023-32856	google - multiple products	interaction is not needed for exploitation. Patch ID: ALPS07993705; Issue ID: ALPS07993705.	2023-12-04	4.4	Mediur
		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			
CVE-2023-32857	google - multiple products	interaction is not needed for exploitation. Patch ID: ALPS07993705; Issue ID: ALPS07993710.	2023-12-04	4.4	Mediur
	p. 044013	In GZ, there is a possible information disclosure due to a missing		1.7	caiai
CVE-2023-32858	google - android	data erasing. This could lead to local information disclosure with System execution privileges needed. User interaction is not	2023-12-04	4.4	Mediur

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

Where NCA provides the vulnerability information as published by وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.