

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 النشّرة 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) for the week from 25th of June to 1st of July. Vulnerabilities are scored using the Common Common Vulnerability علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Vulnerability Scoring System (CVSS) standard as per the following severity:

Critical: CVSS base score of 9.0-10.0 High: CVSS base score of 7.0-8.9 Medium: CVSS base score 4.0-6.9 Low: CVSS base score 0.0-3.9

National Vulnerability Database (NVD) للأسبوع من ٢٥ يونيو إلى ١ يوليو. Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

عالى جدًا: النتيجة الأساسية لـCVSS 9.0-10.0

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
		A path traversal vulnerability in the Trend Micro Apex One and			
		Apex One as a Service could allow an unauthenticated attacker to			
	trendmicro -	upload an arbitrary file to the Management Server which could			
CVE-2023-32557	multiple products	lead to remote code execution with system privileges.	2023-06-26	9.8	Critical
		IBM Informix JDBC Driver 4.10 and 4.50 is susceptible to remote			
	21 112 . 1 .	code execution attack via JNDI injection when driver code or the			
CVE 2022 270CC	ibm - multiple	application using the driver do not verify supplied LDAP URL in	2022 06 20	0.0	Cuitiaal
CVE-2023-27866	products	Connect String. IBM X-Force ID: 249511. In cd CodeMsg of cd codec.c, there is a possible out of bounds	2023-06-28	9.8	Critical
		write 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 exploitation.Product:			
		AndroidVersions: Android kernelAndroid ID: A-			
CVE-2023-21066	google - android	250100597References: N/A	2023-06-28	9.8	Critical
<u>CVL 2023 21000</u>	google unarola	Heap out-of-bound write vulnerability in Exynos baseband prior to	2023 00 20	3.0	Critical
		SMR Jun-2023 Release 1 allows remote attacker to execute			
CVE-2023-21517	samsung - exynos	arbitrary code.	2023-06-28	9.8	Critical
	hp -	,			21.0.001
	laserjet_pro_mfp_	Certain HP LaserJet Pro print products are potentially vulnerable to			
	m478-	Potential Remote Code Execution and/or Elevation of Privilege via			
	m479_w1a75a_fir	Server-Side Request Forgery (SSRF) using the Web Service Eventing			
CVE-2023-35175	mware	model.	2023-06-30	9.8	Critical
		A path traversal exists in a specific service dll of Trend Micro			
	trendmicro -	Mobile Security (Enterprise) 9.8 SP5 which could allow an			
CVE-2023-32521	mobile_security	unauthenticated remote attacker to delete arbitrary files.	2023-06-26	9.1	Critical
		Type Confusion in V8 in Google Chrome prior to 114.0.5735.198			
		allowed a remote attacker to potentially exploit heap corruption			
CVE-2023-3420	google - chrome	via a crafted HTML page. (Chromium security severity: High)	2023-06-26	8.8	High
		Use after free in Media in Google Chrome prior to 114.0.5735.198			
		allowed a remote attacker to potentially exploit heap corruption			
CVE-2023-3421	google - chrome	via a crafted HTML page. (Chromium security severity: High)	2023-06-26	8.8	High
		Use after free in Guest View in Google Chrome prior to			
		114.0.5735.198 allowed an attacker who convinced a user to			
		install a malicious extension to potentially exploit heap corruption			
CVE-2023-3422	google - chrome	via a crafted HTML page. (Chromium security severity: High)	2023-06-26	8.8	High
		Affected versions of Trend Micro Mobile Security (Enterprise) 9.8			
		SP5 contain some widgets that would allow a remote user to			
		bypass authentication and potentially chain with other			
		vulnerabilities.			
		Diagon mater an attackon recent first abtain the ability to such			
		Please note: an attacker must first obtain the ability to execute			
		low-privileged code on the target system in order to exploit these vulnerabilities.			
		vuniciabilities.			
	trendmicro -				
CVE-2023-32523	mobile_security	This is similar to, but not identical to CVE-2023-32524.	2023-06-26	8.8	High
<u> </u>		12 3 10, 100 100 100 100 100		1 3.3	

		Affected versions of Trend Micro Mobile Security (Enterprise) 9.8 SP5 contain some widgets that would allow a remote user to bypass authentication and potentially chain with other vulnerabilities.			
		Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit these vulnerabilities.			
	trendmicro -				
CVE-2023-32524	mobile_security	This is similar to, but not identical to CVE-2023-32523.	2023-06-26	8.8	High
		Trend Micro Mobile Security (Enterprise) 9.8 SP5 contains vulnerable .php files that could allow a remote attacker to execute arbitrary code on affected installations.			
		Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.			
CVE 2022 22527	trendmicro -	This is similar to hut not identical to CVF 2022 22520	2022 06 26	0.0	Hiah
CVE-2023-32527	mobile_security	This is similar to, but not identical to CVE-2023-32528. Trend Micro Mobile Security (Enterprise) 9.8 SP5 contains	2023-06-26	8.8	High
		vulnerable .php files that could allow a remote attacker to execute arbitrary code on affected installations.			
		Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.			
CVE-2023-32528	trendmicro - mobile_security	This is similar to, but not identical to CVE-2023-32527. Vulnerable modules of Trend Micro Apex Central (on-premise) contain vulnerabilities which would allow authenticated users to perform a SQL injection that could lead to remote code execution.	2023-06-26	8.8	High
		Please note: an attacker must first obtain authentication on the target system in order to exploit these vulnerabilities.			
CVE-2023-32529	trendmicro - apex_central	This is similar to, but not identical to CVE-2023-32530. Vulnerable modules of Trend Micro Apex Central (on-premise) contain vulnerabilities which would allow authenticated users to perform a SQL injection that could lead to remote code execution.	2023-06-26	8.8	High
		Please note: an attacker must first obtain authentication on the target system in order to exploit these vulnerabilities.			
CVE-2023-32530	trendmicro -	This is similar to but not identical to CVE 2022 22E20	2023-06-26	8.8	High
	apex_central microsoft -	This is similar to, but not identical to CVE-2023-32529. Microsoft Edge (Chromium-based) Elevation of Privilege			High
CVE-2022-26899	edge_chromium	Vulnerability Improper Input Validation vulnerability in Apache Software	2023-06-29	8.8	High
	apache - apache- airflow-providers-	Foundation Apache Airflow JDBC Provider. Airflow JDBC Provider Connection's [Connection URL] parameters had no restrictions, which made it possible to implement RCE attacks via different type JDBC drivers, obtain airflow server permission. This issue affects Apache Airflow JDBC Provider: before 4.0.0.			
CVE-2023-22886	jdbc hp -		2023-06-29	8.8	High
	laserjet_pro_mfp_ m478-	Certain HP LaserJet Pro print products are potentially vulnerable to			
	m479_w1a75a_fir	Buffer Overflow and/or Denial of Service when using the backup &			
CVE-2023-35176	mware	restore feature through the embedded web service on the device.	2023-06-30	8.8	High

