

تمت مشاركة هذه المعلومة بإشارة مشاركة \*\*\*أبيض\*\*\* حيث يسمح بتبادلها Please note that this notification/advisory has been tagged as TLP \*\*\*WHITE\*\*\* where information can be shared or published on any public forums.

أو نشرها من خلال القنوات العامة.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للتُغرات المسجلة vulnerabilities by the National Institute of Standards and Technology the National Institute of Standards and Technology (NIST) من قبل (NIST) National Vulnerability Database (NVD) from 19 March to 26 للأسبوع من ١٩ مارس إلى ٢٦ National Vulnerability Database (NVD) مارس. ويتم تصنيف هذه الثغرات باستخدام معيار Vulnerability Common Vulnerability مارس. ويتم تصنيف هذه الثغرات باستخدام معيار 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

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

عالى جدًا: النتيجة الأساسية لـCVSS 9.0-10.01

عالى: النتيجة الأساسية لـ8.9-CVSS 7.0

متوسط: النتيجة الأساسية لـ6.9-CVSS 4.0

منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

CVE ID & Source	Vendor – Product	Description	Publish Date	CVSS Score	Severity
		IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1,			
		and 4.1.1 is vulnerable to SQL injection. A remote attacker could			
		send specially crafted SQL statements, which could allow the			
	ibm - multiple	attacker to view, add, modify or delete information in the back-			
CVE-2023-25684	products	end database. IBM X-Force ID: 247597.	2023-03-21	9.8	Critical
		Out of bounds memory access in WebHID in Google Chrome			
		prior to 111.0.5563.110 allowed a remote attacker to potentially			
	google -	exploit heap corruption via a malicious HID device. (Chromium			
CVE-2023-1529	chrome	security severity: High)	2023-03-21	9.8	Critical
		An issue was discovered in Samsung Baseband Modem Chipset			
	samsung -	for Exynos Modem 5123, Exynos Modem 5300, Exynos 980,			
	exynos_mode	Exynos 1080, and Exynos Auto T5125. Memory corruption can			
	m_5300_firm	occur when processing Session Description Negotiation for			
CVE-2023-26497	ware	Video Configuration Attribute.	2023-03-21	9.8	Critical
		A vulnerability in the web-based management interface of			
		ClearPass Policy Manager could allow an unauthenticated			
	arubanetwork	remote attacker to create arbitrary users on the platform. A			
0) /5 2022 25502	s - multiple	successful exploit allows an attacker to achieve total cluster	2022 02 22	0.0	0
CVE-2023-25589	products	compromise.	2023-03-22	9.8	Critical
		An issue was discovered in Samsung Baseband Modem Chipset			
		for Exynos Modem 5123, Exynos Modem 5300, Exynos 980,			
	samsung -	Exynos 1080, Exynos Auto T5126. Memory corruption can occur			
	exynos_mode	due to improper checking of the number of properties while			
CVE-2023-26498	m_5300_firm	parsing the chatroom attribute in the SDP (Session Description Protocol) module.	2023-03-23	9.8	Critical
CVE-2025-20498	ware	An issue was discovered in Samsung Baseband Modem Chipset	2023-03-23	9.6	Critical
		for Exynos Modem 5123, Exynos Modem 5300, Exynos 980,			
	samsung -	Exynos 1080, and Exynos Auto T5124. Memory corruption can			
	exynos_mode	occur due to improper checking of the parameter length while			
	m_5300_firm	parsing the fmtp attribute in the SDP (Session Description			
CVE-2023-26496	ware	Protocol) module.	2023-03-23	9.8	Critical
<u>CVL 2023 20 130</u>	tp-link - tl-	A command injection issue was found in TP-Link MR3020	2023 03 23	3.0	Critical
	mr3020_firm	v.1_150921 that allows a remote attacker to execute arbitrary			
CVE-2023-27078	ware	commands via a crafted request to the tftp endpoint.	2023-03-23	9.8	Critical
	-	Adobe ColdFusion versions 2018 Update 15 (and earlier) and			
		2021 Update 5 (and earlier) are affected by a Deserialization of			
	adobe -	Untrusted Data vulnerability that could result in arbitrary code			
	multiple	execution in the context of the current user. Exploitation of this			
CVE-2023-26359	products	issue does not require user interaction.	2023-03-23	9.8	Critical
		Adobe ColdFusion versions 2018 Update 15 (and earlier) and			
		2021 Update 5 (and earlier) are affected by an Improper Access			
	adobe -	Control vulnerability that could result in arbitrary code execution			
	multiple	in the context of the current user. Exploitation of this issue does			
CVE-2023-26360	products	not require user interaction.	2023-03-23	9.8	Critical
		In parseTrackFragmentRun() of MPEG4Extractor.cpp, there is a			
		possible out of bounds read due to an integer overflow. This			
	google -	could lead to remote escalation of privilege with no additional			
CVE-2022-20532	android	execution privileges needed. User interaction is not needed for	2023-03-24	9.8	Critical

A 232242891  In Prete cellular firmware, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code concellor with no additional concerning or profession of the control of t						
In Pixel cellular firmware, there is a possible out of bounds with due to a mising bounds check. This could lead to remote code execution with no additional execution privileges needed. Liter intendation is not needed for exploitation. Product. Androidversions: Android Seminary (1997) and products. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product. Androidversions: Android seminary (1997) and products. Androidversions. Android seminary (1997) and products. Seminary (1997) and products. Androidversions. Android seminary (1997) and products. Seminary (1997) and products. Androidversions. Android seminary (1997) and products. Seminary (1997) and products. Androidversions. Android			exploitation.Product: AndroidVersions: Android-13Android ID:			
due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation/industry and additional execution privileges needed. Android kernfeldendried ID: A 2022-30-324 9.8 Critic missing and additional execution privileges needed. User interaction is not needed for execution with no additional execution privileges needed. User interaction is not needed for exploitation in Product: Android Versions. Android kernfeldendried in Product. Android Versions. Android Versions and additional execution privileges needed. User interaction is not needed for exploitation in Product: Android Versions. Androi						
execution with no additional execution prolieges needed. User interaction is not needed for exploitation. Product Androidversions: Android SemelAndroid 10: A- 2023-03-24 9.8 Citie This could get in remote code execution with no additional execution prolieges needed. User interaction is not received for exploration. Product Androidversions: Android KernelAndroid 10: A- 2023-03-24 9.8 Citie OVE-2022-12499 android ID-A-2420319318references: IVA Citie Company of the control of the cont			· ·			
interaction is not needed for exploitation/induct. Androide/varions: Androide/ Androide/varions: Andro						
### Appointment of the control of th			, -			
In sam, SendMenCptrintkig of ams, MinconNainagement, Chere is a possible out of bounds write due to a heap buffer overlow. This could lead to remote code execution with no additional execution groups and additional execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android/defanded for exploitation of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution groups and the products of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges exposed and products. Android-Valance-Android 12, A258057881 and 18 pp. Additional color of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges exceeded. User interaction is not needed for exploitation. Product: Android-Valance-Android-12 Android-12 Android-						
is a possible out of bounds with due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for google-multiple out of bounds with due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. Liter interaction is not needed for expiration products. Android Vizines Android Vizines Android Vizines and Products in SPP_Additification of Control of the SPP_Additification of Control of the SPP_Additification of Control of the SPP_Additification of Control of SPP_Additification of SPP_Additification of Control of SPP_Additification	CVE-2022-42498	android	•	2023-03-24	9.8	Critical
This could lead to remote code execution with no additional execution projets product in exploitation. Product: Android/versions: Android kernelAndroid policy in exploration. Product: Android/versions: Android kernelAndroid policy in exploration. Product: Android/versions: Android kernelAndroid policy in exploration. Product: Android/versions: No more deed for exploitation with no additional execution provinges medicular interaction is not needed to remote code execution with no additional execution privileges medicular interaction. Product: Android/versions: Android 1.8. Android 1.8						
execution privileges needed. User interaction is not needed for application/forectic. Android/Versinos. Android kernel/Android (10- A-24001397References: IVA)  In gatt, process, presy writer, spot patt, cl.c., there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for products of the products						
Spogle						
On the content of t		google -	, •			
out of bounds write due to a missing bounds cheek. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration privileges needed. User interaction is not needed for exploration. Product: Admiration privileges needed user interaction is not needed for exploration. Product: Admiration privileges needed user interaction is not needed for exploration. Product: Admiration privileges needed user interaction is not needed for exploration. Product: Admiration privileges needed user interaction is not needed for exploration. Product: Admiration privileges needed user interaction is not needed for exploration. Product: Admiration privileges needed user interaction is not needed for exploration. Product: Admiration privileges needed user interaction is not needed for exploration. Product: Admiration privileges needed user interaction is not needed for exploration. Product: Admiration privileges needed user interaction is not needed for exploration. Product: Admiration privileg	CVE-2022-42499		·	2023-03-24	9.8	Critical
iead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation Product: Android/Versions: Android-11 Android-12 Android-12 Android-13 Android-13 Android-12 Android-13 Android-12 Android-13 A						
products products of respiciation Products Android/1.1 Android-1.2 (Product Android-1.1 Android-1.2 (Product Android-1.1 Android-1.2 (Product Android-1.2 (P						
multiple exploitation Product: Android-Versions: Android-12 2023-03-24 9.8 Critic Products Android-132 Android-12 Android-132 Android Interaction is not needed. Ose products Interaction is not not bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not not needed for exploitation Product: Android-12 Android-12 Android-12 Android-12 Android-13 Android Interaction is not not bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation Product: Android-Versions: Android kernelAndroid Interaction is not not execution with no additional execution privileges needed. User interaction is not needed for exploitation Product: Android-Versions: Android kernelAndroid Product Android-Versions: Android-Versions: Android kernelAndroid Product Android-Versions: Android kernelAndroid Product Android-Versions: Android kernelAndroid Product Android-Versions: Android-Versi						
Products			,			
In SDP AddAttribute of sig. db.c., there is a possible out of bounds wird eute to an incorrect bounds check. This could lead for remote code execution with no additional execution privileges needed. User interaction is not needed for expolation Product: Android-Versions: Android-11 Android-12 Android-12 Android-12 Android-13 Android In 2-261867788    In PROSNDE-comTcpSACOption of RohePacketCommon, there is a possible out of bounds wirds due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation Product. Android-Versions: Android KernelAndroid In Issan Sendfricegui/assist of Issan bounds which exist in the country of the possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation Product. Android-Versions: Android KernelAndroid In Issan Sendfricegui/assist of Issan born assiste, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation Product. Android-Versions: Android KernelAndroid In Android In Issan Sendfricegui/assist of Issan born and Issan Sendfricegui/assist of Issan Sendfricegui/assist	CVF-2023-20951	•	· ·	2023-03-24	9.8	Critical
bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Androidversions: Android 13 Android 12 Android 12. Android 13. Android 13. Android 14. Android 12. Android 12. Android 14. Android 15. A	<u> </u>	products		2020 00 2 1	3.0	Cricical
geogle - multiple products   name						
multiple products   Android-11 Android-12 Android-12 Android-13 Android Dandroid ID - A-28186778   2023-03-24   9.8   Critic			to remote code execution with no additional execution privileges			
CYE-2023-20954   products   13Android ID: A-2618667748   2023-03-24   9.8   Critic			·			
In Profisi/DecomTrpSA/Coption of RohePacketCommon, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android-Versions: Android kernelAndroid ID: A-244450648refereness: N/A 2023-03-24 9.8 Critic in Icsm, SendRARQuilAssist of Icsm, born assist.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation Froduct: Android/versions: Android kernelAndroid ID: A-246169606References: N/A 2023-03-24 9.8 Critic TensorFlow and ID: A-246169606References: N/A 2023-03-24 9.8 Critic TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, there is a heap buffer overflow in TaRy@poolGrad. Aft is included in TensorFlow 2.12.0 and 2.11.1. TensorFlow with a public proversion and advances heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and will also cherrypick this commit or TensorFlow version 2.12.0 and will also cherrypick this commit or TensorFlow version 2.12.0 and will also cherrypick this commit or TensorFlow version 2.12.0 and will also cherrypick this commit or TensorFlow version 2.12.0 and will also cherrypick this commit or TensorFlow version 2.12.0 and will also cherrypick this commit or TensorFlow version 2.12.0 and will also cherrypick this commit or TensorFlow version 2.12.0 and will also cherrypick this commit or TensorFlow version 2.12.0 and will also the restore the tensor of the path of the	CVE 2022 2005 4	•		2022 02 24	0.0	Catation
a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation Product. Androidversions: Android kernelAndroid ID: A-244450646References: N/A  In Issm. SendRrAcquiAssist of Issm. bcm_assist.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation Product: Androidversions: Android kernelAndroid ID: A-246169606References: N/A  Personation Product: Androidversions: Android kernelAndroid ID: A-246169606References: N/A  TensorFlow is an open source platform for machine learning. Prior to resions: 2.12.0 and 2.11.1. there is a heap buffer overflow in TawgPoolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1.  TensorFlow is an open source platform for machine learning. Attackers using TensorFlow prior to 2.12.0 or 2.11.1 can access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and will also otherwipick this committed to a process heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and will also otherwipick this committed to a process heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and will also otherwipick this committed to a process heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and will also otherwipick this committed to a process heap memory which is not in the control of user, leading to a crash or remote code execution when a victime version 2.12 and and will an additional to the past serving to the past serving to the past serving	CVE-2023-20954	products		2023-03-24	9.8	Critical
This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions; Android kernelAndroid 1D: A-244450646References; NA 1 in Icsm. SendRrAcquiAssist of Icsm. bcm_assist.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid 2023-03-24 9.8 Critic 1 in Icsm. Product Products and Confederation is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid 2023-03-24 9.8 Critic 1 in Icsm. Product Products (Products in Icsm. Products and Products in Icsm. Products in Icsm						
execution privileges needed. User interaction is not needed for exploitation Product: Android Versions: Android kernelAndroid 10: A-244450645References: N/A 2023-03-24 9.8 Critic Inc. SenderAcquiAssist of Ism_bcm_assist.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android kernelAndroid 2023-03-24 9.8 Critic Inc. Acid Self-Self-Self-Self-Self-Self-Self-Self-			,			
cyti-2023-21057 android iD: A-244505646References: V/A in Icsm_SendfirAcquiAssist of Icsm_bern_assist.c, there is a possible out of blounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: Android/versions: Android kernelAndroid in: A-246169606References: N/A  TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, there is a heap buffer overflow in TAygPolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1.  TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, there is a heap buffer overflow in TAygPolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1.  TensorFlow is in open source platform for machine learning. Attackers using Tensorflow prior to 2.12.0 or 2.11.1 can access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.1.1 and the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.1.1 and the control of user, leading to a vulnerable to a brute-force attack that leads to a password reset on IDM applications.  A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server reception 6.00.23040 and prior), IGSS baths of a password to the Data Server reception of a pathamete to a feet of the Data Server reception of the Data Server						
In Icsm_SendBrAcquiAssist of Icsm_bern_assist.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android Version		google -				
possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android KernelAndroid 10: A-246169606References: N/A  TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, three is a heap buffer overflow in TavgPoolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1. The same purpose overflow in TavgPoolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1. The same purpose overflow in TavgPoolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1. The same purpose overflow in TavgPoolGrad. A fix is included in TensorFlow is an open source platform for machine learning. Attackers using TensorFlow prior to 2.12.0 or 2.11.1 can access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.11.1.  Zoho ManageEngline ADSelfService Plus through 6203 is unlerable to a brute-force attack that leads to a password reset on IDM applications.  A CWE-305: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Dashboard(DashBoard-exe)(V16.0.0.23040 and prior), LGSS Dashboard(DashBoard-exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dlll)(V16.0.0.23040 and prior), Custom Reports(	CVE-2023-21057	android	·	2023-03-24	9.8	Critical
could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid 10: A-246165606References. N/A 2023-03-24 9.8 Critic Products of the Prior to versions 2.12.0 and 2.11.1, there is a heap buffer overflow in TavgBoolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1, there is a heap buffer overflow in TavgBoolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1 there is a heap buffer overflow in TavgBoolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1 there is a heap buffer overflow in TavgBoolGrad. A fix is included in TensorFlow in TavgBoolGrad. A fix is included in TensorFlow in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and the TensorFlow ve						
execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernelAndroid 1D: A-246169608References: N/A 2023-03-24 9.8 Critic TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, there is a heap buffer overflow in TaygboolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1, there is a heap buffer overflow in TaygboolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1 an access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and vill also cherrypick this commit on TensorFlow version 2.12.0 and vill also cherrypick this commit on TensorFlow version 2.12.0 and vill also cherrypick this commit on TensorFlow version 2.11.1 and access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and vill also cherrypick this commit on TensorFlow version 2.12.0 and vill also cherrypick this commit on TensorFlow version 2.12.0 and vill also cherrypick this commit on TensorFlow version 2.11.1 and version 2.11.1 an			· ·			
google- google- google- tensorflow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, there is a heap buffer overflow in TAvgPoolGrad. A fix is included in Tensorflow 2.12.0 and 2.11.1.  Tensorflow in TavgPoolGrad. A fix is included in Tensorflow 2.12.0 and 2.11.1.  Tensorflow is an open source platform for machine learning. Attackers using Tensorflow prior to 2.12.0 or 2.11.1 can access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.12.0 and will also cherrypick this version 2.12.0 and will also cherrypick this version 2.1						
Dr. A-24619606References: N/A   2023-03-24   9.8   Critic   TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, there is a heap buffer overflow and 2.11.1   2023-03-25   9.8   Critic   2023-25664   TensorFlow   2.11.1   2023-03-25   9.8   Critic   2023-25664   TensorFlow   2.11.1   2023-03-25   9.8   Critic   2023-25666   TensorFlow   2.11.1   2023-03-25   9.8   Critic   2023-25668   TensorFlow   2.11.1   2023-03-25   9.8   Critic   2023-25668   TensorFlow   2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick this commit on TensorFlow version 2.12.0 and valid also cherypick valid this provide valid this provide valid va		google -	. •			
Prior to versions 2.12.0 and 2.11.1, there is a heap buffer overflow in TAyspoolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1.  TensorFlow is an open source platform for machine learning. Attackers using TensorFlow prior to 2.12.0 or 2.11.1 can access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in google - TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.11.1  Zoho ManageEngine ADSelfService Plus through 6203 is will also cherrypick this commit on TensorFlow version 2.11.1  Zoho ManageEngine ADSelfService Plus through 6203 is vill also cherrypick this commit on TensorFlow version 2.11.1  Zoho ManageEngine ADSelfService Plus through 6203 is on IDM applications.  A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a mallicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)[VIG.0.0.23040 and prior), Custom Reports(RMSIG.dll][VIG.0.0.23040 and prior)  A CWE-2013-27982 products Reports (RMSIG.dll)[VIG.0.0.23040 and prior), Custom Reports (RMSIG.dlll)[V	CVE-2023-21058		·	2023-03-24	9.8	Critical
google- tensorflow and 2.11.1.  TensorFlow is an open source platform for machine learning. Attackers using Tensorflow prior to 2.12.0 or 2.11.1 can access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.11.2 and will also cherrypick this commit or TensorFlow version 2.11.1.  Zohocorp- multiple  CVE-2023-25668  CVE-2023-36413  Tohocorp- multiple  Schneider- electric- multiple  CVE-2023-27980  Tohocorp- multiple  CVE-2023-27980  Tohocorp- multiple  CVE-2023-27980  Tohocorp- multiple  CVE-2023-27982  Tohocorp- multiple  CVE-2023-27982  Tohocorp- multiple  Tohocorp- multiple  CVE-2023-27982  Tohocorp- multiple			TensorFlow is an open source platform for machine learning.			
CVE-2023-25664   tensorflow   and 2.11.1.   TensorFlow   and 2.11.1.   TensorFlow   and 2.11.1.   TensorFlow   and pensor   TensorFlow   and pensor   tensorFlow   and pensor   tensorFlow   tensorFlo			·			
TensorFlow is an open source platform for machine learning. Attackers using Tensorflow prior to 2.12.0 or 2.11.1 can access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in Tensorflow version 2.11.1.  zohocorp- Zohocorp- Zohocorp- multiple products  A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server (IGSSdataServer.exe)(V16.00.23040 and prior), GSS Data Server (IGSSdataServer.exe)  A CWE-3023-27980 Products  A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server (IGSSdataServer.exe) (V16.00.23040 and prior), IGSS Data Server(IGSSdataServer.exe) (V16.00.23040 and prior), IGSS Data Server (IGSSdataServer.exe) (V16.00.23040 and prior), IGSS Data Server (IGSSdataSe			9			
Attackers using Tensorflow prior to 2.12.0 or 2.11.1 can access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in Tensorflow version 2.12.0 and will also cherrypick this commit on Tensorflow version 2.11.1.  Zoho WanageEngine ADSelfService Plus through 6203 is vulnerable to a brute-force attack that leads to a password reset on IDM applications.  A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Dashoard(DashBoard exe)(V16.0.0.23040 and prior), IGSS Dashoard(DashBoard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Server IGSSdataServer.exe)(V16.0.0.23040 and p	CVE-2023-25664	tensorflow		2023-03-25	9.8	Critical
heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in remosrFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.11.1.  Zohocorp - Zoho			, , ,			
crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.11.1.  Zoho ManageEngine ADSelfService Plus through 6203 is vulnerable to a brute-force attack that leads to a password reset on IDM applications.  A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior)  A CWE-303-27980 Products Reports(RMS16.dll)(V16.0.0.23040 and prior)  A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), GSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS D			,			
CVE-2023-25668 tensorflow on TensorFlow version 2.11.1.  Zoho ManageEngine ADSelfService Plus through 6203 is multiple products on IDM applications.  A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior)  CVE-2023-27980 Products A CWE-305: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports RMS16.dll)(V16.0.0.23040 and prior), Custom Reports R			, , ,			
zohocorp - multiple vulnerable to a brute-force attack that leads to a password reset vulnerable to a brute-force attack that leads to a password reset on IDM applications.  A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior).  CVE-2023-27980 Products Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard schneider-electric multiple products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), IGSS Dashboar		google -	TensorFlow version 2.12.0 and will also cherrypick this commit			
multiple products on IDM applications. 2023-03-23 9.1 Critical Function vulnerable to a brute-force attack that leads to a password reset on IDM applications. 2023-03-23 9.1 Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Products Reports(RMS16.dll)(V16.0.0.23040 and prior) 2023-03-21 8.8 Hig A CWE-2023-27980 A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victime ventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Peports MarkSf6.dll)(V16.0.0.23040 and prior), Custom Peports MarkSf6.dll)(V16.0.0.23040 and prior), Custom Peports MarkSf6.dll)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer	CVE-2023-25668			2023-03-25	9.8	Critical
CVE-2022-36413 products on IDM applications.  A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer exe)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior)  A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).  CVE-2023-27982 Products Reports(RMS16.dll)(V16.0.0.23040 and prior). 2023-03-21 8.8 Hig A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Server(I		•				
A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior) 2023-03-21 8.8 Hig A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). 2023-03-21 8.8 Hig A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior	CVE 2022 20412	•	·	2022 02 22	0.1	Cuitinal
vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dII)(V16.0.0.23040 and prior) (Sustom Reports) (Sustance and Interval and	<u>CVE-ZUZZ-30413</u>	products		ZUZ3-U3-Z3	9.1	Critical
allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS pashboard(DashBoard.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom products Reports(RMS16.dll)(V16.0.0.23040 and prior)  A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Schneider-electric Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).  CVE-2023-27982 Products Reports(RMS16.dll)(V16.0.0.23040 and prior), IGSS Data a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data Schneider-electric Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Schneider-electric Schn						
report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), IGSS Data Server (IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports Repo			· ·			
electric - multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior)  A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).  CVE-2023-27982 products Reports(RMS16.dll)(V16.0.0.23040 and prior). 2023-03-21 8.8 Hig A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), Custom Reports Path Could Cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), Custom Reports Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Cust						
multiple products   Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior)   2023-03-21   8.8   Hig			, ,			
CVE-2023-27980 products Reports(RMS16.dll)(V16.0.0.23040 and prior)  A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), Custom Products Reports(RMS16.dll)(V16.0.0.23040 and prior).  CVE-2023-27982 products Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data electric Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Data Reports(RMS16.dll)(V16.0.0.23040 and prior), IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), Custom Reports Reports(RMS16.dll)(V16.0.0.23040 and prior).			, , , , , , , , , , , , , , , , , , , ,			
A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-20: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).	CVE 2022 27000	•		2022 02 24	0.0	ماد: ۱۱
vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Products Products Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data electric Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports factor Products Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports factor Products Reports(RMS16.dlll)(V16.0.0.23040 and prior), Custom Reports factor Products Reports(RMS16.dlll)(V16.0.0.23040 and prior).	CVE-2023-2/980	products		2023-03-21	ბ.ბ	High
manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data electric - Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data electric - Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dlll)(V16.0.0.23040 and prior).			,			
directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data electric - Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Products Reports(RMS16.dll)(V16.0.0.23040 and prior). 2023-03-21 8.8 Hig A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data electric - Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and Prior), Custom Reports(			· ·			
execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data electric - Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data electric - Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Products: Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).			directory, when an attacker sends specific crafted messages to			
schneider- electric - Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom products Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious schneider- electric - server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-20: Improper Input Validation vulnerability exists in			·			
electric - multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data electric - Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).  CVE-2023-27981 Products Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-20: Improper Input Validation vulnerability exists in		1.	, .			
multiple products Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).  CVE-2023-27981 Products Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-20: Improper Input Validation vulnerability exists in						
CVE-2023-27982 products Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data electric - Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).  CVE-2023-27981 Products Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-20: Improper Input Validation vulnerability exists in			· · · · · · · · · · · · · · · · · · ·			
A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious schneider- report. Affected Products: IGSS Data electric - Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom CVE-2023-27981 products Reports(RMS16.dll)(V16.0.0.23040 and prior). 2023-03-21 8.8 Hig A CWE-20: Improper Input Validation vulnerability exists in	CVE-2023-27982	•		2023-03-21	8.8	High
a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data electric - Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Products Reports(RMS16.dll)(V16.0.0.23040 and prior).  A CWE-20: Improper Input Validation vulnerability exists in						
schneider- electric - multiple products CVE-2023-27981  Schneider- electric - multiple products Reports(RMS16.dll)(V16.0.0.23040 and prior), Custom A CWE-20: Improper Input Validation vulnerability exists in			, , , , , , , , , , , , , , , , , , , ,			
electric - Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Products Reports(RMS16.dll)(V16.0.0.23040 and prior). 2023-03-21 8.8 Hig A CWE-20: Improper Input Validation vulnerability exists in			•			
multiple Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom products Reports(RMS16.dll)(V16.0.0.23040 and prior). 2023-03-21 8.8 Hig A CWE-20: Improper Input Validation vulnerability exists in			·			
CVE-2023-27981productsReports(RMS16.dll)(V16.0.0.23040 and prior).2023-03-218.8HigA CWE-20: Improper Input Validation vulnerability exists in						
A CWE-20: Improper Input Validation vulnerability exists in	CVF-2023-27021	•		2023-03-21	2 2	High
	CVL 2023 21301	products		2023 UJ-ZI	0.0	111811
		schneider-	· · · · · · · · · · · · · · · · · · ·			
CVE-2023-27984 electric - potentially leading to remote code execution when a user opens 2023-03-21 8.8 Hig	CVE-2023-27984			2023-03-21	8.8	High