Legiple_pro_mriy_ mri29s_st77s_life mreare_ hashing_pro_mriy_ mri29s_st77s_life mreare_ hashing_pro_mriy_ hashing_pro_mr		L.				
CVE-2023-35177 mixing a statishase builder overflow reducted to the compact foot from the provided of the compact from the compact		hp -				
m479_w1373 aft mover was a stack-based buffer overflow related to the compact font format parts. WE 2023-35179 May 3473 aft mover was approximated by the parts of the compact font format parts. CVE-2023-3519 m479_w1373 aft mover was approximated by the parts of the compact format parts. CVE-2023-3519 m479_w1373 aft mover was approximated by the parts of the compact format parts of the compact parts of t			Certain HP Laser let Pro print products are notentially vulnerable to			
December 2015 Process						
h p- laseriet promise ma78 ma78 ma78 ma78 mark promote the place of the promote the place of the promote that the promote tha	CVE-2023-35177		·	2023-06-30	8.8	High
Isseriet, pro_refp_mr/39_stay27s_fr mr/39_stay27s_fr mr						
ma75 ma75 ma75 margared margar		•				
### Output Security Security						
microsoft - Que get from the based Security Feature Bypass (Vet 2021-34475 Getge, thromium based) Flevation of Privilege (Vet 2021-34475 Microsoft right (Chromium based) Flevation of Privilege (Vet 2021-34475 Microsoft right (Chromium based) Flevation of Privilege (Vet 2021-34475 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34478 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2021-34418 Microsoft Edge (Chromium based) Elevation of Privilege (Vet 2		m479_w1a75a_fir	Certain HP LaserJet Pro print products are potentially vulnerable to			
### CVE-2021-34475 edge_chromium Valuerability commitments valuerability commitments valuerability commitments valuerability	CVE-2023-35178	mware	Buffer Overflow when performing a GET request to scan jobs.	2023-06-30	8.8	High
CVE_2023_34456 edge chromium based Elevation of Privilege 2073-07-01 8.8 High						
CVE-2072-39146 edge chromium Valentability CVE-2072-39146 edge chromium Microsoft Edge (Chromium-based) Elevation of Privilege 2073-06-29 8.3 High CVE-2073-31417 edge chromium Valentability edge c	CVE-2021-31982	· -	'	2023-07-01	8.8	High
CVE-2023-34146 edge chromium based Elevation of Privilege 2023-06-78 8.3 High Important						
CVE-2023-34148 cedge chromium CVE-2023-34149 cedge chromium CVE-2023-34140 cedge c	CVE-2021-34475		,	2023-07-01	8.8	High
Microsoft Edge (Chromium-based) Elevation of Privilege 2023-06-28 8.2 Migh						
Section	CVE-2022-29146		,	2023-06-29	8.3	High
lenowo- scalarizy_administrate access to events and other data stored in IXAC bet or a SCI. might of the continue of th	CVE 2024 24027		,	2022 05 20	0.0	112.1.
Apath raversal exists in a specific exist point not defer to exploit this vulnerability in a positive point of the apath raversal exists in a specific exist point not defer to exploit this vulnerability and point of the apath raversal exists in a specific exist point not defer to exploit this vulnerability and the executive files. Apath raversal exists in a specific exist point not defer to exploit this vulnerability and the ability to execute low-privileged code on the target system in order to exploit this vulnerability and trendmicro mobile security. Trend Micro Security 2021, 2022, and 2023 [Consumer] are vulnerability and with respect to a DLL Highding vulnerability which could allow an attacker to use a specific executable file as an execution and/or presistence mechanism which could execute a malicious program each time the executable file is an execution and/or presistence mechanism which could execute a malicious program each first the executable file as an execution and/or presistence mechanism which could execute a malicious program each first the executable file as an execution and/or presistence mechanism which could execute a malicious program each first the executable file as an execution and/or presistence mechanism which could execute a malicious program each first the executable file as an execution and/or presistence mechanism which could execute a malicious groups and anticous program each first the executation file is started. 2023-06-26 7.8 High Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. 2023-06-26 7.8 High	CVE-2021-31937		•	2023-06-28	8.2	High
or injection vulnerability in a specific web API. A path traversal exists in a specific did of Trend Micro Mobile Security (Enterprise) 3.8.595 which could allow an authenticated remote attacker to delete arbitrary files. Viernamicro Piease note: an attacker must first obtain the ability to execute low privileged code on the target system in order to exploit this vulnerability. Viernamicro Trend Micro Security 2021, 2022 and 2023 [Consumer] are vulnerable to a DLH Hipsching which could allow an attacker to use a specific executable file as an execution and/or persistence mechanism which could execute a mulalicous program can deat time the executable file is started. An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Viernamicro Multiple products This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Viernamicro Multiple products This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Viernamicro Multiple products This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Viernamicro Multiple products This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One and Apex One as a Service security agent c			· · · · · · · · · · · · · · · · · · ·			
A path traversal exists in a specific dil of Trend Micro Mobile Security (Europrise) 9.8.59 which could allow an authenticated remote attacker to delete arbitrary files. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trend Micro Security 2021, 2022, and 2023 (Consumer) are vulnerable continued attacker to use a specific executable file as an execution and/or processitence mechanism which could execute a malicious program each time the executable file is as insecution and/or processitence mechanism which could execute a malicious program each time the executable file is as a resecution and/or processitence mechanism which could execute a malicious program each time the executable file is as a resecution and/or processitence mechanism which could execute a malicious program each time the executable file is as resecution and/or processitence mechanism which could execute a malicious program each time the executable file is as resecution and/or page on a malicious and attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an abitrary value to specific Trend Micro apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an abitrary value to specific Trend Micro apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an abitrary value to specific Trend Micro apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an abitrary value to specific Trend Micro apex One and Apex One as a Service security agent could allow a l	CVE 2022 24410	· -	·	2022 06 26	0.1	مادانا
Security (Enterprise) 9.8 SPS which could allow an authenticated remote attacker to delete arbitrary files. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to use a specific executable file is started. An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Trendmicro-multiple products This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Apex One and Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Trendmicro-multiple products This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Apex One as a Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. This is a similar, but not identical vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One as a Service security agent could allow a local attacker to escalate privileges and w	<u>CVE-2023-34418</u>	or		2023-06-26	8.1	High
remote attacker to delete arbitrary files. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trend Micro Security 2021, 2022, and 2023 (Consumer) are vulnerability to use a specific security appears and attacker to use as specific securatiable file as an execution and/or persistence mechanism which could sexcute a malicious program each multiple products an untrusted search path vulnerability in the Trend Micro Apex. One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability in the Trend Micro Apex. One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro— This is a similar, but not identical vulnerability in the Trend Micro Apex. One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro— Apex One and Apex One as a Service security agent could allow a local attacker to escalate receivable and an arbitrary value to specific Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker on a specific Trend Micro Ap						
trendmicro- mobile_security Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability of a DLL Highding vulnerability and 2023 (Consumer) are vulnerability or a DLL Highding vulnerability which could allow an attacker to use a specific executable file as an execution and/or persistence mechanism which could execute a malicious program each time the executed lies is started. An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro- multiple products This is a similar, but not identical vulnerability as CVE-2023-34145. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro- multiple products This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro- This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One and Apex One as a Service securit						
trendmicro mobile_security vollnerability. Trend Micro Security 2011, 2022, and 2023 (Gonsumer) are vulnerabile to a DLL Highdign vulnerability which could allow an attacker to use a specific executable file as an execution and/or persistence mechanism which could execute a malicious program multiple products EVE-2023-28929 Trend Micro Security 2011, 2022, and 2023 (Gonsumer) are vulnerabile to a DLL Highdign vulnerability which could allow an attacker to use a specific executable file as an execution and/or persistence mechanism which could execute a malicious program multiple products An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileged code on the target system in order to exploit this vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Trendmicro multiple products Tris is a similar, but not identical vulnerability as CVE-2023-34145. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro multiple products Tris is a similar, but not identical vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Trendmicro multiple products Trendmicro trendmicro and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations.			remote attacker to delete arbitrary files.			
trendmicro mobile_security vollnerability. Trend Micro Security 2011, 2022, and 2023 (Gonsumer) are vulnerabile to a DLL Highdign vulnerability which could allow an attacker to use a specific executable file as an execution and/or persistence mechanism which could execute a malicious program multiple products EVE-2023-28929 Trend Micro Security 2011, 2022, and 2023 (Gonsumer) are vulnerabile to a DLL Highdign vulnerability which could allow an attacker to use a specific executable file as an execution and/or persistence mechanism which could execute a malicious program multiple products An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileged code on the target system in order to exploit this vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Trendmicro multiple products Tris is a similar, but not identical vulnerability as CVE-2023-34145. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro multiple products Tris is a similar, but not identical vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Trendmicro multiple products Trendmicro trendmicro and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations.						
trendmicro mobile_security vollnerability. Trend Micro Security 2011, 2022, and 2023 (Gonsumer) are vulnerabile to a DLL Highdign vulnerability which could allow an attacker to use a specific executable file as an execution and/or persistence mechanism which could execute a malicious program multiple products EVE-2023-28929 Trend Micro Security 2011, 2022, and 2023 (Gonsumer) are vulnerabile to a DLL Highdign vulnerability which could allow an attacker to use a specific executable file as an execution and/or persistence mechanism which could execute a malicious program multiple products An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileged code on the target system in order to exploit this vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Trendmicro multiple products Tris is a similar, but not identical vulnerability as CVE-2023-34145. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro multiple products Tris is a similar, but not identical vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Trendmicro multiple products Trendmicro trendmicro and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations.						
trendmicro mobile_security vollnerability. Trend Micro Security 2011, 2022, and 2023 (Gonsumer) are vulnerabile to a DLL Highdign vulnerability which could allow an attacker to use a specific executable file as an execution and/or persistence mechanism which could execute a malicious program multiple products EVE-2023-28929 Trend Micro Security 2011, 2022, and 2023 (Gonsumer) are vulnerabile to a DLL Highdign vulnerability which could allow an attacker to use a specific executable file as an execution and/or persistence mechanism which could execute a malicious program multiple products An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileged code on the target system in order to exploit this vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Trendmicro multiple products Tris is a similar, but not identical vulnerability as CVE-2023-34145. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro multiple products Tris is a similar, but not identical vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Trendmicro multiple products Trendmicro trendmicro and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations.			Please note: an attacker must first obtain the ability to execute			
wulnerability. wulnerability which could allow an attacker to use a sperific security 2021, 2022, and 2022 (Consumer) are vulnerable to a DL Hijacking vulnerability which could allow an attacker to use a sperific securitable false as an execution and/or persistence mechanism which could execute a malicious program each time the executable file is started. An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products Trendmicro - multiple products Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note: an attacker to escalate their privileges on affected installations. Please note: an attacker to escalate their privileges on affected installations. Please note: an attacker to escalate their privileges on affected installations. Please note: an attacker to escalate their privileges on affected installations. Please note: an attacker to escalate their privileges on affected installations. Please note: an attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro - multiple products Trendmicro - products -		trendmicro -	·			
Trend Micro Security 2021, 2022, and 2023 (Consumer) are vulnerable to a DLL High disching vulnerability which could allow a stacker to use a specific executable file as an execution and/or persistence mechanism which could execute a maliclous program attacker to use a specific executable file is started. An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34145. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34144. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local and appears of the privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vul	CVE-2023-32522		, , , , , , , , , , , , , , , , , , , ,	2023-06-26	8.1	High
trendmicro- multiple products CVE-2023-28929 multiple products trendmicro- multiple products An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to secalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. An exposed dangerous function vulnerability in the Trend Micro Apex On			·	2 2 2 20	-	
trendmicro- multiple products This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34144. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability in the Trend Micro William Archiver to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. This is a similar, but not identical vulnerability to execute low-privileged code on the target system in order to exploit this vulnerability. An exposed dangerous function vulnerability in the Trend Micro Apox One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific						
williple products each time the executable file is started. 2023-06-26 7.8 High An untrusted search path vulnerability in the Trend Micro Apex One and Apex One a			, e			
An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34145. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro - multiple products This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34144. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability to execute low-privileged code on the target system in order to exploit this vulnerability. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One and Apex		trendmicro -	persistence mechanism which could execute a malicious program			
One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34145. An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34147 This is a similar, but not identical vulnerability to execute low-privileged code on the target system in order to exploit this vulnerability. An exposed dangerous function vulnerability in the Trend Micro and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro An exposed dangerous function vulnerability in the Trend Micro An exposed dangerous function vulnerability in the Trend Micro An exposed dangerous function vulnerability in the Trend Micro An exposed dangerous function vulnerability in the Trend Micro	CVE-2023-28929	multiple products	each time the executable file is started.	2023-06-26	7.8	High
attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro - multiple products This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker one as a Service security agent could allow a local attacker one as a Service security agent could allow a local attacker one as a Service security agent could allow a local attacker one as a Service security agent could allow a local attacker one as a Service security agent could allow a local attacker one as a Service security agent could allow a local attacker one as a Service security agent could allow a local attacker one as a Service security agent could allow a local attacker one as a Service security agent could allow a lo			An untrusted search path vulnerability in the Trend Micro Apex			
Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro - multiple products An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as Apex One			One and Apex One as a Service security agent could allow a local			
Iow-privileged code on the target system in order to exploit this vulnerability.			attacker to escalate their privileges on affected installations.			
Iow-privileged code on the target system in order to exploit this vulnerability.						
Iow-privileged code on the target system in order to exploit this vulnerability.						
Iow-privileged code on the target system in order to exploit this vulnerability.						
vulnerability. trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34145. 2023-06-26 7.8 High An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products An exposed dangerous function vulnerability as CVE-2023-34144. 2023-06-26 7.8 High An exposed dangerous function vulnerability as an abitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations.						
trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34145. An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34144. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a Apex One and Apex One as a Service security agent could allow a						
This is a similar, but not identical vulnerability as CVE-2023-34145. 2023-06-26 7.8 High An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34144. 2023-06-26 7.8 High An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. 2023-06-26 7.8 High An exposed dangerous function vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations.			vulnerability.			
This is a similar, but not identical vulnerability as CVE-2023-34145. 2023-06-26 7.8 High An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34144. 2023-06-26 7.8 High An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. 2023-06-26 7.8 High An exposed dangerous function vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations.						
This is a similar, but not identical vulnerability as CVE-2023-34145. 2023-06-26 7.8 High An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34144. 2023-06-26 7.8 High An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. 2023-06-26 7.8 High An exposed dangerous function vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker one and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations.						
An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34144. 2023-06-26 An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. 2023-06-26 This is a similar, but not identical vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a	CVE 2022 24444		This is a similar but set identical unbased little of CVE 2022 24445	2022 06 26	7.0	118 - -
One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro - multiple products An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a	CVE-2023-34144	multiple products		2023-06-26	7.8	High
attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One as a Service security agent could allow a local allow a service security agent could allow a local allow a local and cve-2023-34148.			l			
Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. Trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34144. 2023-06-26 An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a Apex One and Apex One as a Service security agent could allow a			, -			
low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products An exposed dangerous function vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One and Apex One as a Service security agent could allow a			actacker to escarate their privileges on affected installations.			
low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products An exposed dangerous function vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One and Apex One as a Service security agent could allow a						
low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products An exposed dangerous function vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One and Apex One as a Service security agent could allow a						
low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products An exposed dangerous function vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One and Apex One as a Service security agent could allow a			Please note: an attacker must first obtain the ability to execute			
trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34144. 2023-06-26 An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products trendmicro - multiple products An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a			,			
trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a			, , , , , , , , , , , , , , , , , , , ,			
This is a similar, but not identical vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a High An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a						
This is a similar, but not identical vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a High An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a						
This is a similar, but not identical vulnerability as CVE-2023-34144. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a High An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a		trendmicro -				
An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a	CVE-2023-34145		This is a similar, but not identical vulnerability as CVE-2023-34144.	2023-06-26	7.8	High
Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a		, , , , , , , , ,	•			<u> </u>
local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a			, , , , , , , , , , , , , , , , , , , ,			
specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a						
Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. trendmicro - multiple products This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a			, -			
low-privileged code on the target system in order to exploit this vulnerability. trendmicro - This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. CVE-2023-34146						
low-privileged code on the target system in order to exploit this vulnerability. trendmicro - This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. CVE-2023-34146						
low-privileged code on the target system in order to exploit this vulnerability. trendmicro - This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. CVE-2023-34146						
trendmicro - This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a			·			
trendmicro - This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148. An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a			, , , , , , , , , , , , , , , , , , , ,			
CVE-2023-34146multiple productsand CVE-2023-34148.2023-06-267.8HighAn exposed dangerous function vulnerability in the Trend Micro trendmicro -Apex One and Apex One as a Service security agent could allow a4			vulnerability.			
CVE-2023-34146multiple productsand CVE-2023-34148.2023-06-267.8HighAn exposed dangerous function vulnerability in the Trend Micro trendmicro -Apex One and Apex One as a Service security agent could allow a4						
CVE-2023-34146multiple productsand CVE-2023-34148.2023-06-267.8HighAn exposed dangerous function vulnerability in the Trend Micro trendmicro -Apex One and Apex One as a Service security agent could allow a4						
CVE-2023-34146multiple productsand CVE-2023-34148.2023-06-267.8HighAn exposed dangerous function vulnerability in the Trend Micro trendmicro -Apex One and Apex One as a Service security agent could allow a4						
An exposed dangerous function vulnerability in the Trend Micro trendmicro - Apex One and Apex One as a Service security agent could allow a	CVE 2022 24445		,	2022 00 00	7.0	100.1
trendmicro - Apex One and Apex One as a Service security agent could allow a	CVE-2023-34146	multiple products		2023-06-26	7.8	High
, ,		Appendict to the	, ,			
CVE-2025-34147 multiple products local attacker to escalate privileges and write an arbitrary value to 2023-06-26 7.8 High	CVE 2022 244 47		, ,	2022 00 20	7.0	11:44-
	CVE-2U23-3414/	I muniple products	Tocal attacker to escalate privileges and write an arbitrary value to	∠UZ3-Ub-Zb	/.ŏ	піgп

		specific Trand Micro agent subleve on affected installations			
		specific Trend Micro agent subkeys on affected installations.			
		Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.			
		This is a similar, but not identical vulnerability as CVE-2023-34146 and CVE-2023-34148.			
		An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations.			
		Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.			
CVE-2023-34148	trendmicro - multiple products	This is a similar, but not identical vulnerability as CVE-2023-34146 and CVE-2023-34147.	2023-06-26	7.8	High
		Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability in Apache Software Foundation Apache Airflow ODBC Provider. In OdbcHook, A privilege escalation vulnerability exists in a system due to controllable ODBC driver parameters that allow the loading of arbitrary dynamic-link libraries, resulting in command			
	apache - apache- airflow-providers-	execution. Starting version 4.0.0 driver can be set only from the hook constructor.			
CVE-2023-34395	odbc	This issue affects Apache Airflow ODBC Provider: before 4.0.0.	2023-06-27	7.8	High
	ibm - multiple	IBM Robotic Process Automation for Cloud Pak 21.0.1 through 21.0.7.3 and 23.0.0 through 23.0.3 is vulnerable to security misconfiguration of the Redis container which may provide			
CVE-2023-22593	products	elevated privileges. IBM X-Force ID: 244074. A vulnerability in the client update process of Cisco AnyConnect	2023-06-27	7.8	High
	cisco - multiple	Secure Mobility Client Software for Windows and Cisco Secure Client Software for Windows could allow a low-privileged, authenticated, local attacker to elevate privileges to those of SYSTEM. The client update process is executed after a successful VPN connection is established. This vulnerability exists because improper permissions are assigned to a temporary directory that is created during the update process. An attacker could exploit this vulnerability by abusing a specific function of the Windows installer process. A successful exploit could allow the attacker to			
CVE-2023-20178	products	execute code with SYSTEM privileges. In hasInputInfo of Layer.cpp, there is a possible bypass of user	2023-06-28	7.8	High
		interaction requirements due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13 Android ID: A-			
CVE-2022-20443	google - android	194480991 In lwis_i2c_device_disable of lwis_device_i2c.c, there is a possible UAF due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	2023-06-28	7.8	High
CVE-2023-21147	google - android	AndroidVersions: Android kernelAndroid ID: A- 269661912References: N/A In registerGsmaServiceIntentReceiver of ShannonRcsService.java,	2023-06-28	7.8	High
		there is a possible way to activate/deactivate RCS service due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-			
CVE-2023-21149	google - android	270050709References: N/A In multiple functions of WifiCallingSettings.java, there is a possible way to change calling preferences for the admin user due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-	2023-06-28	7.8	High
CVE-2023-21172	google - android	13Android ID: A-262243015 In isPageSearchEnabled of BillingCycleSettings.java, there is a	2023-06-28	7.8	High
CVE-2023-21174	google - android	possible way for the guest user to change data limits due to a	2023-06-28	7.8	High

		permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-			
		13Android ID: A-235822222 In onCreate of DataUsageSummary.java, there is a possible method for a guest user to enable or disable mobile data due to a permissions bypass. This could lead to local escalation of privilege			
		with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-			
CVE-2023-21175	google - android	13Android ID: A-262243574 In parseSecurityParamsFromXml of XmlUtil.java, there is a possible	2023-06-28	7.8	High
		bypass of user specified wifi encryption protocol due to improperly used crypto. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not			
CVE-2023-21179	google - android	needed for exploitation.Product: AndroidVersions: Android- 13Android ID: A-272755865	2023-06-28	7.8	High
		In ForegroundUtils of ForegroundUtils.java, there is a possible way to read NFC tag data while the app is still in the background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:			
CVE-2023-21183	google - android	AndroidVersions: Android-13Android ID: A-235863754 In getCurrentPrivilegedPackagesForAllUsers of CarrierPrivilegesTracker.java, there is a possible permission bypass	2023-06-28	7.8	High
CVE-2023-21184	google - android	due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13Android ID: A-267809568	2023-06-28	7.8	High
	8008.0	In multiple functions of WifiNetworkFactory.java, there is a missing permission check. This could lead to local escalation of privilege from the guest user with no additional execution privileges needed. User interaction is not needed for			
CVE-2023-21185	google - android	exploitation.Product: AndroidVersions: Android-13Android ID: A-266700762	2023-06-28	7.8	High
		In onCreate of UsbAccessoryUriActivity.java, there is a possible way to escape the Setup Wizard due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-			
CVE-2023-21187	google - android	246542917 In fixNotification of NotificationManagerService.java, there is a	2023-06-28	7.8	High
CVE-2023-21191	google - android	possible bypass of notification hide preference due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-269738057 In setInputMethodWithSubtypeldLocked of InputMethodManagerService.java, there is a possible way to setup input methods that are not enabled due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not	2023-06-28	7.8	High
CVE-2023-21192	google - android	needed for exploitation.Product: AndroidVersions: Android- 13Android ID: A-227207653 there is a possible way to bypass the protected confirmation	2023-06-28	7.8	High
CVE-2023-21225	google - android	screen due to Failure to lock display power. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 270403821References: N/A A heap out-of-bounds write vulnerability in the Linux Kernel ipvlan network driver can be exploited to achieve local privilege escalation.	2023-06-28	7.8	High
		The out-of-bounds write is caused by missing skb->cb initialization in the ipvlan network driver. The vulnerability is reachable if CONFIG_IPVLAN is enabled.			
CVE-2023-3090	linux - linux_kernel	We recommend upgrading past commit 90cbed5247439a966b645b34eb0a2e037836ea8e.	2023-06-28	7.8	High
		A use-after-free vulnerability in the Linux Kernel io_uring subsystem can be exploited to achieve local privilege escalation.			
		Racing a io_uring cancel poll request with a linked timeout can cause a UAF in a hrtimer.			
CVE-2023-3389	linux - multiple products	We recommend upgrading past commit ef7dfac51d8ed961b742218f526bd589f3900a59 (4716c73b188566865bdd79c3a6709696a224ac04 for 5.10 stable	2023-06-28	7.8	High