	multiple products	a malicious report file planted by an attacker. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior),			
		IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).			
CVE-2023-27874	ibm - multiple products	IBM Aspera Faspex 4.4.2 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote authenticated attacker could exploit this vulnerability to execute arbitrary commands. IBM X-Force ID: 249845.	2023-03-21	8.8	High
	netgear - rbs750_firmw	A command execution vulnerability exists in the access control functionality of Netgear Orbi Router RBR750 4.6.8.5. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger			
CVE-2022-37337	are	this vulnerability.  A command execution vulnerability exists in the hidden telnet	2023-03-21	8.8	High
	netgear - rbs750_firmw	service functionality of Netgear Orbi Router RBR750 4.6.8.5. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a network request to			
CVE-2022-38452	are	trigger this vulnerability.  Use after free in Passwords in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit heap	2023-03-21	8.8	High
CVE-2023-1528	google - chrome	corruption via a crafted HTML page. (Chromium security severity: High)	2023-03-21	8.8	High
CVE-2023-1530	google - chrome	Use after free in PDF in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)  Use after free in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit	2023-03-21	8.8	High
CVE-2023-1531	google - chrome	heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-03-21	8.8	High
<u> </u>	google -	Out of bounds read in GPU Video in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security	2023 03 21	0.0	
CVE-2023-1532	chrome	severity: High)  Use after free in WebProtect in Google Chrome prior to	2023-03-21	8.8	High
CVE-2023-1533	google - chrome	111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)  Out of bounds read in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had	2023-03-21	8.8	High
CVE-2023-1534	google - chrome	compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)  TXOne StellarOne has an improper access control privilege escalation vulnerability in every version before V2.0.1160 that sould allow a malicious falsely authoritisated year to associate his	2023-03-21	8.8	High
CVE-2023-25069	trendmicro - txone_stellaro ne	could allow a malicious, falsely authenticated user to escalate his privileges to administrator level. With these privileges, an attacker could perform actions they are not authorized to. Please note: an attacker must first obtain a low-privileged authenticated user's profile on the target system in order to exploit this vulnerability.  A vulnerability in the web-based management interface of ClearPass Policy Manager allows an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of this vulnerability allows an attacker to complete state-changing	2023-03-22	8.8	High
CVE 2022 25504	arubanetwork s - multiple	actions in the web-based management interface that should not be allowed by their current level of authorization on the	2022 02 22	0.0	112.15
CVE-2023-25594	products ibm - multiple	platform.  IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to perform actions that they should not have access to due to improper	2023-03-22	8.8	High
CVE-2023-25924	cisco - multiple	authorization. IBM X-Force ID: 247630.  A vulnerability in the management API of Cisco DNA Center could allow an authenticated, remote attacker to elevate privileges in the context of the web-based management interface on an affected device. This vulnerability is due to the unintended exposure of sensitive information. An attacker could exploit this vulnerability by inspecting the responses from the API. Under certain circumstances, a successful exploit could allow the attacker to access the API with the privileges of a higher-level user account. To successfully exploit this vulnerability, the	2023-03-22	8.8	High
CVE-2023-20055	products  google - multiple	attacker would need at least valid Observer credentials.  In launchDeepLinkIntentToRight of SettingsHomepageActivity.java, there is a possible way to launch arbitrary activities due to improper input validation. This could lead to local escalation of privilege with User execution privileges	2023-03-23	8.8	High
CVE-2023-20960	products	needed. User interaction is not needed for exploitation.Product:	2023-03-24	8.8	High