		and 0e388fce7aec40992eadee654193cad345d62663 for 5.15 stable).			
		Improper access control vulnerability in SearchWidget prior to			
CVE-2023-21518	samsung - searchwidget	version 3.3 in China models allows untrusted applications to start arbitrary activity.	2023-06-28	7.8	High
ZVL-2023-21318	Searchwinger	A use-after-free vulnerability was found in the Linux kernel's	2023-00-28	7.8	High
		netfilter subsystem in net/netfilter/nf_tables_api.c.			
		Mishandled error handling with NFT_MSG_NEWRULE makes it			
		possible to use a dangling pointer in the same transaction causing			
		a use-after-free vulnerability. This flaw allows a local attacker with user access to cause a privilege escalation issue.			
		user access to cause a privilege escalation issue.			
CVE-2023-3390	linux - linux_kernel	We recommend upgrading past commit 1240eb93f0616b21c675416516ff3d74798fdc97.	2023-06-28	7.8	High
	_	A use-after-free flaw was found in the Netfilter subsystem of the			
		Linux kernel when processing named and anonymous sets in batch			
		requests, which can lead to performing arbitrary reads and writes			
	linux - multiple	in kernel memory. This flaw allows a local user with CAP_NET_ADMIN capability to crash or potentially escalate their			
CVE-2023-3117	products	privileges on the system.	2023-06-30	7.8	High
	p. co.a.co	Multiple vulnerabilities in Cisco Expressway Series and Cisco			
		TelePresence Video Communication Server (VCS) could allow an			
		authenticated attacker with Administrator-level read-only			
		credentials to elevate their privileges to Administrator with read-			
	cisco -	write credentials on an affected system. Note: "Cisco Expressway Series" refers to Cisco Expressway Control (Expressway-C) devices			
	telepresence_video	and Cisco Expressway Edge (Expressway-E) devices. For more			
	_communication_s	information about these vulnerabilities, see the Details section of			
VE-2023-20192	erver	this advisory.	2023-06-28	7.7	High
		An unauthenticated denial of service vulnerability exists in the			
	lenovo -	SMM v1, SMM v2, and FPC management web server which can be			
CVE-2023-2992	nextscale_n1200_e nclosure firmware	triggered under crafted conditions. Rebooting SMM or FPC will restore access to the management web server.	2023-06-26	7.5	High
<u> </u>	lenovo -	An unauthenticated XML external entity injection (XXE)	2023 00 20	7.5	11161
	xclarity_administrat	vulnerability exists in LXCA's Common Information Model (CIM)			
CVE-2023-3113	or	server that could result in read-only access to specific files.	2023-06-26	7.5	High
		A remote attacker could leverage a vulnerability in Trend Micro			
	trendmicro -	Mobile Security (Enterprise) 9.8 SP5 to download a particular log			
CVE-2023-35695	mobile_security	file which may contain sensitive information regarding the product.	2023-06-26	7.5	High
	_ ′	IBM QRadar SIEM 7.5.0 uses weaker than expected cryptographic			
	ibm - multiple	algorithms that could allow an attacker to decrypt highly sensitive			
VE-2023-26276	products ibm -	information. IBM X-Force ID: 248147.	2023-06-27	7.5	High
	cloud_pak_for_sec	IBM Cloud Pak for Security (CP4S) 1.9.0.0 through 1.9.2.0 could allow an attacker with a valid API key for one tenant to access data			
VE-2023-30993	urity	from another tenant's account. IBM X-Force ID: 254136.	2023-06-27	7.5	High
	,	A vulnerability in the hardware-based SSL/TLS cryptography			
		functionality of Cisco Adaptive Security Appliance (ASA) Software			
		and Cisco Firepower Threat Defense (FTD) Software for Cisco			
		Firepower 2100 Series Appliances could allow an unauthenticated, remote attacker to cause an affected device to reload			
		unexpectedly, resulting in a denial of service (DoS) condition. This			
		vulnerability is due to an implementation error within the			
		cryptographic functions for SSL/TLS traffic processing when they			
		are offloaded to the hardware. An attacker could exploit this			
		vulnerability by sending a crafted stream of SSL/TLS traffic to an			
	cisco - multiple	affected device. A successful exploit could allow the attacker to cause an unexpected error in the hardware-based cryptography			
CVE-2023-20006	products	engine, which could cause the device to reload.	2023-06-28	7.5	High
	'	In xmlParseTryOrFinish of parser.c, there is a possible out of			
		bounds read due to a heap buffer overflow. This could lead to			
		remote information disclosure with no additional execution			
		privileges needed. User interaction is not needed for			
VE-2023-21180	google - android	exploitation.Product: AndroidVersions: Android-13Android ID: A-261365944	2023-06-28	7.5	High
<u> </u>	Boogle - allululu	In LogResponse of Dns.cpp, there is a possible out of bounds read	2023-00-20	د. ۱	ı ııgı
		due to a missing bounds check. This could lead to remote denial of			
		service with no additional execution privileges needed. User			
	_	interaction is not needed for exploitation.Product:	_		
:VE-2023-21186	google - android	AndroidVersions: Android-13Android ID: A-261079188	2023-06-28	7.5	High
		In VideoFrame of VideoFrame.h, there is a possible abort due to an integer overflow. This could lead to remote information disclosure			
		with no additional execution privileges needed. User interaction is			
		not needed for exploitation.Product: AndroidVersions: Android-			
CVE-2023-21193	google - android	13Android ID: A-233006499	2023-06-28	7.5	High
VE-2023-21193	google - android	13Android ID: A-233006499 In btm_acl_process_sca_cmpl_pkt of btm_acl.cc, there is a possible out of bounds read due to an incorrect bounds check. This	2023-06-28	7.5	High

		execution privileges needed. User interaction is not needed for			
		exploitation.Product: AndroidVersions: Android-13Android ID: A-251427561			
CVE-2023-21201	google - android	In on_create_record_event of btif_sdp_server.cc, there is a possible out of bounds read due to a missing null check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-263545186	2023-06-28	7.5	High
<u>CVL*2023*21201</u>	google - anuroid	there is a possible use of unencrypted transport over cellular networks due to an insecure default value. 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:	2023-00-28	7.5	111811
CVE-2023-21219	google - android	A-264698379References: N/A	2023-06-28	7.5	High
		there is a possible use of unencrypted transport over cellular networks due to an insecure default value. 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:			
CVE-2023-21220	google - android	A-264590585References: N/A In LPP_ConvertGNSS_DataBitAssistance of LPP_CommonUtil.c,	2023-06-28	7.5	High
		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: Android Versions: Android			
CVE-2023-21223	google - android	kernelAndroid ID: A-256047000References: N/A In ss_ProcessReturnResultComponent of	2023-06-28	7.5	High
		ss_MmConManagement.c, there is a possible out of bounds read due to a heap buffer overflow. 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-			
CVE-2023-21224	google - android	265276966References: N/A In SAEMM_RetrieveTaiList of SAEMM_ContextManagement.c,	2023-06-28	7.5	High
CVE-2023-21226	google android	there is a possible out of bounds read due to an incorrect 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-240728187References: N/A	2023-06-28	7.5	∐igh.
CVE-2023-21220	google - android microsoft -	Microsoft Edge (Chromium-based) Elevation of Privilege	2023-00-26	7.5	High
CVE-2022-29144	edge_chromium	Vulnerability A flaw null pointer dereference in the Linux kernel DECnet networking protocol was found. A remote user could use this flaw	2023-06-29	7.5	High
CVE-2023-3338	linux - linux_kernel	to crash the system. In startLockTaskMode of LockTaskController.java, there is a	2023-06-30	7.5	High
		possible bypass of lock task mode 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 needed for			
CVE 2022 21180	google android	exploitation.Product: AndroidVersions: Android-13Android ID: A-	2022 06 29	7.2	High
CVE-2023-21189	google - android lenovo -	213942596 A valid, authenticated LXCA user with elevated privileges may be	2023-06-28	7.3	High
CVE-2023-34420	xclarity_administrat or	able to execute command injections through crafted calls to a specific web API.	2023-06-26	7.2	High
	veritas - multiple	In Veritas NetBackup Appliance before 4.1.0.1 MR3, insecure permissions may allow an authenticated Admin to bypass shell restrictions and execute arbitrary operating system commands via			
CVE-2023-37237	products	SSH. A Time-of-Check Time-Of-Use vulnerability in the Trend Micro Apex One and Apex One as a Service agent could allow a local	2023-06-29	7.2	High
		attacker to escalate privileges on affected installations. Please note: a local attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.			
	trendmicro -				
CVE-2023-32554	multiple products	This is similar to, but not identical to CVE-2023-32555. A Time-of-Check Time-Of-Use vulnerability in the Trend Micro Apex One and Apex One as a Service agent could allow a local attacker to escalate privileges on affected installations.	2023-06-26	7	High
CVE-2023-32555	trendmicro - multiple products	Please note: a local attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this	2023-06-26	7	High

		vulnerability.			
		This is similar to, but not identical to CVE-2023-32554.			
		A time-of-check to time-of-use issue exists in io_uring subsystem's			
		IORING_OP_CLOSE operation in the Linux kernel's versions 5.6 - 5.11 (inclusive), which allows a local user to elevate their privileges			
		to root. Introduced in			
		b5dba59e0cf7e2cc4d3b3b1ac5fe81ddf21959eb, patched in			
CVE-2023-1295	linux - linux_kernel	9eac1904d3364254d622bf2c771c4f85cd435fc2, backported to stable in 788d0824269bef539fe31a785b1517882eafed93.	2023-06-28	7	High
	_	Improper privilege management vulnerability in CC Mode prior to			
	samsung - multiple	SMR Jun-2023 Release 1 allows physical attackers to manipulate device to operate in way that results in unexpected behavior in CC			
CVE-2023-21513	products	Mode under specific condition.	2023-06-28	6.8	Mediur
	lenovo - thinkpad_e14_firm	A potential vulnerability in the LenovoFlashDeviceInterface SMI handler may allow an attacker with local access and elevated			
CVE-2023-2290	ware	privileges to execute arbitrary code.	2023-06-26	6.7	Mediur
		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 needed for			
		exploitation.Product: AndroidVersions: Android kernelAndroid ID:			
CVE-2023-21146	google - android	A-239867994References: N/A In the Google BMS kernel module, there is a possible out of	2023-06-28	6.7	Mediur
		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-			
CVE-2023-21151	google - android	265149414References: N/A In Do_AIMS_SET_CALL_WAITING of imsservice.cpp, there is a	2023-06-28	6.7	Mediur
		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: AndroidVersions: Android kernelAndroid ID:			
CVE-2023-21153	google - android	A-264259730References: N/A	2023-06-28	6.7	Mediur
		In encode of wlandata.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-			
CVE-2023-21157	google - android	263783137References: N/A	2023-06-28	6.7	Mediun
		In Parse of simdata.cpp, 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:			
CVE-2023-21159	google - android	AndroidVersions: Android kernelAndroid ID: A- 263783565References: N/A	2023-06-28	6.7	Mediur
	google america	In Parse of simdata.cpp, 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:			
CVE-2023-21161	google - android	AndroidVersions: Android kernelAndroid ID: A-263783702References: N/A	2023-06-28	6.7	Mediur
CVE-2023-21101	google - allulolu	In verifyInputEvent of InputDispatcher.cpp, there is a possible way	2023-00-26	0.7	iviedidi
		to conduct click fraud due to side channel information disclosure.			
		This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for			
CVE 2022 24474		exploitation.Product: AndroidVersions: Android-13Android ID: A-	2022 06 20	6.7	
CVE-2023-21171	google - android	261085213 In startWpsPbcInternal of sta_iface.cpp, there is a possible out of	2023-06-28	6.7	Mediur
		bounds read 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:			
CVE-2023-21203	google - android	AndroidVersions: Android-13Android ID: A-262246082	2023-06-28	6.7	Mediur
		In initiateTdlsSetupInternal of sta_iface.cpp, 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:			
CVE-2023-21207	google - android	AndroidVersions: Android-13Android ID: A-262236670 In multiple functions of sta_iface.cpp, there is a possible out of	2023-06-28	6.7	Mediur
		bounds read due to unsafe deserialization. This could lead to local			
		escalation of privilege with System execution privileges needed.			
CVE-2023-21209	google - android	User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236273	2023-06-28	6.7	Mediun
		In load_dt_data of storage.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.			
CVE-2023-21222	google - android	User interaction is not needed for exploitation.Product:	2023-06-28	6.7	Mediun