		AndroidVersions: Android-12L Android-13Android ID: A-			
		250589026 A vulnerability in the fragmentation handling code of tunnel			
		protocol packets in Cisco IOS XE Software could allow an			
		unauthenticated, remote attacker to cause an affected system			
		to reload, resulting in a denial of service (DoS) condition. This			
		vulnerability is due to the improper handling of large fragmented			
		tunnel protocol packets. One example of a tunnel protocol is			
		Generic Routing Encapsulation (GRE). An attacker could exploit			
		this vulnerability by sending crafted fragmented packets to an affected system. A successful exploit could allow the attacker to			
	cisco -	cause the affected system to reload, resulting in a DoS condition.			
	multiple	Note: Only traffic directed to the affected system can be used to			
CVE-2023-20072	products	exploit this vulnerability.	2023-03-23	8.6	High
		In the Linux kernel before 6.1.3, fs/ntfs3/record.c does not			
	linux -	validate resident attribute names. An out-of-bounds write may			
CVE-2022-48423	linux_kernel	OCCUR.	2023-03-19	7.8	High
	linux -	In the Linux kernel before 6.1.3, fs/ntfs3/inode.c does not validate the attribute name offset. An unhandled page fault may			
CVE-2022-48424	linux_kernel	occur.	2023-03-19	7.8	High
012 2022 10121	max_kerrier	In the Linux kernel through 6.2.7, fs/ntfs3/inode.c has an invalid	2020 00 13	7.0	111611
	linux -	kfree because it does not validate MFT flags before replaying			
CVE-2022-48425	linux_kernel	logs.	2023-03-19	7.8	High
		org-babel-execute:latex in ob-latex.el in Org Mode through 9.6.1			
		for GNU Emacs allows attackers to execute arbitrary commands			
CVE-2023-28617	gnu -	via a file name or directory name that contains shell metacharacters.	2023-03-19	7.8	High
CVL-ZUZ3-Z601/	org_mode	A CWE-502: Deserialization of Untrusted Data vulnerability exists	2023-03-19	7.0	High
		in the Dashboard module that could cause an interpretation of			
		malicious payload data, potentially leading to remote code			
		execution when an attacker gets the user to open a malicious			
	schneider-	file. Affected Products: IGSS Data			
	electric -	Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS			
CVE-2023-27978	multiple products	Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).	2023-03-21	7.8	High
<u>CVL 2023 27370</u>	products	A vulnerability in the ClearPass OnGuard Linux agent could allow	2023 03 21	7.0	111811
		malicious users on a Linux instance to elevate their user			
	arubanetwork	privileges to those of a higher role. A successful exploit allows			
	s - multiple	malicious users to execute arbitrary code with root level			_
CVE-2023-25590	products	privileges on the Linux instance.	2023-03-22	7.8	High
		Use After Free vulnerability in Linux kernel traffic control index filter (tcindex) allows Privilege Escalation. The imperfect hash			
		area can be updated while packets are traversing, which will			
		cause a use-after-free when 'tcf_exts_exec()' is called with the			
		destroyed tcf_ext. A local attacker user can use this vulnerability			
	linux -	to elevate its privileges to root. This issue affects Linux Kernel:			
CVE 2022 1201	multiple	from 4.14 before git commit	2022 02 22	7.0	l li ala
CVE-2023-1281	products	ee059170b1f7e94e55fa6cadee544e176a6e59c2.  A use-after-free flaw was found in Linux kernel before 5.19.2.	2023-03-22	7.8	High
		This issue occurs in cmd_hdl_filter in			
	linux -	drivers/staging/rtl8712/rtl8712_cmd.c, allowing an attacker to			
	multiple	launch a local denial of service attack and gain escalation of			
CVE-2022-4095	products	privileges.	2023-03-22	7.8	High
		Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are			
	adobe -	affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current			
	multiple	user. Exploitation of this issue requires user interaction in that a			
CVE-2023-25859	products	victim must open a malicious file.	2023-03-22	7.8	High
		Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are			<u> </u>
		affected by an out-of-bounds write vulnerability that could result			
	adobe -	in arbitrary code execution in the context of the current user.			
CVE 2022 25900	multiple	Exploitation of this issue requires user interaction in that a victim	2022 02 22	7.0	⊔i∼h
CVE-2023-25860	products	must open a malicious file.  Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are	2023-03-22	7.8	High
		affected by an out-of-bounds write vulnerability that could result			
	adobe -	in arbitrary code execution in the context of the current user.			
	multiple	Exploitation of this issue requires user interaction in that a victim			
CVE-2023-25861	products	must open a malicious file.	2023-03-22	7.8	High
		Creative Cloud version 5.9.1 (and earlier) is affected by an			
		Untrusted Search Path vulnerability that might allow attackers to			
		execute their own programs, access unauthorized data files, or modify configuration in unexpected ways. If the application uses			
		a search path to locate critical resources such as programs, then			
		an attacker could modify that search path to point to a malicious			
		an attacker could mount that search path to point to a mancious i	ļ		
		program, which the targeted application would then execute.			
CVE-2023-26358	adobe - creative_cloud		2023-03-22	7.8	High

		Illustrator version 26 F 2 (and earlier) and 27 2 0 (and earlier) are			
		Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by a Use After Free vulnerability that could result in			
	adobe -	arbitrary code execution in the context of the current user.			
	multiple	Exploitation of this issue requires user interaction in that a victim			
CVE-2023-26426	products	must open a malicious file.	2023-03-22	7.8	High
		A flaw was found in the Linux kernel, where unauthorized access			
		to the execution of the setuid file with capabilities was found in			
	12.	the Linux kernel's OverlayFS subsystem in how a user copies a			
	linux -	capable file from a nosuid mount into another mount. This uid mapping bug allows a local user to escalate their privileges on			
CVE-2023-0386	multiple products	the system.	2023-03-22	7.8	High
CVL 2023 0300	products	An issue was discovered in Veritas NetBackup before 10.0. A	2023 03 22	7.0	111811
		vulnerability in the way NetBackup validates the path to a DLL			
	veritas -	prior to loading may allow a lower level user to elevate privileges			
CVE-2023-28759	netbackup	and compromise the system.	2023-03-23	7.8	High
	linux -	An issue was discovered in the Linux kernel before 5.13.3.			
CVE-2023-28772	linux_kernel	lib/seq_buf.c has a seq_buf_putmem_hex buffer overflow.	2023-03-23	7.8	High
		A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could			
		allow an authenticated, local attacker to execute arbitrary			
		commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with			
		privileges to run commands could exploit this vulnerability by			
		first authenticating to an affected device using either local			
		terminal access or a management shell interface and then			
		submitting crafted input to the system CLI. A successful exploit			
		could allow the attacker to execute commands on the underlying			
		operating system with root-level privileges. An attacker with			
		limited user privileges could use this vulnerability to gain			
	_:	complete control over the system. Note: For additional			
CVE 2022 2002E	cisco -	information about specific impacts, see the Details section of this	2023-03-23	7.0	Hiah
CVE-2023-20035	ios_xe_sd-wan	advisory.  A vulnerability in the Cisco IOx application hosting subsystem of	2023-03-23	7.8	High
		Cisco IOS XE Software could allow an authenticated, local			
		attacker to elevate privileges to root on an affected device. This			
		vulnerability is due to insufficient restrictions on the hosted			
		application. An attacker could exploit this vulnerability by			
		logging in to and then escaping the Cisco IOx application			
	cisco -	container. A successful exploit could allow the attacker to			
	multiple	execute arbitrary commands on the underlying operating system			
CVE-2023-20065	products	with root privileges.	2023-03-23	7.8	High
		A use-after-free flaw was found in the Linux kernel's Ext4 File			
		System in how a user triggers several file operations simultaneously with the overlay FS usage. This flaw allows a local			
		user to crash or potentially escalate their privileges on the			
		system. Only if patch 9a2544037600 ("ovl: fix use after free in			
	linux -	struct ovl_aio_req") not applied yet, the kernel could be			
CVE-2023-1252	linux_kernel	affected.	2023-03-23	7.8	High
		Apache OpenOffice versions before 4.1.14 may be configured to			
	apache -	add an empty entry to the Java class path. This may lead to run			
CVE-2022-38745	openoffice	arbitrary Java code from the current directory.	2023-03-24	7.8	High
		Apache OpenOffice documents can contain links that call			
		internal macros with arbitrary arguments. Several URI Schemes			
		are defined for this purpose. Links can be activated by clicks, or			
		by automatic document events. The execution of such links must be subject to user approval. In the affected versions of			
		OpenOffice, approval for certain links is not requested; when			
	apache -	activated, such links could therefore result in arbitrary script			
CVE-2022-47502	openoffice	execution.	2023-03-24	7.8	High
	'	In parseParamsBlob of types.cpp, there is a possible out of			
		bounds write due to a missing bounds check. This could lead to			
		local escalation of privilege with no additional execution			
		privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:		_	
CVE-2022-20542	android	A-238083570	2023-03-24	7.8	High
		In onPackageAddedInternal of PermissionManagerService.java,			
		there is a possible way to silently grant a permission after a Target SDK update due to a permissions bypass. This could lead			
		to local escalation of privilege after updating an app to a higher			
		Target SDK with no additional execution privileges needed. User			
	google -	interaction is not needed for exploitation.Product:			
	multiple	AndroidVersions: Android-11 Android-12 Android-12L Android-			
CVE-2023-20906	products	13Android ID: A-221040577	2023-03-24	7.8	High
		In addPermission of PermissionManagerServiceImpl.java , there			<del>-</del>
		is a possible failure to persist permission settings due to resource			
	Ì	exhaustion. This could lead to local escalation of privilege with			
		, ,			
	google -	no additional execution privileges needed. User interaction is			
CVE-2023-20911	google - multiple products	, ,	2023-03-24	7.8	High

					T
		In onTargetSelected of ResolverActivity.java, there is a possible			
		way to share a wrong file due to a logic error in the code. This could lead to local escalation of privilege with no additional			
	google -	execution privileges needed. User interaction is not needed for			
	multiple	exploitation.Product: AndroidVersions: Android-11 Android-12			
CVE-2023-20917	products	Android-12L Android-13Android ID: A-242605257	2023-03-24	7.8	High
<u> </u>	p. calacte	In avdt_scb_hdl_write_req of avdt_scb_act.cc, there is a		7.0	
		possible out of bounds write due to a heap buffer overflow. This			
		could lead to local escalation of privilege with no additional			
	google -	execution privileges needed. User interaction is not needed for			
	multiple	exploitation.Product: AndroidVersions: Android-11 Android-12			
CVE-2023-20931	products	Android-12L Android-13Android ID: A-242535997	2023-03-24	7.8	High
		In bta_av_rc_disc_done of bta_av_act.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			
	google -	privileges needed. User interaction is not needed for			
	multiple	exploitation.Product: AndroidVersions: Android-11 Android-12			
CVE-2023-20936	products	Android-12L Android-13Android ID: A-226927612	2023-03-24	7.8	High
		In getGroupState of GrantPermissionsViewModel.kt, there is a			
		possible way to keep a one-time permission granted due to a			
		permissions bypass. This could lead to local escalation of			
		privilege with no additional execution privileges needed. User			
	google -	interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android			
CVE-2023-20947	multiple products	ID: A-237405974	2023-03-24	7.8	⊔iah
CVE-2025-20947	products		2023-03-24	7.0	High
		In onPrimaryClipChanged of ClipboardListener.java, there is a possible way to bypass factory reset protection due to incorrect			
		UI being shown prior to setup completion. This could lead to			
		local escalation of privilege with no additional execution			
		privileges needed. User interaction is needed for			
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:			
CVE-2023-20953	android	A-251778420	2023-03-24	7.8	High
<u>CVL 2023 20333</u>	unarora	In onPrepareOptionsMenu of AppInfoDashboardFragment.java,	2023 03 2 1	7.0	111811
		there is a possible way to bypass admin restrictions and uninstall			
		applications for all users due to a missing permission check. This			
		could lead to local escalation of privilege with no additional			
	google -	execution privileges needed. User interaction is not needed for			
	multiple	exploitation.Product: AndroidVersions: Android-11 Android-12			
CVE-2023-20955	products	Android-12L Android-13Android ID: A-258653813	2023-03-24	7.8	High
	·	In onAttach of SettingsPreferenceFragment.java, there is a			
		possible bypass of Factory Reset Protections due to a confused			
		deputy. This could lead to local escalation of privilege with no			
	google -	additional execution privileges needed. User interaction is not			
	multiple	needed for exploitation.Product: AndroidVersions: Android-11			
CVE-2023-20957	products	Android-12 Android-12LAndroid ID: A-258422561	2023-03-24	7.8	High
		In AddSupervisedUserActivity, guest users are not prevented			
		from starting the activity due to missing permissions checks. This			
		could lead to local escalation of privilege with no additional			
		execution privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:			_
CVE-2023-20959	android	A-249057848	2023-03-24	7.8	High
		In WorkSource, there is a possible parcel mismatch. This could			
		lead to local escalation of privilege with no additional execution			
	google -	privileges needed. User interaction is not needed for			
CVE 2022 200C2	multiple	exploitation.Product: AndroidVersions: Android-11 Android-12	2022 02 24	7.0	111.1
CVE-2023-20963	products	Android-12L Android-13Android ID: A-220302519	2023-03-24	7.8	High
		In multiple functions of MediaSessionRecord.java, there is a			
		possible Intent rebroadcast due to a confused deputy. This could lead to local denial of service or escalation of privilege with no			
	google -	additional execution privileges needed. User interaction is not			
	googie - multiple	needed for exploitation.Product: AndroidVersions: Android-12			
CVE-2023-20964	products	Android-12L Android-13Android ID: A-238177121	2023-03-24	7.8	High
<u> </u>	ρισαασιδ	In inflate of inflate.c, there is a possible out of bounds write due	2023-03-24	7.0	ıııgıı
		to a heap buffer overflow. This could lead to local escalation of			
		privilege with no additional execution privileges needed. User			
	google -	interaction is not needed for exploitation.Product:			
	multiple	AndroidVersions: Android-11 Android-12 Android-12L Android-			
CVE-2023-20966	products	13Android ID: A-242299736	2023-03-24	7.8	High
		In updatePermissionTreeSourcePackage of		<del></del>	
		PermissionManagerServiceImpl.java, there is a possible way to			
		obtain dangerous permission without the user's consent due to			
		a logic error in the code. This could lead to local escalation of			
		privilege with no additional execution privileges needed. User			
	google -	interaction is not needed for exploitation.Product:			
CVE-2023-20971	android	AndroidVersions: Android-13Android ID: A-225880325	2023-03-24	7.8	High
		In getAvailabilityStatus of		-	
		EnableContentCapturePreferenceController.lava. there is a l	ı.		
	google -	EnableContentCapturePreferenceController.java, there is a possible way to bypass DISALLOW CONTENT CAPTURE due to a			

					1
		privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:			
		AndroidVersions: Android-13Android ID: A-250573776			
		In BTA_GATTS_HandleValueIndication of bta_gatts_api.cc, there			
		is a possible out of bounds write due to improper input			
		validation. This could lead to local escalation of privilege with no			
		additional execution privileges needed. User interaction is not			
0) /5 2022 20225	google -	needed for exploitation.Product: AndroidVersions: Android-	2022 02 24	7.0	
CVE-2023-20985	android	13Android ID: A-245915315	2023-03-24	7.8	High
		In multiple functions of SnoozeHelper.java, there is a possible failure to persist settings due to an uncaught exception. This			
		could lead to local escalation of privilege with no additional			
		execution privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:			
CVE-2023-20993	android	A-261588851	2023-03-24	7.8	High
		In captureImage of CustomizedSensor.cpp, there is a possible			
		way to bypass the fingerprint unlock due to a logic error in the			
		code. This could lead to local escalation of privilege with no			
	google -	additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-			
CVE-2023-20995	android	13Android ID: A-241910279	2023-03-24	7.8	High
<u> </u>	<u> </u>	In MediaCodec.cpp, there is a possible use after free due to			
		improper locking. This could lead to local escalation of privilege			
		with no additional execution privileges needed. User interaction			
	google -	is not needed for exploitation.Product: AndroidVersions:			
CVE-2023-21000	android	Android-13Android ID: A-194783918	2023-03-24	7.8	High
		In onContextItemSelected of NetworkProviderSettings.java,			
		there is a possible way for users to change the Wi-Fi settings of			
		other users due to a missing permission check. This could lead to local escalation of privilege with no additional execution			
		privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:			
CVE-2023-21001	android	A-237672190	2023-03-24	7.8	High
		In getAvailabilityStatus of several Transcode Permission			
		Controllers, there is a possible permission bypass due to a			
		missing permission check. This could lead to local escalation of			
	googlo	privilege with no additional execution privileges needed. User			
CVE-2023-21002	google - android	interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193935	2023-03-24	7.8	High
<u>CVL 2023 21002</u>	anaroia	In getAvailabilityStatus of several Transcode Permission	2023 03 24	7.0	111611
		Controllers, there is a possible permission bypass due to a			
		missing permission check. This could lead to local escalation of			
		privilege with no additional execution privileges needed. User			
	google -	interaction is not needed for exploitation.Product:			_
CVE-2023-21003	android	AndroidVersions: Android-13Android ID: A-261193711	2023-03-24	7.8	High
		In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a			
		missing permission check. This could lead to local escalation of			
		privilege with no additional execution privileges needed. User			
	google -	interaction is not needed for exploitation.Product:			
CVE-2023-21004	android	AndroidVersions: Android-13Android ID: A-261193664	2023-03-24	7.8	High
		In getAvailabilityStatus of several Transcode Permission			
		Controllers, there is a possible permission bypass due to a			
		missing permission check. This could lead to local escalation of			
	g00g -	privilege with no additional execution privileges needed. User			
CVE-2023-21005	google - android	interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193946	2023-03-24	7.8	High
<u> </u>	anarola	In getAvailabilityStatus of several Transcode Permission	2023 03-24	7.0	111811
		Controllers, there is a possible permission bypass due to a			
		missing permission check. This could lead to local escalation of			
		privilege with no additional execution privileges needed. User			
	google -	interaction is not needed for exploitation.Product:			
CVE-2023-21015	android	AndroidVersions: Android-13Android ID: A-244569778	2023-03-24	7.8	High
		In InstallStart of InstallStart.java, there is a possible way to			
		change the installer package name due to an improper input validation. This could lead to local escalation of privilege with			
		User execution privileges needed. User interaction is not needed			
	google -	for exploitation.Product: AndroidVersions: Android-13Android			
CVE-2023-21017	android	ID: A-236687884	2023-03-24	7.8	High
		In isTargetSdkLessThanQOrPrivileged of WifiServiceImpl.java,			
		there is a possible way for the guest user to change admin user			
		network settings due to a missing permission check. This could			
		lead to local escalation of privilege with no additional execution			
Į.		privileges needed. User interaction is not needed for			ĺ
	google				
CVF-2023-21021	google -	exploitation.Product: AndroidVersions: Android-13Android ID:	2023-03-24	7 2	High
CVE-2023-21021	google - android	exploitation.Product: AndroidVersions: Android-13Android ID: A-255537598	2023-03-24	7.8	High
CVE-2023-21021		exploitation.Product: AndroidVersions: Android-13Android ID:	2023-03-24	7.8	High