		AndroidVersions: Android kernelAndroid ID: A-			<u> </u>
		266977723References: N/A			
CVE-2023-21236	google - android	In aoc_service_set_read_blocked of aoc.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 kernelAndroid ID: A-270148537References: N/A	2023-06-28	6.7	Medium
		A vulnerability in Cisco Duo Two-Factor Authentication for macOS could allow an authenticated, physical attacker to bypass secondary authentication and access an affected macOS device. This vulnerability is due to the incorrect handling of responses from Cisco Duo when the application is configured to fail open. An attacker with primary user credentials could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the affected			
CVE-2023-20199	cisco - duo lenovo -	device without valid permission. A valid, authenticated LXCA user with elevated privileges may be	2023-06-28	6.6	Medium
CVE-2023-34421	xclarity_administrat or	able to replace filesystem data through a specifically crafted web API call due to insufficient input validation.	2023-06-26	6.5	Medium
CVE-2023-34422	lenovo - xclarity_administrat or	A valid, authenticated LXCA user with elevated privileges may be able to delete folders in the LXCA filesystem through a specifically crafted web API call due to insufficient input validation. Trend Micro Mobile Security (Enterprise) 9.8 SP5 contains widget	2023-06-26	6.5	Medium
		vulnerabilities that could allow a remote attacker to create arbitrary files on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.			
CVE-2023-32525	trendmicro - mobile_security	This is similar to, but not identical to CVE-2023-32526.	2023-06-26	6.5	Medium
		vulnerabilities that could allow a remote attacker to create arbitrary files on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.			
CVE-2023-32526	trendmicro - mobile_security proofpoint - insider_threat_man	This is similar to, but not identical to CVE-2023-32525. A missing authorization check in the MacOS agent configuration endpoint of the Insider Threat Management Server enables an anonymous attacker on an adjacent network to obtain sensitive information. Successful exploitation requires an attacker to first obtain a valid agent authentication token. All versions before	2023-06-26	6.5	Mediun
CVE-2023-36000	agement_server	7.14.3 are affected.	2023-06-27	6.5	Medium
CVE-2022-34352	ibm - multiple products	IBM QRadar SIEM 7.5.0 is vulnerable to information exposure allowing a delegated Admin tenant user with a specific domain security profile assigned to see data from other domains. IBM X-Force ID: 230403.	2023-06-27	6.5	Medium
	cisco - telepresence_video _communication_s	Multiple vulnerabilities in Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated attacker with Administrator-level read-only credentials to elevate their privileges to Administrator with read- write credentials on an affected system. Note: "Cisco Expressway Series" refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. For more information about these vulnerabilities, see the Details section of	2020 02 5		
CVE-2023-20105	erver	this advisory. A vulnerability in the OpenAPI of Cisco Secure Workload could allow an authenticated, remote attacker with the privileges of a read-only user to execute operations that should require Administrator privileges. The attacker would need valid user credentials. This vulnerability is due to improper role-based access control (RBAC) of certain OpenAPI operations. An attacker could exploit this vulnerability by issuing a crafted OpenAPI function call with valid credentials. A successful exploit could allow the attacker	2023-06-28	6.5	Medium
CVE-2023-20136	secure_workload	to execute OpenAPI operations that are reserved for the	2023-06-28	6.5	Medium

	T	Administrator usor including the greation and deletion of usor			
CVE 2022 2002	lenovo - nextscale_n1200_e	Administrator user, including the creation and deletion of user labels. A valid, authenticated user with limited privileges may be able to use specifically crafted web management server API calls to execute a limited number of commands on SMM v1, SMM v2, and FPC that the user does not normally have sufficient privileges to	2022 06 26	6.2	Modium
CVE-2023-2993	nclosure_firmware	execute.	2023-06-26	6.3	Medium
		Certain dashboard widgets on Trend Micro Apex Central (on- premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers.			
CVE-2023-32531	trendmicro - apex_central	This is similar to, but not identical to CVE-2023-32532 through 32535.	2023-06-26	6.1	Medium
		Certain dashboard widgets on Trend Micro Apex Central (on- premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers.			
CVE-2023-32532	trendmicro - apex_central	This is similar to, but not identical to CVE-2023-32531 through 32535. Certain dashboard widgets on Trend Micro Apex Central (onpremise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers.	2023-06-26	6.1	Medium
CVE-2023-32533	trendmicro - apex_central	This is similar to, but not identical to CVE-2023-32531 through 32535.	2023-06-26	6.1	Medium
CVE-2023-32534	trendmicro - apex_central	Certain dashboard widgets on Trend Micro Apex Central (onpremise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. This is similar to, but not identical to CVE-2023-32531 through 32535.	2023-06-26	6.1	Medium
CVL-2023-32334	арех_сеппа	Certain dashboard widgets on Trend Micro Apex Central (on- premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers.	2023-00-20	0.1	Wedum
CVE-2023-32535	trendmicro - apex_central	This is similar to, but not identical to CVE-2023-32531 through 32534. IBM Business Automation Workflow is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended	2023-06-26	6.1	Medium
CVE-2023-32339	ibm - multiple products	functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 255587. Multiple vulnerabilities in the web-based management interface of	2023-06-27	6.1	Medium
	cisco - multiple	Cisco AsyncOS Software for Cisco Secure Email and Web Manager; Cisco Secure Email Gateway, formerly Cisco Email Security Appliance (ESA); and Cisco Secure Web Appliance, formerly Cisco Web Security Appliance (WSA), could allow a remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. For more information about these vulnerabilities, see			
CVE-2023-20119	products	the Details section of this advisory. Multiple vulnerabilities in the web-based management interface of	2023-06-28	6.1	Medium
	oices muchining	Cisco AsyncOS Software for Cisco Secure Email and Web Manager; Cisco Secure Email Gateway, formerly Cisco Email Security Appliance (ESA); and Cisco Secure Web Appliance, formerly Cisco Web Security Appliance (WSA), could allow a remote attacker to conduct a cross-site scripting (XSS) attack against a user of the			
CVE-2023-20120	cisco - multiple products	interface. For more information about these vulnerabilities, see the Details section of this advisory.	2023-06-28	6.1	Medium
	cisco - multiple	A vulnerability in the Administrative XML Web Service (AXL) API of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.			
CVE-2023-20116	products	This vulnerability is due to insufficient validation of user-supplied	2023-06-28	5.7	Medium