	1				
		needed. User interaction is not needed for exploitation. Product:			
		AndroidVersions: Android-13Android ID: A-236098131			
		In maybeFinish of FallbackHome.java, there is a possible delay of			
		lockdown screen due to logic error. This could lead to local escalation of privilege with no additional execution privileges			
	google -	needed. User interaction is not needed for exploitation. Product:			
CVE-2023-21024	android	AndroidVersions: Android-13Android ID: A-246543238	2023-03-24	7.8	High
CVL 2023 21024	anaroia	In Confirmation of keystore_cli_v2.cpp, there is a possible way	2023 03 24	7.0	111811
		to corrupt memory due to a double free. This could lead to local			
		escalation of privilege in an unprivileged process with no			
		additional execution privileges needed. User interaction is not			
	google -	needed for exploitation.Product: AndroidVersions: Android-			
CVE-2023-21030	android	13Android ID: A-226234140	2023-03-24	7.8	High
		In multiple functions of SensorService.cpp, there is a possible			
		access of accurate sensor data due to a permissions bypass. This			
		could lead to local escalation of privilege with User execution			
		privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:			
CVE-2023-21034	android	A-230358834	2023-03-24	7.8	High
		In multiple functions of BackupHelper.java, there is a possible			
		way for an app to get permissions previously granted to another			
		app with the same package name due to a permissions bypass.			
		This could lead to local escalation of privilege with no additional			
		execution privileges needed. User interaction is not needed for			
0.45.55.5	google -	exploitation.Product: AndroidVersions: Android-13Android ID:		<u>-</u>	
CVE-2023-21035	android	A-184847040	2023-03-24	7.8	High
		In buildCommand of bluetooth_ccc.cc, there is a possible out of			
		bounds write due to a logic error in the code. This could lead to			
		local escalation of privilege with no additional execution			
		privileges needed. User interaction is not needed for			
CVE 2022 24040	google -	exploitation.Product: AndroidVersions: Android kernelAndroid	2022 02 24	7.0	1 1 : la
CVE-2023-21040	android	ID: A-238420277References: N/A	2023-03-24	7.8	High
		In append_to_params of param_util.c, there is a possible out of			
		bounds write due to an incorrect bounds check. This could lead			
		to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android kernelAndroid			
CVE-2023-21041	android	ID: A-250123688References: N/A	2023-03-24	7.8	High
CVL-2023-21041	android	In (TBD) of (TBD), there is a possible way to boot with a hidden	2023-03-24	7.0	riigii
		debug policy due to a missing warning to the user. This could lead			
		to local escalation of privilege after preparing the device, hiding			
		the warning, and passing the phone to a new user, with no			
		additional execution privileges needed. User interaction is not			
	google -	needed for exploitation.Product: AndroidVersions: Android			
CVE-2023-21068	android	kernelAndroid ID: A-243433344References: N/A	2023-03-24	7.8	High
	apache -	Excessive Iteration vulnerability in Apache Software Foundation			
	sling_resource	Apache Sling Resource Merger.This issue affects Apache Sling			
CVE-2023-26513	_merger	Resource Merger: from 1.2.0 before 1.4.2.	2023-03-20	7.5	High
		A CWE-345: Insufficient Verification of Data Authenticity		<del>-</del>	
		vulnerability exists in the Data Server that could cause access to			
		delete files in the IGSS project report directory, this could lead to			
		loss of data when an attacker sends specific crafted messages to			
	schneider-	the Data Server TCP port. Affected Products: IGSS Data			
	electric -	Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS			
	multiple	Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom			
CVE-2023-27977	products	Reports(RMS16.dll)(V16.0.0.23040 and prior).	2023-03-21	7.5	High
		A CWE-345: Insufficient Verification of Data Authenticity			
		vulnerability exists in the Data Server that could allow the			
		renaming of files in the IGSS project report directory, this could			
		lead to denial of service when an attacker sends specific crafted			
	schneider-	messages to the Data Server TCP port. Affected Products: IGSS			
	electric -	Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS			
	multiple	Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom			
CVE-2023-27979	products	Reports(RMS16.dll)(V16.0.0.23040 and prior).	2023-03-21	7.5	High
		IBM Aspera Faspex 4.4.2 could allow a remote attacker to obtain			
0.45	ibm - multiple				
CVE-2023-27871	products	specially crafted SQL query. IBM X-Force ID: 249613.	2023-03-21	7.5	High
		IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1,			
	ileans or to t	and 4.1.1 could allow an attacker to upload files that could be			
OVE 2022 25225	ibm - multiple	used in a denial of service attack due to incorrect authorization.	2022 02 04	<b>-</b> -	
CVE-2023-25923	products	IBM X-Force ID: 247629.	2023-03-21	7.5	High
		A security vulnerability has been identified in all supported			
		versions of OpenSSL related to the verification of X.509			
		certificate chains that include policy constraints. Attackers may			
		be able to exploit this vulnerability by creating a malicious			
		certificate chain that triggers exponential use of computational			
	openssl -	resources, leading to a denial-of-service (DoS) attack on affected			
CVE 2022 0464	multiple	systems. Policy processing is disabled by default but can be	2022 02 22	7 -	111:
CVE-2023-0464	products	enabled by passing the `-policy' argument to the command line	2023-03-22	7.5	High

		utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function.			
	cisco -	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A			
6) /5 2022 2020	multiple	successful exploit could allow the attacker to cause the device to	2022 02 22	7.5	
CVE-2023-20080	products google -	reload unexpectedly.  In serializePasspointConfiguration of PasspointXmlUtils.java, there is a possible logic error in the code. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID:	2023-03-23	7.5	High
CVE-2023-21027	android	A-216854451	2023-03-24	7.5	High
CVE-2023-21028	google - android	In parse_printerAttributes of ipphelper.c, there is a possible out of bounds read due to a string without a null-terminator. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-180680572  In sms_ExtractCbLanguage of sms_CellBroadcast.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional	2023-03-24	7.5	High
	google -	execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android			
CVE-2023-21053	android	ID: A-251805610References: N/A	2023-03-24	7.5	High
CVE-2023-21059	google - android	In EUTRAN_LCS_DecodeFacilityInformationElement of LPP_LcsManagement.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-247564044References: N/A  In sms_GetTpPile of sms_PduCodec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android kernelAndroid	2023-03-24	7.5	High
CVE-2023-21060	google - android	exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-253770924References: N/A	2023-03-24	7.5	High
CVE-2023-21061	google - android	Product: AndroidVersions: Android kernelAndroid ID: A-229255400References: N/A	2023-03-24	7.5	High
CVE-2023-21067	google - android	Product: AndroidVersions: Android kernelAndroid ID: A-254114726References: N/A	2023-03-24	7.5	High
CVE-2023-25658	google - tensorflow	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, an out of bounds read is in GRUBlockCellGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1.	2023-03-25	7.5	High
CVE-2023-25659	google - tensorflow	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, if the parameter 'indices' for 'DynamicStitch' does not match the shape of the parameter 'data', it can trigger an stack OOB read. A fix is included in TensorFlow version 2.12.0 and version 2.11.1.  TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, when the parameter 'summarize' of 'tf.raw_ops.Print' is zero, the new method 'SummarizeArray <bool>' will reference to a nullptr, leading to a</bool>	2023-03-25	7.5	High
CVE-2022-25660	google - tensorflow	seg fault. A fix is included in TensorFlow version 2.12 and version 2.11.1.	2023-03-25	7.5	High
CVE-2023-25660  CVE-2023-25662	google - tensorflow	TensorFlow is an open source platform for machine learning. Versions prior to 2.12.0 and 2.11.1 are vulnerable to integer overflow in EditDistance. A fix is included in TensorFlow version 2.12.0 and version 2.11.1.  TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, when `ctx->step_containter()` is a null ptr, the Lookup function will be	2023-03-25	7.5	High High
CVE-2023-25663	google - tensorflow	executed with a null pointer. A fix is included in TensorFlow 2.12.0 and 2.11.1.	2023-03-25	7.5	High
	google -	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, when `SparseSparseMaximum` is given invalid sparse tensors as inputs, it can give a null pointer error. A fix is included in			
CVE-2023-25665	tensorflow google -	TensorFlow version 2.12 and version 2.11.1.  TensorFlow is an open source platform for machine learning.  Prior to versions 2.12.0 and 2.11.1, there is a floating point exception in AudioSpectrogram. A fix is included in TensorFlow	2023-03-25	7.5	High
CVE-2023-25666	tensorflow	version 2.12.0 and version 2.11.1.	2023-03-25	7.5	High

<u></u>	T				T
		TensorFlow is an open source platform for machine learning.			
		Prior to versions 2.12.0 and 2.11.1, integer overflow occurs when			
	googlo	`2^31 <= num_frames * height * width * channels < 2^32`, for example Full HD screencast of at least 346 frames. A fix is			
CVE-2023-25667	google - tensorflow	included in TensorFlow version 2.12.0 and version 2.11.1.	2023-03-25	7.5	High
CVL-2023-23007	tensornow	TensorFlow is an open source platform for machine learning.	2023-03-23	7.5	riigii
		Prior to versions 2.12.0 and 2.11.1, if the stride and window size			
		are not positive for `tf.raw_ops.AvgPoolGrad`, it can give a			
	google -	floating point exception. A fix is included in TensorFlow version			
CVE-2023-25669	tensorflow	2.12.0 and version 2.11.1.	2023-03-25	7.5	High
		TensorFlow is an open source platform for machine learning.			
		Versions prior to 2.12.0 and 2.11.1 have a null point error in			
	google -	QuantizedMatMulWithBiasAndDequantize with MKL enabled. A			
CVE-2023-25670	tensorflow	fix is included in TensorFlow version 2.12.0 and version 2.11.1.	2023-03-25	7.5	High
		TensorFlow is an open source platform for machine learning.			
		There is out-of-bounds access due to mismatched integer type			
0.45 2022 25674	google -	sizes. A fix is included in TensorFlow version 2.12.0 and version	2022 02 25	7.5	
CVE-2023-25671	tensorflow	2.11.1.	2023-03-25	7.5	High
		TensorFlow is an open source platform for machine learning. The			
		function `tf.raw_ops.LookupTableImportV2` cannot handle			
CVE 2022 25672	google - tensorflow	scalars in the 'values' parameter and gives an NPE. A fix is included in TensorFlow version 2.12.0 and version 2.11.1.	2023-03-25	7 -	High
CVE-2023-25672	tensorriow		2023-03-25	7.5	High
		TensorFlow is an open source platform for machine learning.  Versions prior to 2.12.0 and 2.11.1 have a Floating Point			
	google -	Exception in TensorListSplit with XLA. A fix is included in			
CVE-2023-25673	tensorflow	TensorFlow version 2.12.0 and version 2.11.1.	2023-03-25	7.5	High
<u> </u>	CCTISOTTIOW	TensorFlow is an open source machine learning platform.	2023 UJ-ZJ	1.5	111811
		Versions prior to 2.12.0 and 2.11.1 have a null pointer error in			
	google -	RandomShuffle with XLA enabled. A fix is included in TensorFlow			
CVE-2023-25674	tensorflow	2.12.0 and 2.11.1.	2023-03-25	7.5	High
		TensorFlow is an end-to-end open source platform for machine			Ü
		learning. Constructing a tflite model with a paramater			
		`filter_input_channel` of less than 1 gives a FPE. This issue has			
	google -	been patched in version 2.12. TensorFlow will also cherrypick the			
CVE-2023-27579	tensorflow	fix commit on TensorFlow 2.11.1.	2023-03-25	7.5	High
		In getConfirmationMessage of DefaultAutofillPicker.java, there			
		is a possible way to mislead the user to select default autofill			
		application due to improper input validation. This could lead to			
		local escalation of privilege with no additional execution			
		privileges needed. User interaction is needed for			
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:			
CVE-2023-20976	android	A-216117246	2023-03-24	7.3	High
		A command execution vulnerability exists in the ubus backend			
	notaoar	communications functionality of Netgear Orbi Satellite RBS750			
	netgear - rbs750_firmw	4.6.8.5. A specially-crafted JSON object can lead to arbitrary command execution. An attacker can send a sequence of			
CVE-2022-36429	are	malicious packets to trigger this vulnerability.	2023-03-21	7.2	High
CVL-2022-30429	are	IBM QRadar SIEM 7.4 and 7.5 is vulnerable to privilege	2023-03-21	7.2	riigii
	ibm - multiple	escalation, allowing a user with some admin capabilities to gain			
CVE-2022-43863	products	additional admin capabilities. IBM X-Force ID: 239425.	2023-03-22	7.2	High
	p. 2 5 5 5 5 5	In EUTRAN_LCS_ConvertLCS_MOLRReq of LPP_CommonUtil.c,			0''
		there is a possible out of bounds write due to a logic error in the			
		code. This could lead to remote code execution with System			
		execution privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android kernelAndroid			
CVE-2023-21054	android	ID: A-244556535References: N/A	2023-03-24	7.2	High
	jenkins -	Jenkins AbsInt a <sup>3</sup> Plugin 1.1.0 and earlier does not configure its			
CVE-2023-28685	absint_a3	XML parser to prevent XML external entity (XXE) attacks.	2023-03-22	7.1	High
		An issue was discovered in Veritas NetBackup before 8.3.0.2.			
		BPCD allows an unprivileged user to specify a log file path when			
	veritas -	executing a NetBackup command. This can be used to overwrite			
CVE-2023-28758	netbackup	existing NetBackup log files.	2023-03-23	7.1	High
		In read_paint of ttcolr.c, there is a possible out of bounds read			
		due to a heap buffer overflow. This could lead to local			
		information disclosure with no additional execution privileges			
CVE 2022 20050	google -	needed. User interaction is not needed for exploitation. Product:	2022 02 24	7.4	11:
CVE-2023-20958	android	AndroidVersions: Android-13Android ID: A-254803162	2023-03-24	7.1	High
		A vulnerability in Trend Micro Endpoint Encryption Full Disk Encryption version 6.0.0.3204 and below could allow an attacker			
		with physical access to an affected device to bypass Microsoft			
		Windows? Secure Boot process in an attempt to execute other			
		attacks to obtain access to the contents of the device. An			
		attacks to obtain access to the contents of the device. An attacker must first obtain physical access to the target system in			
	trendmicro -	order to exploit this vulnerability. It is also important to note that			
	trend_micro_e	the contents of the drive(s) encrypted with TMEE FDE would still			
	ndpoint_encry	be protected and would NOT be accessible by the attacker by			
CVE-2023-28005	ption	exploitation of this vulnerability alone.	2023-03-22	6.8	Medium
		,			