		input to the web UI of the Self Care Portal. An attacker could			
		exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow the attacker to cause a DoS condition on the affected device.			
		end_pattern (called from internal_fnmatch) in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent			
		attackers to cause a denial of service (application crash), as demonstrated by use of the fnmatch library function with the **(!() pattern. NOTE: this is not the same as CVE-2015-8984; also,			
CVE-2015-20109	gnu - glibc	some Linux distributions have fixed CVE-2015-8984 but have not fixed this additional fnmatch issue.	2023-06-25	5.5	Medium
	trendmicro -	A privilege escalation vulnerability in the Trend Micro Apex One and Apex One as a Service agent could allow a local attacker to unintentionally delete privileged Trend Micro registry keys			
CVE-2023-30902	multiple products	including its own protected registry keys on affected installations. A link following vulnerability in the Trend Micro Apex One and Apex One as a Service agent could allow a local attacker to disclose	2023-06-26	5.5	Medium
		sensitive information.			
	trendmicro -	Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this			
CVE-2023-32556	multiple products	vulnerability.	2023-06-26	5.5	Medium
	proofpoint -	An insecure filesystem permission in the Insider Threat Management Agent for Windows enables local unprivileged users			
01/5 2022 2233	insider_threat_man	to disrupt agent monitoring. All versions prior to 7.14.3 are	2022 22 ==		
CVE-2023-2818	agement	affected. Agents for MacOS and Linux and Cloud are unaffected. IBM Robotic Process Automation for Cloud Pak 21.0.1 through	2023-06-27	5.5	Medium
		21.0.7.3 and 23.0.0 through 23.0.3 is vulnerable to insufficient			
CVE-2023-23468	ibm - multiple products	security configuration which may allow creation of namespaces within a cluster. IBM X-Force ID: 244500.	2023-06-27	5.5	Medium
<u>CVE 2023 23 100</u>	products	This issue was addressed with improved data protection. This issue	2023 00 27	3.3	Wicarain
CVE-2022-48505	annia macas	is fixed in macOS Ventura 13. An app may be able to modify protected parts of the file system	2023-06-28	5.5	Medium
CVE-2022-48303	apple - macos	In FaceStatsAnalyzer::InterpolateWeightList of	2023-00-28	5.5	Medium
		face_stats_analyzer.cc, there is a possible out of bounds read due			
		to a missing bounds check. This could lead to local information disclosure with User execution privileges needed. User interaction			
		is not needed for exploitation.Product: AndroidVersions: Android			
CVE-2023-21152	google - android	kernelAndroid ID: A-269174022References: N/A In BuildSetRadioNode of protocolmiscbuilder.cpp, there is a	2023-06-28	5.5	Medium
		possible out of bounds read due to a missing null check. This could			
		lead to local information disclosure with no additional execution			
		privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID:			
CVE-2023-21155	google - android	A-264540700References: N/A	2023-06-28	5.5	Medium
		In BuildSetTcsFci of protocolmiscbuilder.cpp, 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			
CVE-2023-21160	google - android	exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-263784118References: N/A	2023-06-28	5.5	Medium
		In setProfileName of DevicePolicyManagerService.java, there is a			
		possible way to crash the SystemUI menu due to a missing bounds check. This could lead to local denial of service with no additional			
		execution privileges needed. User interaction is not needed for			
CVE 2022 24467	and and and	exploitation.Product: AndroidVersions: Android-13Android ID: A-	2022 06 20		NA o diviso
CVE-2023-21167	google - android	259942964 In convertCbYCrY of ColorConverter.cpp, there is a possible out of	2023-06-28	5.5	Medium
		bounds read due to a missing bounds check. This could lead to			
		local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product:			
CVE-2023-21168	google - android	AndroidVersions: Android-13Android ID: A-253270285	2023-06-28	5.5	Medium
		In multiple methods of DataUsageList.java, there is a possible way			
		to learn about admin user's network activities due to a missing permission check. This could lead to local information disclosure			
		with no additional execution privileges needed. User interaction is			
CVE-2023-21173	google - android	not needed for exploitation.Product: AndroidVersions: Android- 13Android ID: A-262741858	2023-06-28	5.5	Medium
OAF 5052-51112	800gic · anaroid	In requestAppKeyboardShortcuts of WindowManagerService.java,	2023 00-20	ر. ح	iviculant
		there is a possible way to infer the app a user is interacting with			
		due to a missing permission check. This could lead to local information disclosure with no additional execution privileges			
		needed. User interaction is not needed for exploitation.Product:			
CVE-2023-21177	google - android	AndroidVersions: Android-13Android ID: A-273906410	2023-06-28	5.5	Medium
		In remove_sdp_record of btif_sdp_server.cc, there is a possible out of bounds read due to a missing bounds check. This could lead			
CVE-2023-21198	google - android	to local information disclosure with no additional execution	2023-06-28	5.5	Medium