		T			
		A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300			
		Series Switches could allow an authenticated, local attacker with			
		level-15 privileges or an unauthenticated attacker with physical			
		access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that			
		occur when retrieving the public release key that is used for			
		image signature verification. An attacker could exploit this			
		vulnerability by modifying specific variables in the Serial			
		Peripheral Interface (SPI) flash memory of an affected device. A			
		successful exploit could allow the attacker to execute persistent			
		code on the underlying operating system. Note: In Cisco IOS XE			
		Software releases 16.11.1 and later, the complexity of an attack			
	cisco -	using this vulnerability is high. However, an attacker with level-			
	multiple	15 privileges could easily downgrade the Cisco IOS XE Software			
CVE-2023-20082	products	on a device to a release that would lower the attack complexity.	2023-03-23	6.8	Medium
		In onParentVisible of HeaderPrivacyIconsController.kt, there is a			
		possible way to bypass factory reset protections due to a missing			
		permission check. This could lead to local escalation of privilege			
	1 .	with physical access to a device that's been factory reset with no			
	google -	additional execution privileges needed. User interaction is not			
CVE 2022 20026	multiple	needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-253043058	2023-03-24	6.0	Modium
CVE-2023-20926	products		2023-03-24	6.8	Medium
	mcafee -	McAfee Total Protection prior to 16.0.50 may allow an adversary (with full administrative access) to modify a McAfee specific			
	total_protecti	Component Object Model (COM) in the Windows Registry. This			
CVE-2023-25134	on	can result in the loading of a malicious payload.	2023-03-21	6.7	Medium
<u> </u>	011	In OEM_OnRequest of sced.cpp, there is a possible shell		<u> </u>	ivicalani
		command execution due to improper input validation. This could			
		lead to local escalation of privilege with System execution			
		privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android kernelAndroid			
CVE-2022-42500	android	ID: A-239701389References: N/A	2023-03-24	6.7	Medium
		In _ufdt_output_property_to_fdt of ufdt_convert.c, there is a			
		possible out of bounds write due to an incorrect bounds check.			
		This could lead to local escalation of privilege with System			
		execution privileges needed. User interaction is not needed for			
01/5 0055 555	google -	exploitation.Product: AndroidVersions: Android-13Android ID:	2225	• =	
CVE-2023-20994	android	A-259062118	2023-03-24	6.7	Medium
		In UnwindingWorker of unwinding.cc, there is a possible out of			
		bounds write due to a use after free. This could lead to local			
	google -	escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation.Product:			
CVE-2023-21018	googie - android	AndroidVersions: Android-13Android ID: A-233338564	2023-03-24	6.7	Medium
2 A F 7072-71010	android	In registerSignalHandlers of main.c, there is a possible local	2020-00-24	0.7	ivicululli
		arbitrary code execution due to a use after free. This could lead			
		to local escalation of privilege with System execution privileges			
	google -	needed. User interaction is not needed for exploitation. Product:			
CVE-2023-21020	android	AndroidVersions: Android-13Android ID: A-256591441	2023-03-24	6.7	Medium
	<del>-</del>	In cs40l2x_cp_trigger_queue_show of cs40l2x.c, there is a			
		possible out of bounds write due to a use after free. This could			
		lead to local escalation of privilege with System execution			
		privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android kernelAndroid			
CVE-2023-21038	android	ID: A-224000736References: N/A	2023-03-24	6.7	Medium
		In (TBD) of (TBD), there is a possible way to corrupt memory due			
		to a use after free. This could lead to local escalation of privilege			
		with System execution privileges needed. User interaction is not			
	google -	needed for exploitation.Product: AndroidVersions: Android		_	
CVE-2023-21042	android	kernelAndroid ID: A-239873326References: N/A	2023-03-24	6.7	Medium
		In (TBD) of (TBD), there is a possible way to corrupt memory due			
		to a use after free. This could lead to local escalation of privilege			
	~~~!-	with System execution privileges needed. User interaction is not			
CVE 2022 24042	google -	needed for exploitation.Product: AndroidVersions: Android	2022 02 24	67	Madium
CVE-2023-21043	android	kernelAndroid ID: A-239872581References: N/A	2023-03-24	6.7	Medium
		In load_png_image of ExynosHWCHelper.cpp, there is a possible			
		out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution			
		privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android kernelAndroid			
CVE-2023-21050	android	ID: A-244423702References: N/A	2023-03-24	6.7	Medium
5.2 2023 21030	anaroid	In dwc3_exynos_clk_get of dwc3-exynos.c, there is a possible	2020 00 24	5.7	ivicularii
		out of bounds write due to an incorrect bounds check. This could			
		lead to local escalation of privilege in the kernel with System			
		execution privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android kernelAndroid			
CVE-2023-21051	android	ID: A-259323322References: N/A	2023-03-24	6.7	Medium
		In setToExternal of ril_external_client.cpp, there is a possible out		_	
			· ·		
	google -	of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges			

needed. User Interaction is not redeed for exploitation. Product.  Androut/Versiators.						1
25906438936erronces NA			needed. User interaction is not needed for exploitation. Product:			
the feet, act further Line of I Was, device, stace, there is a possible in memory corruption due to type convision. This could lead to local escalation of privilege with system execution privileges in the control of						
CVE 2023 21056   Songle   Améndéric Province   Am			·			
people people android with a provided for exploitation Product Android Versions Android Versions (Android Versions) Android Versions (Android Versions) Android Versions (Android Versions) Android Versions (Android Versions) Android Versions) Android Versions) Android Versions) Android Versions (Android Versions) Android Versions) Android Versions (Android Versions) Android Versions) Android Versions (Android Versions) Android Versions) Android Versions (Android Versions) Android Versions) Android Versions (Android Versions) Android Versions (Android Versions) Android Versions) Android Versions (Android Versions) Android Versions) Android Versions (Android Versions) Android Versions) Android Versions) Android Versions (Android Versions) Android Versions) Andr			· · · · · · · · · · · · · · · · · · ·			
CVE-2023-21058 poggle- CVE-2023-21062 pandroid CVE-2023-21063 poggle- CVE-2023-21063 pandroid CVE-2023-21064 pandroid CVE-2023-21065 pandroid CVE-2023-21065 pandroid CVE-2023-21065 pandroid CVE-2023-21066 pandroid CVE-2023-21067 pandroid CVE-2023-21068 pandroid CVE-2023-21069 pandroid CVE-2023-21070 pandroid CVE-2023			, , , , , , , , , , , , , , , , , , , ,			
CVE-2023-21069 and mind    A 23300358Peleremees. N/A		google	·			
in DesetTempEcc of Imsservice. opp, there is a possible out of bounds read due to an increrect bounds reck. This could lead to local escalation of privilege with System execution privileges and an increase of the privilege with System execution privileges and an increase of the privilege with System execution privileges and to local escalation of privilege with System execution privileges and to local escalation of privilege with System execution. Product.  CVE-2023-21063 and and an increase of the privilege with System execution privileges and execution privileges and and an increase of the privilege with System execution privileges and execution privileges and execution privileges and execution privileges with System execution privileges and execution privileges with System execution privileges and execution privileges with system execution privileges with System execution privileges and execution privileg	CVF-2023-21056			2023-03-24	6.7	Medium
bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation-Product. Android/versions: Android versions: Android versions versions of Android versions: Androi	012 2023 21030	anaroid	·	2020 00 2 .	<u> </u>	- Wiediaiii
medical Liber interaction is not needed for exploitation Product. Android Versions: Android & medical product in the CVF 2013-1082   Android & medical properties of the CVF 2013-1083   Android & medical properties of the CVF 2013-1083   Android & medical product in the CVF 2013-1084   Android & medical product in the CVF 2013-1						
AndroidVersions: Android kernelandroid ID: A. 2023-03-24 6.7 Medium in parcewithbutthType of similar control for providing with System execution privileges medical to local escalation of privilege with System execution privileges in control of the control of th			, , , , , , , , , , , , , , , , , , , ,			
CVE-2023-21002 android 24337877908eferences: N/A 2433787908eferences: N/A 2433787908eferences: N/A 24312986Evences. N/A 24312986Evences			·			
In Parael/Publishy per of smoklar.pp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android kernel/Android ID: A-2323-20628 References: N/A products read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android kernel/Android ID: A-2303-03-24 for Medium developed android in the product of the privilege with System execution privileges in the product of the privilege with System execution privileges in the product of the privilege with System execution privileges and privilege with System execution privileges in the privilege with System execution privileges and privilege with System execution privileges needed. User interaction is not needed for exploitation Product: Android/Versions: Android versions: Android versions to privilege with System execution privileges needed. User interaction is not needed for exploitation Product: Android/Versions: Android versions: Android	CVF-2023-21062			2023-03-24	6.7	Madium
bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges in proceded. User interaction is not needed for exploitation. Product. Android Variants. Android & Armellandroid ID: A 231379802References. N/A 243129802References. N/A 24312902References. N/A 24312902Refere	CVL-2023-21002	anuroid	·	2023-03-24	0.7	iviculani
pogle - Android Versions: Android Remelandroid ID: A 2023-03-24 6.7 Medium Interaction is not needed for exploitation Product: Description of privilege with System execution privilege into coloral escalation of privilege with System execution privilege into coloral escalation of privilege with System execution privilege and Description in the product of the CVE-2023-21061 android Product: Android Versions: Android Remelandroid ID: A 24333078References: N/A android Versions: Android Remelandroid ID: A 24333078References: N/A android Versions: Android Remelandroid ID: A 24333078References: N/A android Versions: Android Remelandroid ID: A 23950998References: N/A android Versions: Android Remelandroid ID: A 2395098References: N/A android Versions: Android Remelandroid ID: A 2395098References: N/A android Versions: Android Remelandroid ID: A 2003-03-24 6.7 Medium Versions: Android Remelandroid ID: A 2003-0						
google - Android Versions: Android kernelAndroid ID: A 2023-03-24 6.7 Medium in DestPrinCentrol of miscaservice cpp, there is a possible out of local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation Product. Android/versions: Android kernelAndroid ID: A 2023-03-24 6.7 Medium in fot_next_tag of fdtc, there is a possible out of privilege medium interaction is not needed for exploitation product. Android/versions: Android lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation Product. Android/versions: Android kernelAndroid ID: A 2023-03-24 6.7 Medium interaction is not needed for exploitation Product. Android/versions: Android kernelAndroid ID: A 2023-03-24 6.7 Medium interaction is not needed for exploitation Product. Android/versions: Android kernelAndroid ID: A 2023-03-24 6.7 Medium interaction is not needed for exploitation Product. Android/versions: Android kernelAndroid ID: A 2023-03-24 6.7 Medium interaction is not needed for exploitation Product. Android/versions: Android kernelAndroid ID: A 2023-03-24 6.7 Medium interaction in a for exploitation Product. Android/versions: Android kernelAndroid ID: A 2023-03-24 6.7 Medium in add, roam, cache jist of wir. Jonan, cache jist of wir. Jon						
Additional Association of the province of the properties of the properties of the province of the properties of the properties of the province			·			
in DosSetPinControl of misseservice.op, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product. Android/versions: Android kernelAndroid ID: A 2023-03-24 6.7 Medium of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product interaction is not needed for exploitation. Produ	CVE 2022 24062			2022 02 24	6.7	N. A. a. alii a
bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Vasions: Android ID: A- 2023-03-24 6.7 Medium Info. Privilege with System execution privileges needed. User interaction is not needed for exploitation of privilege with System execution privilege and the calculation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android Remelandroid ID: A- 2023-03-24 6.7 Medium Info. Privilege with System execution privileges in the privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android ID: A- 2023-03-24 6.7 Medium Indianation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android ID: A- 254023309References: IV/A Indianation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android ID: A- 2540287/66eferences: IV/A Indianation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android ID: A- 257029378. References: IV/A Indianation of privilege with System execution privileges needed. User interaction is not needed for exploitation product: Android/versions: Android ID: A- 257029378. References: IV/A Indianation of privilege with System execution privileges needed. User interaction is not needed f	CVE-2023-21063	android	·	2023-03-24	6.7	Medium
local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In fit, next, tag of lift.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In with update pidden. ap is of wit. (fspcana., 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 privilege and android in ID: A- 2023-03-24 6.7 Medium  In with update pidden. ap is of wit. (fspcana., there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In add pram_cache_list of wit. pram.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In ded_prot_loctcmpilt_process of didn magbuf.c, there is a possible out of bounds write due to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In ded_prot_loctcmpilt_process of didn magbuf.c, there is a possible out of bounds write due to a borifer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android kernelAndroid ID: A- 2023-03-24 6.7 M			, , ,			
needed. User interaction is not needed for exploitation. Product: Android/Versions: Android ID: A. 2023-03-24 6.7 Medium  In fift_next_pate of fift_c. there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges in needed. User interaction is not needed for exploitation. Product: Android/Versions: Android kernelAndroid ID: A. 2038-030438eferences: N/A  In wi_update_hidden_ap_le of wi_cfgscan.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product:  VE-2023-21069 android ID: A.  2023-03-24 6.7 Medium  In add_roam_csche_list of wi_roam.c, there is a possible out of bounds write due to a missing bound scheck. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product:  VE-2023-21070 in add to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product:  Android/versions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In add_prot_ioctcmpti_process of dhd_magbufc, there is a possible out of bounds write due to improper input validation.  This could lead to local escalation of privilege with System execution privileges with System execution privileges with System execution privileges with System execution privilege with System execution privilege with System execution privilege with System execution privilege with System execution privileges with System			_			
SVE-2023-21064 android 243130078References: IV/A linity provides with the due to an integer overflow. This could lead to local escalation of privilege with System execution privileges preeded. User interaction is not needed for exploitation. Product: Android/versions: Android kernel/android ID: A-2023-03-24 6.7 Medium of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges and privileges and product of bounds with execution privileges with system execution privileges and product of bounds with execution privileges with system execution privileges and product of bounds with execution privileges with system e			needed. User interaction is not needed for exploitation.Product:			
In fat_nex_tag of fatc, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product:						
due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android kernelAndroid ID: A-29630493References: N/A  In wit_update_hidden_ap_led wit_descanct, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android kernelAndroid ID: A-254023030References: N/A  In add_roam_cache_list of wit_roam.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android kernelAndroid ID: A-25402378feferences: N/A  In add_roam_cache_list of with younce, there is a possible out of local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android ID: A-254023518References: N/A  In dh_prot_loctcmplt_process of dhd_msgbuf.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android kernelAndroid ID: A-254028518References: N/A  In rtt_uppack_with_cffin of hd_rttc, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation. Product: Android/Versions: Android kernelAndroid ID: A-257290381References: N/A  In rtt_uppack_with_cffin of hd_rttc, there is a possible out of bounds write due to a hepa buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed	CVE-2023-21064	android	·	2023-03-24	6.7	Medium
privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kemelAndroid ID: A. 2023-03-24 6.7 Medium  In W. update, hidden, ag. le of W. Ligscanc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kemelAndroid ID: A.254023909References: N/A  In Add, roam, cache, list of Wr, oram.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android lead to local escalation of privilege with System execution privileges headed.  User interaction is not needed for exploitation. Product: AndroidVersions: Android lead to local escalation of privilege with System execution privileges headed.  User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid ID: A.25402851886ferences: N/A  In rtt_uppack_ytb_cthir of hid_ttc, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid ID: A.25729038186ferences: N/A  In rtt_uppack_ytb_cthir of hid_ttc, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for expl						
Interaction is not needed for exploitation.Product: Android/versions: Android bernelAndroid   10: A 2023-03-24   6.7   Medium						
CVE-2023-21065 and/old 239630493References: N/A						
in wt. update, hidden, ap. je of wt. (fgscanct, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation-Product: AndroidVersions: Android kernelAndroid 2023-03-24 6.7 Medium in the product in the province of the p		google -	AndroidVersions: Android kernelAndroid ID: A-			
out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploration. Product: Android Versions: Android KernelAndroid Di. A 254023309References: N/A  In add, roam_cache, list of wl, roam.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android KernelAndroid ID: A 254028776References: N/A  In dhd_prot_iottcmpft_process of dhd_msgbuf.c, there is a possible out of bounds write due to a middle activation of privilege with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Android/Versions: Android kernelAndroid ID: A 254028518References: N/A  In rtt_unpack_xtlv_cbfn of dhd_rttc, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android kernelAndroid ID: A 2572093fReferences: N/A  In rtt_unpack_xtlv_cbfn of dhd_rttc, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android kernelAndroid ID: A 2572093fReferences: N/A  In rtt_unpack_xtlv_cbfn of dhd_rttc, there is a possible out of bounds write due to a hadroid were due to a base possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android kernelAndroid ID: A 257290	CVE-2023-21065	android	·	2023-03-24	6.7	Medium
lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid local escalation of privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid local escalation of privileges needed. User interaction is not needed for exploitation. This could lead to local escalation of privileges needed. User interaction is not needed for exploitation. This could lead to local escalation of privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid local escalation of privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid local escalation of privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid local escalation of privileges with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for						
privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android			- I			
google - exploitation.Product: Android/versions: Android kernelAndroid 1D: A-254029309References: N/A			· · · · · · · · · · · · · · · · · · ·			
In add_roam_cache_list of wl_roam.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: Android/Versions: Android kernelAndroid ID: A- 254028776References: N/A  In dhd_prot_loctcmpit_process of dhd_msgbuf.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: Android/Versions: Android kernelAndroid ID: A-254028518References: N/A  In rtt_unpack_wtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: Android/Versions: Android kernelAndroid ID: A- 257290781References: N/A  In rtt_unpack_wtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: Android/Versions: Android kernelAndroid ID: A- 257290781References: N/A  In rtt_unpack_wtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: Android/Versions: Android kernelAndroid ID: A- 257290396References: N/A  In get_sv_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: Android/Versions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In createTransmitfelOlouyDRequest of nan.cpp, there is a possible out of bounds write due t		google -				
bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254028376References: N/A  In dhd_prot_loctcmplt_process of dhd_msgbufc, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254028518References: N/A  In rtt_unpack_xtv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privileges with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257290781References: N/A  In rtt_unpack_xtv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257290781References: N/A  In rtt_unpack_xtv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257290396References: N/A  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-251857862References: N/A  In receteransmittellowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privileges	CVE-2023-21069	android	·	2023-03-24	6.7	Medium
local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:   AndroidVersions: Android   Di: A- android						
needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid ID: A-2023-21070   ndhd_prot_joctcmplt_process of dhd_msgbuf.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for bounds write due to a buffer overflow. This could lead to local escalation of privileges needed. User interaction is not needed for bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernelAndroid ID: A-257290781References: N/A   2023-03-24   6.7   Medium    CVE-2023-21072   android   AndroidVersions: Android kernelAndroid   ID: A-257290781References: N/A   2023-03-24   6.7   Medium    CVE-2023-21073   android   AndroidVersions: Android kernelAndroid   ID: A-257290781References: N/A   2023-03-24   6.7   Medium    CVE-2023-21073   android   AndroidVersions: Android kernelAndroid   ID: A-257290398References: N/A   2023-03-24   6.7   Medium    CVE-2023-21075   android   AndroidVersions: Android kernelAndroid   ID: A-257290398References: N/A   2023-03-24   6.7   Medium    In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid   ID: A-257290398References: N/A   2023-03-24   6.7   Medium    In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid   ID: A-26185763References: N/A   2023-03-24   6.7   Medium   ID: A-26185763References: N/A   2023-03-			_			
google - android			, , , , , , , , , , , , , , , , , , , ,			
In dhd_prot_ioctcmplt_process of dhd_msgbuf.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid    CVE-2023-21071		google -	·			
possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254028518References: N/A  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 257290781References: N/A  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857623References: N/A  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with	CVE-2023-21070		254028776References: N/A	2023-03-24	6.7	Medium
This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for or bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-2023-03-24 6.7 Medium    CVE-2023-21072						
execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: google - AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: android werite due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: androidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: androidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: androidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: androidVersions: Android kernelAndroid local escalation of privilege with System execution privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: androidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: androidVersions: Android kernelAndroid local escalation						
google android lip: A-254028518References: N/A			, ,			
In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:   AndroidVersions: Android kernelAndroid ID: A- 257290781References: N/A   2023-03-24   6.7   Medium		google -	, -			
bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257290781References: N/A  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257290396References: N/A  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-2023-03-24 6.7 Medium  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857862References: N/A  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-26185762References: N/A  In createTransmitFollowupRequest of nan.cpp, there is a possible out of exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-26185762References: N/A  In trt_unpack_xtv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.	CVE-2023-21071		· ·	2023-03-24	6.7	Medium
escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: android 257290781References: N/A 2023-03-24 6.7 Medium  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: google - AndroidVersions: Android kernelAndroid ID: A- 257290396References: N/A 2023-03-24 6.7 Medium  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: google - AndroidVersions: Android kernelAndroid ID: A- 261857862References: N/A 2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: google - android In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857623References: N/A 2023-03-24 6.7 Medium  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857623References: N/A 2023-03-24 6.7 Medium  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privilege						
User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 257290781References: N/A  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 257290396References: N/A  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: User interaction is not needed for exploitation.Product: google - AndroidVersions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privilege with System execution privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857623References: N/A  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.						
google - android 257290781References: N/A 2023-03-24 6.7 Medium  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:  AndroidVersions: Android kernelAndroid ID: A-257290396References: N/A 2023-03-24 6.7 Medium  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:  AndroidVersions: Android kernelAndroid ID: A-2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857623References: N/A 2023-03-24 6.7 Medium  In rtt_unpack_xtlv_cbfn of dh_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.						
CVE-2023-21072 android 257290781References: N/A 2023-03-24 6.7 Medium  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:  AndroidVersions: Android kernelAndroid ID: A-257290396References: N/A 2023-03-24 6.7 Medium  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:  AndroidVersions: Android kernelAndroid ID: A-261857862References: N/A 2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: Android lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privilege with System execution privilege with System execution privilege with System execution bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.		google -	·			
bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- android  257290396References: N/A  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- android  261857862References: N/A  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- android local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid  ID: A-261857623References: N/A  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.	CVE-2023-21072			2023-03-24	6.7	Medium
escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 257290396References: N/A  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium    CVE-2023-21075			_ , ,			
User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 257290396References: N/A  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: google - AndroidVersions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation.Product: AndroidVersions: Android kernelAndroid  UD: A-261857623References: N/A  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.						
google - android 257290396References: N/A 2023-03-24 6.7 Medium  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:  google - android 261857862References: N/A 2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid local escalation of privilege with System execution privileges needed.						
CVE-2023-21073 android 257290396References: N/A 2023-03-24 6.7 Medium  In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857862References: N/A 2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857623References: N/A 2023-03-24 6.7 Medium  CVE-2023-21076 android ID: A-261857623References: N/A 2023-03-24 6.7 Medium  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.		google -	· ·			
In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.  User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- android 261857862References: N/A 2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857623References: N/A 2023-03-24 6.7 Medium  CVE-2023-21076 In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.	CVE-2023-21073			2023-03-24	6.7	Medium
escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 261857862References: N/A  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid  CVE-2023-21076    In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local google - escalation of privilege with System execution privileges needed.			·			
User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 261857862References: N/A  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid    CVE-2023-21076			write due to a heap buffer overflow. This could lead to local			
google - android 261857862References: N/A 2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid  CVE-2023-21076 android ID: A-261857623References: N/A 2023-03-24 6.7 Medium  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.						
CVE-2023-21075 android 261857862References: N/A 2023-03-24 6.7 Medium  In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid  CVE-2023-21076 android ID: A-261857623References: N/A 2023-03-24 6.7 Medium  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local google - escalation of privilege with System execution privileges needed.		g0.0ala	·			
In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid    D: A-261857623References: N/A   2023-03-24   6.7   Medium	CVF-2023-21075			2023-03-24	6.7	Medium
possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-261857623 References: N/A 2023-03-24 6.7 Medium  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local google - escalation of privilege with System execution privileges needed.	0.2 2023 210/3	anarola	·	2020 00 24	5.7	ivicalulli
privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid  ID: A-261857623References: N/A  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.						
google - exploitation.Product: AndroidVersions: Android kernelAndroid  ID: A-261857623References: N/A  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.						
CVE-2023-21076 android ID: A-261857623References: N/A 2023-03-24 6.7 Medium  In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed.			1.			
In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local google - escalation of privilege with System execution privileges needed.	CVE 2022 24070		· ·	2022 02 24	67	N / a d!
bounds write due to a buffer overflow. This could lead to local google - escalation of privilege with System execution privileges needed.	CVE-2023-210/6	android	·	2023-03-24	b./	ivieaium
google - escalation of privilege with System execution privileges needed.			_ , ,			
		google -				
<u>.</u>	CVE-2023-21077		, - , - , - , - , - , - , - , - , - , -	2023-03-24	6.7	Medium

			Т		
		AndroidVersions: Android kernelAndroid ID: A-			
		257289560References: N/A In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of			
		bounds write due to a buffer overflow. This could lead to local			
		escalation of privilege with System execution privileges needed.			
		User interaction is not needed for exploitation.Product:			
	google -	AndroidVersions: Android kernelAndroid ID: A-			
CVE-2023-21078	android	254840211References: N/A	2023-03-24	6.7	Medium
012 2020 22070	anarora	In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of	2023 03 2 .	<u> </u>	Wiediaiii
		bounds write due to a heap buffer overflow. This could lead to			
		local escalation of privilege with System execution privileges			
		needed. User interaction is not needed for exploitation. Product:			
	google -	AndroidVersions: Android kernelAndroid ID: A-			
CVE-2023-21079	android	254839721References: N/A	2023-03-24	6.7	Medium
		IBM Aspera Faspex 4.4.2 could allow a remote authenticated			
	ibm - multiple	attacker to obtain sensitive credential information using			
CVE-2023-27873	products	specially crafted XML input. IBM X-Force ID: 249654.	2023-03-21	6.5	Medium
		A vulnerability in the web-based management interface of			
		ClearPass Policy Manager could allow a remote attacker			
		authenticated with low privileges to access sensitive			
	arubanetwork	information. A successful exploit allows an attacker to retrieve			
	s - multiple	information which could be used to potentially gain further			
CVE-2023-25591	products	privileges on the ClearPass instance.	2023-03-22	6.5	Medium
		A vulnerability in the implementation of the Cisco Network Plug-			
		and-Play (PnP) agent of Cisco DNA Center could allow an			
		authenticated, remote attacker to view sensitive information in			
		clear text. The attacker must have valid low-privileged user			
		credentials. This vulnerability is due to improper role-based			
		access control (RBAC) with the integration of PnP. An attacker			
	oicea	could exploit this vulnerability by authenticating to the device			
	cisco -	and sending a query to an internal API. A successful exploit could			
CVE-2023-20059	multiple products	allow the attacker to view sensitive information in clear text, which could include configuration files.	2023-03-23	6.5	Medium
CVE-2025-20059	products	A vulnerability in the web UI of Cisco IOS XE Software could allow	2023-03-23	0.5	Medium
		an authenticated, remote attacker to perform a directory			
		traversal and access resources that are outside the filesystem			
		mountpoint of the web UI. This vulnerability is due to an			
		insufficient security configuration. An attacker could exploit this			
		vulnerability by sending a crafted request to the web UI. A			
		successful exploit could allow the attacker to gain read access to			
		files that are outside the filesystem mountpoint of the web UI.			
	cisco -	Note: These files are located on a restricted filesystem that is			
	multiple	maintained for the web UI. There is no ability to write to any files			
CVE-2023-20066	products	on this filesystem.	2023-03-23	6.5	Medium
		In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25,			
		5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported			
	vmware -	versions, it is possible for a user to provide a specially crafted			
	multiple	SpEL expression that may cause a denial-of-service (DoS)			
CVE-2023-20861	products	condition.	2023-03-23	6.5	Medium
		In dit_hal_ioctl of dit.c, there is a possible use after free due to a			
		race condition. This could lead to local escalation of privilege			
		with System execution privileges needed. User interaction is not			
	google -	needed for exploitation.Product: AndroidVersions: Android			
CVE-2023-21055	android	kernelAndroid ID: A-244301523References: N/A	2023-03-24	6.4	Medium
		Vulnerabilities within the web-based management interface of			
		ClearPass Policy Manager could allow a remote attacker to			
	ال المناج معطورية	conduct a reflected cross-site scripting (XSS) attack against a user			
	arubanetwork	of the interface. A successful exploit allows an attacker to			
CVE 2022 25502	s - multiple	execute arbitrary script code in a victim's browser in the context of the affected interface.	2023-03-22	<i>C</i> 1	Medium
CVE-2023-25592	products		2023-03-22	6.1	iviealum
		Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to			
		conduct a reflected cross-site scripting (XSS) attack against a user			
	arubanetwork	of the interface. A successful exploit allows an attacker to			
	s - multiple	execute arbitrary script code in a victim's browser in the context			
CVE-2023-25593	products	of the affected interface.	2023-03-22	6.1	Medium
	r. 5446t5	A cleartext transmission vulnerability exists in the Remote	=0=0 00 22	Ų.±	
	netgear -	Management functionality of Netgear Orbi Router RBR750			
	rbs750_firmw	4.6.8.5. A specially-crafted man-in-the-middle attack can lead to			
CVE-2022-38458	are	a disclosure of sensitive information.	2023-03-21	5.9	Medium
	<b>-</b>	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco		<del>.</del>	
		Adaptive Security Appliance (ASA) Software, Cisco Firepower			
		Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS			
					1
		XE Software could allow an unauthenticated, remote attacker to			
		XE Software could allow an unauthenticated, remote attacker to			
	cisco -	XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.			
	cisco - multiple	XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6			

		resulting in a DoS condition. Note: To successfully exploit this			<u> </u>
		vulnerability, the attacker would need to either control the			
		DHCPv6 server or be in a man-in-the-middle position.			
		IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1,			
	ibm - multiple	and 4.1.1 stores user credentials in plain clear text which can be			
CVE-2023-25686	products	read by a local user. IBM X-Force ID: 247601.	2023-03-21	5.5	Medium
		A vulnerability exists in the ClearPass OnGuard Ubuntu agent			
		that allows for an attacker with local Ubuntu instance access to			
		potentially obtain sensitive information. Successful Exploitation			
	arubanetwork	of this vulnerability allows an attacker to retrieve information			
CVE 2022 25505	s - multiple	that is of a sensitive nature to the ClearPass/OnGuard	2022 02 22		NA a alicens
CVE-2023-25595	products	environment.	2023-03-22	5.5	Medium
		Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead			
		to disclosure of sensitive memory. An attacker could leverage			
	adobe -	this vulnerability to bypass mitigations such as ASLR. Exploitation			
	multiple	of this issue requires user interaction in that a victim must open			
CVE-2023-25862	products	a malicious file.	2023-03-22	5.5	Medium
<u> </u>	products	A vulnerability in the management CLI of Cisco access point (AP)			
		software could allow an authenticated, local attacker to cause a			
		denial of service (DoS) condition on an affected device. This			
		vulnerability is due to insufficient input validation of commands			
		supplied by the user. An attacker could exploit this vulnerability			
	cisco -	by authenticating to a device and submitting crafted input to the			
	wireless_lan_c	affected command. A successful exploit could allow the attacker			
	ontroller_soft	to cause an affected device to reload spontaneously, resulting in			
CVE-2023-20056	ware	a DoS condition.	2023-03-23	5.5	Medium
		A use-after-free flaw was found in the Linux kernel's core dump			
		subsystem. This flaw allows a local user to crash the system. Only			
	linux -	if patch 390031c94211 ("coredump: Use the vma snapshot in			
CVE-2023-1249	linux_kernel	fill_files_note") not applied yet, then kernel could be affected.	2023-03-23	5.5	Medium
		In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x			
	vmware -	prior to 2.3.3 and older versions, an application is vulnerable to			
	multiple	insertion of sensitive information into a log file when it attempts			
CVE-2023-20859	products	to revoke a Vault batch token.	2023-03-23	5.5	Medium
		An issue was discovered in the Linux kernel before 5.8.			
		lib/nlattr.c allows attackers to cause a denial of service			
CVE 2020 26604	linux -	(unbounded recursion) via a nested Netlink policy with a back	2022 02 24		D. A. a. Italia
CVE-2020-36691	linux_kernel	reference.	2023-03-24	5.5	Medium
		In isBluetoothShareUri of BluetoothOppUtility.java, there is a			
		possible incorrect file read due to a confused deputy. This could lead to local information disclosure with no additional execution			
	googlo	privileges needed. User interaction is needed for			
	google - multiple	exploitation.Product: AndroidVersions: Android-11 Android-12			
CVE-2022-20467	products	Android-12L Android-13Android ID: A-225880741	2023-03-24	5.5	Medium
CVE 2022 20407	products	In validateForCommonR1andR2 of PasspointConfiguration.java,	2023 03 24	3.3	IVICUIUIII
		uncaught errors in parsing stored configs could lead to local			
		persistent denial of service with no additional execution			
	google -	privileges needed. User interaction is not needed for			
	multiple	exploitation.Product: AndroidVersions: Android-12 Android-12L			
CVE-2022-20499	products	Android-13Android ID: A-246539931	2023-03-24	5.5	Medium
	•	In ffa_mrd_prot of shared_mem.c, there is a possible ID 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.Product:			
	google -	AndroidVersions: Android kernelAndroid ID: A-			
CVE 2022 42E20		2422225722			N 4 = alta
CVE-2022-42528	android	242203672References: N/A	2023-03-24	5.5	Medium
<u>CVE-2022-42328</u>	android	In addNetworkSuggestions of WifiManager.java, there is a	2023-03-24	5.5	Medium
<u>CVE-2UZZ-4Z5Z8</u>	android	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource	2023-03-24	5.5	Medium
CVE-2022-42528		In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no	2023-03-24	5.5	Medium
<u>CVE-2022-42528</u>	google -	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not	2023-03-24	5.5	Medium
	google - multiple	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11			
CVE-2022-42528  CVE-2023-20910	google -	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920	2023-03-24	5.5 5.5	Medium
	google - multiple	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920 In sendHalfSheetCancelBroadcast of HalfSheetActivity.java,			
	google - multiple	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920 In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to			
	google - multiple	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920 In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local			
	google - multiple products	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920  In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges			
CVE-2023-20910	google - multiple products google -	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920  In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	2023-03-24	5.5	Medium
	google - multiple products	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920 In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-234442700			
CVE-2023-20910	google - multiple products google -	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920  In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-234442700  In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a	2023-03-24	5.5	Medium
CVE-2023-20910	google - multiple products google -	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920  In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-234442700  In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write due to a missing bounds check. This	2023-03-24	5.5	Medium
CVE-2023-20910	google - multiple products google - android	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920  In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-234442700  In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with no additional	2023-03-24	5.5	Medium
CVE-2023-20910	google - multiple products google - android google -	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920  In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-234442700  In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write 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	2023-03-24	5.5	Medium
CVE-2023-20910  CVE-2023-20929	google - multiple products google - android google - multiple	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920  In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-234442700  In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write 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.Product: AndroidVersions: Android-11 Android-12	2023-03-24	5.5 5.5	Medium
CVE-2023-20910	google - multiple products google - android google -	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920  In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-234442700  In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write 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.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-186803518	2023-03-24	5.5	Medium
CVE-2023-20910  CVE-2023-20929	google - multiple products google - android google - multiple	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920  In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-234442700  In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write 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.Product: Android-12 Android-12L Android-13Android ID: A-186803518  In getSliceEndItem of MediaVolumePreferenceController.java,	2023-03-24	5.5 5.5	Medium
CVE-2023-20910  CVE-2023-20929	google - multiple products google - android google - multiple	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920  In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-234442700  In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write 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.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-186803518	2023-03-24	5.5 5.5	Medium

		privileges needed. User interaction is not needed for			
		exploitation.Product: AndroidVersions: Android-13Android ID: A-256590210			
		In btm_vendor_specific_evt of btm_devctl.cc, there is a possible			
		out of bounds read due to a missing bounds check. This could			
		lead to local information disclosure with System execution			
	google -	privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID:			
CVE-2023-20972	android	A-255304665	2023-03-24	5.5	Medium
<u> </u>		In btm_create_conn_cancel_complete of btm_sec.cc, there is a			
		possible out of bounds read due to a missing bounds check. This			
		could lead to local information disclosure with System execution			
		privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:			
CVE-2023-20973	android	A-260568245	2023-03-24	5.5	Medium
		In btm_ble_add_resolving_list_entry_complete of btm_ble_privacy.cc, there is a possible out of bounds read due			
		to a missing bounds check. This could lead to local information			
		disclosure with System execution privileges needed. User			
	google -	interaction is not needed for exploitation.Product:			
CVE-2023-20974	android	AndroidVersions: Android-13Android ID: A-260078907	2023-03-24	5.5	Medium
		In BtaAvCo::GetNextSourceDataPacket of bta_av_co.cc, 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			
CVE-2023-20979	google - android	exploitation.Product: AndroidVersions: Android-13Android ID: A-259939364	2023-03-24	5.5	Medium
CVE-2023-20979	anuroid	In btu_ble_ll_conn_param_upd_evt of btu_hcif.cc, there is a	2023-03-24	٥.٥	ivieululli
		possible out of bounds read due to a missing bounds check. This			
		could lead to local information disclosure in the Bluetooth server			
		with System execution privileges needed. User interaction is not			
	google -	needed for exploitation.Product: AndroidVersions: Android-			
CVE-2023-20980	android	13Android ID: A-260230274	2023-03-24	5.5	Medium
		In multiple locations, there is a possible way to trigger a			
		persistent reboot loop due to improper input validation. This			
		could lead to local denial of service with User execution privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:			
CVE-2023-20996	android	A-246749764	2023-03-24	5.5	Medium
		In multiple locations, there is a possible way to trigger a			
		persistent reboot loop due to improper input validation. This			
		could lead to local denial of service with User execution			
		privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:			
CVF-2023-20997		A 246740702	2022 02 24		N A 12
CVE-2023-20997	android	A-246749702	2023-03-24	5.5	Medium
CVE-2023-20997	android	In multiple locations, there is a possible way to trigger a	2023-03-24	5.5	Medium
CVE-2023-20997	android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This	2023-03-24	5.5	Medium
CVE-2023-20997	android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution	2023-03-24	5.5	Medium
CVE-2023-20997	android google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This	2023-03-24	5.5	Medium
		In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for	2023-03-24	5.5 5.5	
	google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID:			
	google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This			
	google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution			
	google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for			
CVE-2023-20998	google - android google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID:	2023-03-24	5.5	Medium
CVE-2023-20998	google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467			Medium
CVE-2023-20998	google - android google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246750467  In Account Type Preference of Account Type Preference. java,	2023-03-24	5.5	Medium
CVE-2023-20998	google - android google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246750467  In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts	2023-03-24	5.5	Medium
CVE-2023-20998	google - android google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246750467  In Account Type Preference of Account Type Preference. java,	2023-03-24	5.5	Medium
CVE-2023-20998	google - android google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246750467  In Account Type Preference of Account Type Preference. java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This	2023-03-24	5.5	Medium
CVE-2023-20998  CVE-2023-20999	google - android google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467  In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID:	2023-03-24	5.5 5.5	Medium
CVE-2023-20998  CVE-2023-20999	google - android google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467  In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213905884	2023-03-24	5.5	Medium
CVE-2023-20998  CVE-2023-20999	google - android google - android google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467  In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213905884  In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible	2023-03-24	5.5 5.5	Medium
CVE-2023-20998  CVE-2023-20999	google - android google - android google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467  In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213905884  In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead	2023-03-24	5.5 5.5	Medium
CVE-2023-20998  CVE-2023-20999	google - android google - android google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467  In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213905884  In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution	2023-03-24	5.5 5.5	Medium
CVE-2023-20998  CVE-2023-20999	google - android google - android google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467  In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213905884  In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	2023-03-24	5.5 5.5	Medium
CVE-2023-20998  CVE-2023-20999  CVE-2023-21016	google - android google - android google -	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467  In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213905884  In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution	2023-03-24	5.5 5.5	Medium
CVE-2023-20998  CVE-2023-20999  CVE-2023-21016	google - android google - android google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467  In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213905884  In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID:	2023-03-24 2023-03-24	5.5 5.5	Medium
CVE-2023-20998  CVE-2023-20999  CVE-2023-21016  CVE-2023-21019	google - android google - android google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467  In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213905884  In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242379731	2023-03-24 2023-03-24	5.5 5.5	Medium
CVE-2023-20998  CVE-2023-20999  CVE-2023-21016	google - android google - android google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246750467  In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-213905884  In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-242379731  In updateInputChannel of WindowManagerService.java, there is a possible way to set a touchable region beyond its own SurfaceControl due to a logic error in the code. This could lead	2023-03-24 2023-03-24	5.5 5.5	Medium
CVE-2023-20998  CVE-2023-20999  CVE-2023-21016	google - android google - android google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246750467  In Account Type Preference of Account Type Preference. java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-213905884  In ih 264e_init_proc_ctxt of ih 264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-242379731  In updateInputChannel of Window Manager Service. java, there is a possible way to set a touchable region beyond its own Surface Control due to a logic error in the code. This could lead to local denial of service with no additional execution privileges	2023-03-24 2023-03-24	5.5 5.5	Medium
CVE-2023-20998  CVE-2023-20999  CVE-2023-21016	google - android  google - android  google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246750467  In AccountTypePreference of AccountTypePreference. java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-213905884  In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-242379731  In updateInputChannel of WindowManagerService.java, there is a possible way to set a touchable region beyond its own SurfaceControl due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product:	2023-03-24 2023-03-24 2023-03-24	5.5 5.5 5.5	Medium
CVE-2023-20998  CVE-2023-20999  CVE-2023-21016	google - android google - android google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467  In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213905884  In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242379731  In updateInputChannel of WindowManagerService.java, there is a possible way to set a touchable region beyond its own SurfaceControl due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254681548	2023-03-24 2023-03-24	5.5 5.5	Medium
CVE-2023-20998  CVE-2023-20999  CVE-2023-21016	google - android  google - android  google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246749936  In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-246750467  In AccountTypePreference of AccountTypePreference. java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-213905884  In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-242379731  In updateInputChannel of WindowManagerService.java, there is a possible way to set a touchable region beyond its own SurfaceControl due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Product:	2023-03-24 2023-03-24 2023-03-24	5.5 5.5 5.5	Medium  Medium  Medium  Medium

		interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-217934898			
		In addNetwork of WifiManager.java, there is a possible way to			
		trigger a persistent DoS due to resource exhaustion. This could			
		lead to local denial of service with no additional execution			
	1 .	privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:			
CVE-2023-21033	android	A-244713323	2023-03-24	5.5	Medium
		In BitmapExport.java, there is a possible failure to truncate			
		images due to a logic error in the code.Product:			
	google -	AndroidVersions: Android kernelAndroid ID: A-			
CVE-2023-21036	android	264261868References: N/A	2023-03-24	5.5	Medium
		A NULL pointer dereference was found in io_file_bitmap_get in			
		io_uring/filetable.c in the io_uring sub-component in the Linux			
		Kernel. When fixed files are unregistered, some context			
		information (file_alloc_{start,end} and alloc_hint) is not cleared.			
		A subsequent request that has auto index selection enabled via			
	linux -	IORING_FILE_INDEX_ALLOC can cause a NULL pointer			
	multiple	dereference. An unprivileged user can use the flaw to cause a			
CVE 2022 1502	·		2023-03-24	<b>.</b>	Medium
CVE-2023-1583	products	system crash.	2023-03-24	5.5	iviedium
		A remote Cross-site Scripting vulnerability was discovered in HPE			
		Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5)			
	hp -	and Integrated Lights-Out 4 (iLO 4). HPE has provided software			
	integrated_lig	updates to resolve this vulnerability in HPE Integrated Lights-			
CVE-2023-28083	hts-out_4	Out.	2023-03-22	5.4	Mediun
		Experience Manager versions 6.5.15.0 (and earlier) are affected		_	
		by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-			
	adobe -	privileged attacker is able to convince a victim to visit a URL			
	multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-21615	products	be executed within the context of the victim's browser.	2023-03-22	5.4	Medium
		Experience Manager versions 6.5.15.0 (and earlier) are affected	- <del>-</del>		1
		by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-			
	adobe -	privileged attacker is able to convince a victim to visit a URL			
	multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE 2022 24C4C			2022 02 22	Г 4	N/Lo alia
CVE-2023-21616	products	be executed within the context of the victim's browser.	2023-03-22	5.4	Medium
		Experience Manager versions 6.5.15.0 (and earlier) are affected			
		by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-			
	adobe -	privileged attacker is able to convince a victim to visit a URL			
	multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-22252	products	be executed within the context of the victim's browser.	2023-03-22	5.4	Medium
		Experience Manager versions 6.5.15.0 (and earlier) are affected			
		by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-			
	adobe -	privileged attacker is able to convince a victim to visit a URL			
	multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-22253	products	be executed within the context of the victim's browser.	2023-03-22	5.4	Medium
<u> </u>	p. c d. d. c. c	Experience Manager versions 6.5.15.0 (and earlier) are affected			11100110111
		by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-			
	adobe -	privileged attacker is able to convince a victim to visit a URL			
		1,			
0.45 2022 22254	multiple	referencing a vulnerable page, malicious JavaScript content may	2022 02 22	- 4	
CVE-2023-22254	products	be executed within the context of the victim's browser.	2023-03-22	5.4	Medium
		Experience Manager versions 6.5.15.0 (and earlier) are affected			
		by a URL Redirection to Untrusted Site ('Open Redirect')			
	adobe -	vulnerability. A low-privilege authenticated attacker could			
	multiple	leverage this vulnerability to redirect users to malicious			
CVE-2023-22256	products	websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Mediun
		Experience Manager versions 6.5.15.0 (and earlier) are affected			
		by a URL Redirection to Untrusted Site ('Open Redirect')			
	adobe -	vulnerability. A low-privilege authenticated attacker could			
	multiple	leverage this vulnerability to redirect users to malicious			
CVE-2023-22257	products	websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Mediun
<u> </u>	products	Experience Manager versions 6.5.15.0 (and earlier) are affected	2023 UJ-22	J. <del>1</del>	ivicululi
		by a URL Redirection to Untrusted Site ('Open Redirect')			
	ا جا جاء	'			
	adobe -	vulnerability. A low-privilege authenticated attacker could			
0.48 - 5.55	multiple	leverage this vulnerability to redirect users to malicious		_	
CVE-2023-22258	products	websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Mediun
		Experience Manager versions 6.5.15.0 (and earlier) are affected			
		by a URL Redirection to Untrusted Site ('Open Redirect')			
	adobe -	vulnerability. A low-privilege authenticated attacker could			
	multiple	leverage this vulnerability to redirect users to malicious			
CVE-2023-22259	products	websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Mediun
	1. 2.3.300	Experience Manager versions 6.5.15.0 (and earlier) are affected			
		by a URL Redirection to Untrusted Site ('Open Redirect')			
	adobe -	vulnerability. A low-privilege authenticated attacker could			
		, , , , , , , , , , , , , , , , , , , ,			
OVE 2000 2000	multiple	leverage this vulnerability to redirect users to malicious	2022 22 22		
CVE-2023-22260	products	websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Mediun
	adobe -	Experience Manager versions 6.5.15.0 (and earlier) are affected			
	multiple	by a URL Redirection to Untrusted Site ('Open Redirect')			
	products	vulnerability. A low-privilege authenticated attacker could	2023-03-22	5.4	Medium

	T				1
		leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction.			
		Experience Manager versions 6.5.15.0 (and earlier) are affected			
		by a URL Redirection to Untrusted Site ('Open Redirect')			
	adobe -	vulnerability. A low-privilege authenticated attacker could			
	multiple	leverage this vulnerability to redirect users to malicious			
CVE-2023-22262	products	websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Medium
	promote in the second	Experience Manager versions 6.5.15.0 (and earlier) are affected			
		by a URL Redirection to Untrusted Site ('Open Redirect')			
	adobe -	vulnerability. A low-privilege authenticated attacker could			
	multiple	leverage this vulnerability to redirect users to malicious			
CVE-2023-22263	products	websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Medium
		Experience Manager versions 6.5.15.0 (and earlier) are affected			
		by a URL Redirection to Untrusted Site ('Open Redirect')			
	adobe -	vulnerability. A low-privilege authenticated attacker could			
	multiple	leverage this vulnerability to redirect users to malicious			
CVE-2023-22264	products	websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Medium
		Experience Manager versions 6.5.15.0 (and earlier) are affected			
		by a URL Redirection to Untrusted Site ('Open Redirect')			
	adobe -	vulnerability. A low-privilege authenticated attacker could			
	multiple	leverage this vulnerability to redirect users to malicious			
CVE-2023-22265	products	websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Medium
		Experience Manager versions 6.5.15.0 (and earlier) are affected			
		by a URL Redirection to Untrusted Site ('Open Redirect')			
	adobe -	vulnerability. A low-privilege authenticated attacker could			
	multiple	leverage this vulnerability to redirect users to malicious			
CVE-2023-22266	products	websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Medium
		Experience Manager versions 6.5.15.0 (and earlier) are affected			
		by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-			
	adobe -	privileged attacker is able to convince a victim to visit a URL			
CVE 2022 22260	multiple	referencing a vulnerable page, malicious JavaScript content may	2022 02 22	<b>5</b> 4	N A !!
CVE-2023-22269	products	be executed within the context of the victim's browser.	2023-03-22	5.4	Medium
		A CWE-306: Missing Authentication for Critical Function			
		vulnerability exists in the Data Server TCP interface that could			
		allow deletion of reports from the IGSS project report directory,			
		this would lead to loss of data when an attacker abuses this functionality. Affected Products: IGSS Data			
	schneider- electric -	functionality. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS			
	multiple	Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom			
CVE-2023-27983	products	Reports(RMS16.dll)(V16.0.0.23040 and prior).	2023-03-21	5.3	Medium
CVL-2023-27363	products	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1	2023-03-21	3.3	iviculum
		, and 4.1.1 could allow a remote attacker to traverse directories			
		on the system. An attacker could send a specially crafted URL			
	ibm - multiple	request containing "dot dot" sequences (//) to view arbitrary			
CVE-2023-25689	products	files on the system. IBM X-Force ID: 247618.	2023-03-21	5.3	Medium
<u> </u>	products	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1,	2023 03 21	5.0	ivicaiaiii
		and 4.1.1could allow a remote attacker to traverse directories on			
		the system. An attacker could send a specially crafted URL			
	ibm - multiple	request containing "dot dot" sequences (//) to view arbitrary			
CVE-2023-25688	products	files on the system. IBM X-Force ID: 247606.	2023-03-22	5.3	Medium
		Experience Manager versions 6.5.15.0 (and earlier) are affected			
		by a Weak Cryptography for Passwords vulnerability that can			
		lead to a security feature bypass. A low-privileged attacker can			
	adobe -	exploit this in order to decrypt a user's password. The attack			
	multiple	complexity is high since a successful exploitation requires to			
CVE-2023-22271	products	already have in possession this encrypted secret.	2023-03-22	5.3	Medium
		An issue was discovered in Veritas NetBackup IT Analytics 11			
		before 11.2.0. The application upgrade process included			
		unsigned files that could be exploited and result in a customer			
		installing unauthentic components. A malicious actor could			
	veritas -	install rogue Collector executable files (aptare.jar or			
	multiple	upgrademanager.zip) on the Portal server, which might then be			
CVE-2023-28818	products	downloaded and installed on collectors.	2023-03-24	5.3	Medium
		A vulnerability exists in ClearPass Policy Manager that allows for			
		an attacker with administrative privileges to access sensitive			
		information in a cleartext format. A successful exploit allows an			
	arubanetwork	attacker to retrieve information which could be used to			
	s - multiple	potentially gain further access to network services supported by			
CVE-2023-25596	products	ClearPass Policy Manager.	2023-03-22	4.9	Medium
		Adobe ColdFusion versions 2018 Update 15 (and earlier) and			
		2021 Update 5 (and earlier) are affected by an Improper			
		Limitation of a Pathname to a Restricted Directory ('Path			
	adobe -	Traversal') vulnerability that could result in Arbitrary file system			
	multiple	read. Exploitation of this issue does not require user interaction,			
CVE-2023-26361	products	but does require administrator privileges.	2023-03-23	4.9	Medium
		Grafana is an open-source platform for monitoring and			
	grafana -	observability. Grafana had a stored XSS vulnerability in the			
	multiple	Graphite FunctionDescription tooltip. The stored XSS			1
CVE-2023-1410	products	vulnerability was possible due the value of the Function	2023-03-23	4.8	Medium

		Description was not appeared, as ritized. As attached and to			<u> </u>
		Description was not properly sanitized. An attacker needs to have control over the Graphite data source in order to			
		manipulate a function description and a Grafana admin needs to			
		configure the data source, later a Grafana user needs to select a			
		tampered function and hover over the description. Users may			
		upgrade to version 8.5.22, 9.2.15 and 9.3.11 to receive a fix.			
		A use-after-free flaw was found in qdisc_graft in			
		net/sched/sch_api.c in the Linux Kernel due to a race problem.			
	linux -	This flaw leads to a denial of service issue. If patch ebda44da44f6			
	multiple	("net: sched: fix race condition in qdisc_graft()") not applied yet,			
CVE-2023-0590	products	then kernel could be affected.	2023-03-23	4.7	Medium
		In Display::setPowerMode of HWC2.cpp, there is a possible out			
		of bounds read due to a race condition. This could lead to local			
	googlo	information disclosure with no additional execution privileges			
CVE-2023-21031	google - android	needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242688355	2023-03-24	4.7	Medium
CVE-2023-21031	anuroiu	In btm_read_link_quality_complete of btm_acl.cc, there is a	2023-03-24	4.7	Medium
		possible out of bounds read due to a missing bounds check. This			
		could lead to local information disclosure over Bluetooth with			
		System execution privileges needed. User interaction is not			
	google -	needed for exploitation.Product: AndroidVersions: Android-			
CVE-2023-20987	android	13Android ID: A-260569414	2023-03-24	4.5	Medium
		In btm_read_rssi_complete of btm_acl.cc, there is a possible out			
		of bounds read due to a missing bounds check. This could lead to			
		local information disclosure in the Bluetooth server with System			
		execution privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:			
CVE-2023-20988	android	A-260569232	2023-03-24	4.5	Medium
		In on_iso_link_quality_read of btm_iso_impl.h, there is a			
		possible out of bounds read due to a missing bounds check. This			
		could lead to local information disclosure in the Bluetooth server			
		with System execution privileges needed. User interaction is not			
	google -	needed for exploitation.Product: AndroidVersions: Android-			
CVE-2023-20992	android	13Android ID: A-260568750	2023-03-24	4.5	Medium
		In Import of C2SurfaceSyncObj.cpp, there is a possible out of			
		bounds write due to a missing bounds check. This could lead to			
		local information disclosure with System execution privileges			
	google -	needed. User interaction is not needed for exploitation. Product:			
CVE 2022 20056	multiple	AndroidVersions: Android-12 Android-12L Android-13Android ID: A-240140929	2023-03-24	4.4	Medium
CVE-2023-20956	products	In multiple locations of p2p_iface.cpp, there is a possible out of	2023-03-24	4.4	iviedium
		bounds read due to a missing bounds check. This could lead to			
		local information disclosure with System execution privileges			
	google -	needed. User interaction is not needed for exploitation. Product:			
CVE-2023-20968	android	AndroidVersions: Android-13Android ID: A-262235935	2023-03-24	4.4	Medium
		In multiple locations of p2p_iface.cpp, there is a possible out of			
		bounds read due to a missing bounds check. This could lead to			
		local information disclosure with System execution privileges			
	google -	needed. User interaction is not needed for exploitation. Product:			
CVE-2023-20969	android	AndroidVersions: Android-13Android ID: A-262236313	2023-03-24	4.4	Medium
		In multiple locations of p2p_iface.cpp, there is a possible out of			
		bounds read due to a missing bounds check. This could lead to			
		local information disclosure with System execution privileges			
	google -	needed. User interaction is not needed for exploitation.Product:			
CVE-2023-20970	android	AndroidVersions: Android-13Android ID: A-262236005	2023-03-24	4.4	Medium
		In btm_ble_read_remote_features_complete of			
		btm_ble_gap.cc, there is a possible out of bounds read due to			
		improper input validation. This could lead to local information			
		disclosure if the firmware were compromised with System			
		execution privileges needed. User interaction is not needed for			
CVE 2022 200==	google -	exploitation.Product: AndroidVersions: Android-13Android ID:	2022 02 03	A 4	
CVE-2023-20977	android	A-254445952	2023-03-24	4.4	Medium
		In btu_ble_rc_param_req_evt of btu_hcif.cc, there is a possible			
		out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution			
		privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:			
CVE-2023-20981	android	A-256165737	2023-03-24	4.4	Medium
2 V L 2023-20301	anaroid	In btm_read_tx_power_complete of btm_acl.cc, there is a	2023 03-24	7.7	iviculalii
		possible out of bounds read due to a missing bounds check. This			
		could lead to local information disclosure in the Bluetooth server			
		with System execution privileges needed. User interaction is not			
	google -	needed for exploitation.Product: AndroidVersions: Android-			
Į.	00	•	2023-03-24	4.4	Medium
CVE-2023-20982	android	13Android ID: A-260568083	2023-03-24		
CVE-2023-20982	android		2023-03-24		
CVE-2023-20982	android	In btm_ble_rand_enc_complete of btm_sec.cc, there is a possible out of bounds read due to a missing bounds check. This	2023-03-24		
CVE-2023-20982	android google -	In btm_ble_rand_enc_complete of btm_sec.cc, there is a	2023-03-24		

		avalation Product. AndraidVersions, Andraid 12Andraid ID.			1
		exploitation.Product: AndroidVersions: Android-13Android ID: A-260569449			
		In ParseBqrLinkQualityEvt of btif_bqr.cc, there is a possible out			
		of bounds read due to a missing bounds check. This could lead to			
		local information disclosure with System execution privileges			
	google -	needed. User interaction is not needed for exploitation. Product:	1		
CVE-2023-20984	android	AndroidVersions: Android-13Android ID: A-242993878	2023-03-24	4.4	Medium
		In btm_ble_clear_resolving_list_complete of			
		btm_ble_privacy.cc, there is a possible out of bounds read due			
		to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User	1		
	google -	interaction is not needed for exploitation.Product:	1		
CVE-2023-20986	android	AndroidVersions: Android-13Android ID: A-255304475	2023-03-24	4.4	Medium
		In btm_ble_write_adv_enable_complete_of_btm_ble_gap.cc,			
		there is a possible out of bounds read due to a missing bounds			
		check. This could lead to local information disclosure with	1		
		System execution privileges needed. User interaction is not			
CVE 2022 20000	google -	needed for exploitation.Product: AndroidVersions: Android-	2022 02 24	4.4	N. A. a. aliin maa
CVE-2023-20989	android	13Android ID: A-260568367  In btm_read_local_oob_complete of btm_sec.cc, there is a	2023-03-24	4.4	Medium
		possible out of bounds read due to a missing bounds check. This	1		
		could lead to local information disclosure with System execution	1		
		privileges needed. User interaction is not needed for	1		
	google -	exploitation.Product: AndroidVersions: Android-13Android ID:	1		
CVE-2023-20990	android	A-260568354	2023-03-24	4.4	Medium
		In btm_ble_process_periodic_adv_sync_lost_evt of			
		ble_scanner_hci_interface.cc, there is a possible out of bounds			
		read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.			
	google -	User interaction is not needed for exploitation.Product:	1		
CVE-2023-20991	android	AndroidVersions: Android-13Android ID: A-255305114	2023-03-24	4.4	Medium
012 2023 20331	anaroia	In multiple locations of p2p_iface.cpp, there is a possible out of	2020 00 2 1		Mediam
		bounds read due to a missing bounds check. This could lead to			
		local information disclosure with System execution privileges	1		
	google -	needed. User interaction is not needed for exploitation.Product:			
CVE-2023-21006	android	AndroidVersions: Android-13Android ID: A-257030027	2023-03-24	4.4	Medium
		In multiple locations of p2p_iface.cpp, there is a possible out of	1		
		bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges	1		
	google -	needed. User interaction is not needed for exploitation. Product:			
CVE-2023-21007	android	AndroidVersions: Android-13Android ID: A-257029965	2023-03-24	4.4	Medium
	<u> </u>	In multiple locations of p2p_iface.cpp, there is a possible out of			
		bounds read due to a missing bounds check. This could lead to	1		
		local information disclosure with System execution privileges	1		
	google -	needed. User interaction is not needed for exploitation.Product:	1		
CVE-2023-21008	android	AndroidVersions: Android-13Android ID: A-257030100	2023-03-24	4.4	Medium
		In multiple locations of p2p_iface.cpp, there is a possible out of	1		
		bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges			
	google -	needed. User interaction is not needed for exploitation. Product:	1		
CVE-2023-21009	android	AndroidVersions: Android-13Android ID: A-257029925	2023-03-24	4.4	Medium
		In multiple locations of p2p_iface.cpp, there is a possible out of			
		bounds read due to a missing bounds check. This could lead to			
	_	local information disclosure with System execution privileges			
CVE 2022 24042	google -	needed. User interaction is not needed for exploitation. Product:	2022.02.24	A A	NA = -1:
CVE-2023-21010	android	AndroidVersions: Android-13Android ID: A-257029915  In multiple locations of p2p_iface.cpp, there is a possible out of	2023-03-24	4.4	Medium
		bounds read due to a missing bounds check. This could lead to			
		local information disclosure with System execution privileges			
	google -	needed. User interaction is not needed for exploitation. Product:			
CVE-2023-21011	android	AndroidVersions: Android-13Android ID: A-257029912	2023-03-24	4.4	Medium
		In multiple locations of p2p_iface.cpp, there is a possible out of			
		bounds read due to a missing bounds check. This could lead to			
		local information disclosure with System execution privileges			
CVE 2022 24042	google -	needed. User interaction is not needed for exploitation. Product:	2022.02.24	A A	NA a alt
CVE-2023-21012	android	AndroidVersions: Android-13Android ID: A-257029812  In forceStaDisconnection of hostapd.cpp, there is a possible out	2023-03-24	4.4	Medium
		of bounds read due to a missing bounds check. This could lead to			
		local information disclosure with System execution privileges			
	google -	needed. User interaction is not needed for exploitation. Product:			
CVE-2023-21013	android	AndroidVersions: Android-13Android ID: A-256818945	2023-03-24	4.4	Medium
		In multiple locations of p2p_iface.cpp, there is a possible out of			
		bounds read due to a missing bounds check. This could lead to			
	-	local information disclosure with System execution privileges			
CVE 2022 24211	google -	needed. User interaction is not needed for exploitation. Product:	2022 02 2 :	4.6	N.A !!
CVE-2023-21014	android	AndroidVersions: Android-13Android ID: A-257029326	2023-03-24	4.4	Medium
İ		In ufdt_local_fixup_prop of ufdt_overlay.c, there is a possible	i		
	ء ماموام	out of hounds read due to an incorrect hounds check. This could be	!		
CVE-2023-21025	google - android	out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution	2023-03-24	4.4	Medium

		privileges needed liser interaction is not needed for			
		privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13Android ID:			
		A-254929746			
		In _ufdt_output_node_to_fdt_of_ufdt_convert.c, there is a			
		possible out of bounds read due to a heap buffer overflow. This			
		1 '			
		could lead to local information disclosure with System execution			
	la	privileges needed. User interaction is not needed for			
CVE 2022 24022	google -	exploitation.Product: AndroidVersions: Android-13Android ID:	2022 02 24	4.4	0.4
CVE-2023-21032	android	A-248085351	2023-03-24	4.4	Medium
		In dumpstateBoard of Dumpstate.cpp, there is a possible out of			
		bounds read due to an incorrect bounds check. This could lead			
		to local information disclosure with System execution privileges			
		needed. User interaction is not needed for exploitation.Product:			
	google -	AndroidVersions: Android kernelAndroid ID: A-			
CVE-2023-21039	android	263783650References: N/A	2023-03-24	4.4	Medium
		In init of VendorGraphicBufferMeta, there is a possible out of			
		bounds read due to a missing bounds check. This could lead to			
		local information disclosure with System execution privileges			
		needed. User interaction is not needed for exploitation.Product:			
	google -	AndroidVersions: Android kernelAndroid ID: A-			
CVE-2023-21044	android	253425086References: N/A	2023-03-24	4.4	Medium
		When cpif handles probe failures, there is a possible out of			
		bounds read due to a use after free. This could lead to local			
		information disclosure with System execution privileges needed.			
		User interaction is not needed for exploitation.Product:			
	google -	AndroidVersions: Android kernelAndroid ID: A-			
CVE-2023-21045	android	259323725References: N/A	2023-03-24	4.4	Medium
		In ConvertToHalMetadata of aidl_utils.cc, there is a possible out			
		of bounds read due to an incorrect bounds check. This could lead			
		to local information disclosure with System execution privileges			
		needed. User interaction is not needed for exploitation.Product:			
	google -	AndroidVersions: Android kernelAndroid ID: A-			
CVE-2023-21046	android	253424924References: N/A	2023-03-24	4.4	Medium
		In ConvertToHalMetadata of aidl_utils.cc, there is a possible out			
		of bounds read due to a missing bounds check. This could lead to			
		local information disclosure with System execution privileges			
		needed. User interaction is not needed for exploitation.Product:			
	google -	AndroidVersions: Android kernelAndroid ID: A-			
CVE-2023-21047	android	256166866References: N/A	2023-03-24	4.4	Medium
		In handleEvent of nan.cpp, there is a possible out of bounds read			
		due to a missing bounds check. This could lead to local			
		information disclosure with System execution privileges needed.			
		User interaction is not needed for exploitation.Product:			
	google -	AndroidVersions: Android kernelAndroid ID: A-			
CVE-2023-21048	android	259304053References: N/A	2023-03-24	4.4	Medium
		In append_camera_metadata of camera_metadata.c, there is a			
		possible out of bounds read due to a missing bounds check. This			
		could lead to local information disclosure with System execution			
		privileges needed. User interaction is not needed for			
	google -	exploitation.Product: AndroidVersions: Android kernelAndroid			
CVE-2023-21049	android	ID: A-236688120References: N/A	2023-03-24	4.4	Medium
_		IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1,			
	ibm - multiple	and 4.1.1 could allow an authenticated user to obtain sensitive			
CVE-2023-25687	products	information from log files. IBM X-Force ID: 247602.	2023-03-21	4.3	Medium
		When using the RemotelpFilter with requests received from a			
		reverse proxy via HTTP that include the X-Forwarded-Proto			
		header set to https, session cookies created by Apache Tomcat			
		11.0.0-M1 to 11.0.0M2, 10.1.0-M1 to 10.1.5, 9.0.0-M1 to			
	apache -	9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute.			
	multiple	This could result in the user agent transmitting the session			
CVE-2023-28708	products	cookie over an insecure channel.	2023-03-22	4.3	Medium
		7 7 7		<u>-</u> '	1

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's الله 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 and their impacts.