In startWpsPhiDisplayInternal of Sta, Jaface.pp, there is a possible out of bounds read due to unsafe describtation. This could lead to local Information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13Android ID: A. 262245376 Z. 2023-06-28 S. 5. Medi in multiple files, 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-13Android ID: A-262235998 Z. 2023-06-28 S. 5. Medi in application in some needed for exploitation Product: Android Versions: Android-13Android ID: A-262235998 Z. 2023-06-28 S. 5. Medi in application in the control of exploitation Product: Android Versions: Android-13Android ID: A-262235998 Z. 2023-06-28 S. 5. Medi in application in the control of exploitation in the control of exploitation in the control of the control o			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-			
possible out of bounds read due to improper input validation. 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. 2023-06-28 5.5 Medi of bounds read due to unsafe describitation. 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. 2023-06-28 5.5 Medi of bounds read due to unsafe describitation. 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. 2023-06-28 5.5 Medi of the products with no additional execution privileges needed. User interaction is not needed for exploitation Product. Android/Versions: Android-13-Android ID: A. 25125998 1.0 Android/Versions: Android-13-Android ID: A. 25125998 1.0 Android/Versions: Android-13-Android ID: A. 25125999 2.0 2023-06-28 5.5 Medi in apphylamorete/leve of Notification Contentinifiates gave, there is a possible way to hide foregonal service notification due to a discourse with no additional execution privileges needed. User interaction is not needed for exploitation Product. VE-2023-21237 google - android Iniux - multiple iniux - multiple products of the version of the products of the return value of knalloci). This is sue allows a local user to crash the system. A NULL pointer dereference flaw was found in the Linux kernel's interaction is not needed for exploitation Product. VE-2023-3359 products can be producted to the system. A null pointer dereference flaw was found in the Linux kernel's hord of the return value of knalloci). This is sue allows a local user to crash the system. A null pointer dereference flaw was found in the Linux kernel's integrated Sensor Hub (ISH) driver. This liss allows a local user to crash the system. A nul						
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 2023-06-28 5.5 Medi to InstartWpsPinDisplayIntermal of stal_Hace.cpp, there is a possible out of brunds read due to unsafe deservilation. 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 2023-06-28 5.5 Medi multiple files flee 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: VE 2023-21221 google - android AndroidVersions: Android-13Android ID: A 2023-06-28 5.5 Medi in applicamental very interaction is not needed for exploitation privileges needed. User interaction is not needed for exploitation privileges needed. User interaction is not needed for exploitation privileges needed. User interaction is not needed for exploitation product: VE 2023-21221 google - android AndroidVersions: Android-13Android ID: A 2023-06-28 5.5 Medi in applicamental very interaction is not needed for exploitation products: VE 2023-21222 google - android AndroidVersions: Android-13Android ID: A 2023-06-28 5.5 Medi interaction is not needed for exploitation products: VE 2023-21223 google - android AndroidVersions: Android-13Android ID: A 2023-06-28 5.5 Medi interaction is not needed for exploitation products: VE 2023-21224 google - android AndroidVersions: Android-13Android ID: A 2023-06-28 5.5 Medi interaction is not needed for exploitation products: VE 2023-3355 products Inux - multiple products Inux - m						
cyt-2023-21200 google - android In startWpsPhiDisplayInternal of sta_lface.cop. there is a possible out of bounds read due to unsate describitation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product. Android/Versions: Android-13Android ID-A-262245376 In multiple files, 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 products and 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 products. Cyt-2023-21211 google - android Cyt-2023-21221 google - android Cyt-2023-21222 google - android In appNermete/wew for Notification Contentifiater plays, there is a possible way to hide foreground service notification due to misleading or insufficient Link Scould lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation Product: Cyt-2023-21227 google - android Innux - multiple Cyt-2023-3355 groducts Innux - multiple Cyt-2023-3355 groducts Innux - multiple Cyt-2023-3359 groducts Innux - multiple						
CVE-2023-21209 google - android 2, 26588764 in multiple files, there is a possible out of bounds read due to unsafe description. This could lead to local information disclosure with no additional execution privileges neceded. User interaction is not needed for exploitation Product: Android/Versions: Android-13-android ID-A-2023-06-28 5.5 Medi disclosure with no additional execution privileges neceded. User interaction is not needed for exploitation Product: Android-12-3-235998						
In startWpsPhiDisplayInternal of sta_face.opp, there is a possible out of bounds read due to unsafe describilation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Protection of the country of the products and read of the country of the co			· ·			
out of bounds read due to unsafe deserialization. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Annirol/VEX.2023-21205 google - android	CVE-2023-21200	google - android		2023-06-28	5.5	Medium
to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android-13Android ID: A-25225376 2023-06-28 5.5 Medi in multiple files, 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-13Android ID: A-25225398 2023-06-28 5.5 Medi in applyRemotevileve of Notification. Contentinifater javo, there is a possible way to hide foreground service notification due to misleading or insufficient UI. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android-13Android ID: A-25225398 2023-06-28 5.5 Medi interaction is not needed for exploitation. Product: Interaction is not needed for exploitation. Product: Android/Versions: Android-13Android ID: A-25225369812 2023-06-28 5.5 Medi interaction is not needed for exploitation. Product: Android/Versions: Android-13Android ID: A-25225369812 2023-06-28 5.5 Medi interaction is not needed for exploitation. Product: Android/Versions: Android-13Android ID: A-25225369812 2023-06-28 5.5 Medi interaction is not needed for exploitation. Product: Android/Versions: Android-13Android ID: A-25225369812 2023-06-28 5.5 Medi interaction is not needed for exploitation. Product: Android/Versions: Android-13Android ID: A-25225369812 2023-06-28 5.5 Medi interaction is not needed for exploitation. Product: Android/Versions: Android-13Android ID: A-25225369812 2023-06-28 5.5 Medi interaction is not needed for exploitation. Product: Android-Version-13Android ID: A-25225369812 2023-06-28 5.5 Medi interaction						
privileges needed. User interaction is not needed for exploitation Product: Analorid Versions: Anioridol-33 Android ID: A- 2023-06-28 5.5 Medi In multiple files, 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:						
Section Sect						
In multiple files, 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. Products 2023-06-28 5.5 Media			·			
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-13Android ID: A-262235998 2023-06-28 5.5 Medi In applyRemoteView of Notification.Contentinflater.java, there is a possible way to hide foreground service notification due to misleading or insufficient UI. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android-13Android ID: A-25136912 2023-06-28 5.5 Medi Inux - multiple products Inux - multiple Inux - multiple products Inux - multiple Inux - mu	CVE-2023-21205	google - android		2023-06-28	5.5	Medium
disclosure with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-13Android ID: A-262235998 In applyRemoteView of NotificationContentinifater.java, there is a possible way to hide foreground service notification due to misleading or insufficient UI. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: ANULL pointer dereference flaw was found in the Linux kernel's drivers/gpu/fam/msm.gem.submit.c code in the submit. Lookup_cmds function, which fails because it lacks a check of the return value of kmalloc(). This issue allows a local user to crash the system. A NULL pointer dereference flaw was found in the Linux kernel's drivers/gpu/fam/msm.gem.submit.c code in the submit. Lookup_cmds function, which fails because it lacks a check of the return value of kmalloc(). This issue allows a local user to crash the system. A NULL pointer dereference flaw was found in the Linux kernel CVE-2023-3355 Products A NULL pointer dereference was found in the Linux kernel's integrated Sensor Hub (fiver). This flaw allows a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Hub (fiver). In the products integrated Sensor Hub (fiver). In the products integrated Sensor Hub (fiver). In the products integrated Sensor Hub (fiver). In the Linux kernel brom. parse in drivers/nomem/brom. provam.c. Lacks for the check of the return value of kalloc() can cause the NULL Pointer Dereference. Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Affected versions Trend						
interaction is not needed for exploitation.Product: An image			· ·			
Section			, -			
possible way to hide foreground service notification due to misleading or insufficient UI. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: A NULL pointer dereference flaw was found in the Linux kernel's drivers/gpu/drm/msm/msm_gem_submit. 2006 in the submit. Jookup. cmds function, which fails because it lacks a check of the return value of kmalloc(). This issue allows a local user to crash the system. A NULL pointer dereference flaw was found in the Linux kernel with the submit. Jookup. cmds function, which fails because it lacks a check of the return value of kmalloc(). This issue allows a local user to crash the system. A NULL pointer dereference flaw was found in the Linux kernel with the system. A NULL pointer dereference flaw was found in the Linux kernel with the system. A NULL pointer dereference flaw was found in the Linux kernel with the system. A NULL pointer dereference flaw was found in the Linux kernel with the system. A NULL pointer dereference flaw was found in the Linux kernel with the system. A NULL pointer dereference flaw was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A NULL pointer dereference was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A Insurance of the dereference was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A Insurance of the dereference was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A Null pointer dereference was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A Null pointer dereference was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local use	CVE-2023-21211	google - android	·	2023-06-28	5.5	Medium
misleading or insufficient UI. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android-13Android ID: A-251586912 2023-06-28 5.5 Medi ANUL pointer dereference flaw was found in the Linux kernel's drivers/gpu/drm/msm/msm_gem_submit.code in the submit_lookup_cmds function, which fails because it lacks a check of the return value of kmalloc(). This issue allows a local user to crash the system. ANUL pointer dereference flaw was found in the Linux kernel and products products and the very street of the return value of kmalloc(). This flaw allows a local user to crash the system. ANUL pointer dereference flaw was found in the Linux kernel and products products and the very street of the return value of kmalloc(). This flaw allows a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Flub (ISFI) driver. This flaw allows a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Flub (ISFI) driver. This issue could allow a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Flub (ISFI) driver. This issue could allow a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Flub (ISFI) driver. This flaw allows a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Flub (ISFI) driver. This flaw allows a local user to crash the system of the system can be sent to crash the system of the syste			In applyRemoteView of NotificationContentInflater.java, there is a			
disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: A NULL pointer dereference flaw was found in the Linux kernel's driver/sgpu/drm/smm/smm/smm/smm/smm/smm/smm/smm/smm/s			'			
interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-251586912 ANULI pointer dereference flaw was found in the Linux kernel's drivers/gpu/drm/msm/msm_gem_submit.c code in the bubmit_lookup_cmds function, which fails because it lacks a check of the return value of kmalloc(). This issue allows a local user to crash the system. ANULI pointer dereference flaw was found in the Linux kernel linux - multiple products products products ANULI pointer dereference flaw was found in the Linux kernel AMD Sensor Fusion Hub driver. This flaw allows a local user to crash the system. A null pointer dereference was found in the Linux kernel's linux - multiple products products products An ull pointer dereference was found in the Linux kernel's linux - multiple products products An ull pointer dereference was found in the Linux kernel's linux - multiple products An ull pointer dereference was found in the Linux kernel's linux - multiple products An issue was discovered in the Linux kernel brcm_nvram_parse in were vulnersely was discovered in the Linux kernel brcm_nvram_parse in value of kzalloc() can cause the NULL Pointer Dereference. Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. Trendmicro - apex_central Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. Trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. Trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. Trend						
Android/versions: Android-13Android ID: A-251586912 2023-06-28 5.5 Medi A NULL pointer dereference flaw was found in the Linux kernel's drivers/gpu/drm/msm/msm_gem_submitc. code in the submit Lookup_cmds function, which fails because it lacks a check of the return value of kmalloc(). This issue allows a local user to crash the system. A NULL pointer dereference flaw was found in the Linux kernel A NULL pointer dereference flaw was found in the Linux kernel I inux - multiple products I inux - multiple products A NULL pointer dereference flaw was found in the Linux kernel A NULL pointer dereference was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This flaw allows a local user to crash the system. A null pointer dereference was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A nisue was discovered in the Linux kernel's Integrated Sensor Hub (ISH) driver. This flaw allows a local user to crash the system. A nisue was discovered in the Linux kernel's Integrated Sensor Hub (ISH) driver. This flaw allows a local user to crash the system. A nisue was discovered in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A flax to expect the flax to expect the return value of kaalloc() can cause the NULL Pointer Dereference. A flax to expect the system in order to exploit this vulnerability. A flax to expect the system in order to exploit this vulnerability. Trendmicro apex central on the target system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32537. A pex central on the target system in order to exploit this vulnerability.						
A NULL pointer dereference flaw was found in the Linux kernel's drivers/gpu/drm/msm/msm_gem_submit.c code in the bubmit_lookup cmds function, which falls because it lacks a check of the return value of kmalloc(). This issue allows a local user to crash the system. A NULL pointer dereference flaw was found in the Linux kernel linux - multiple products Products A NULL pointer dereference flaw was found in the Linux kernel AMD Sensor Fusion Hub driver. This flaw allows a local user to crash the system. A null pointer dereference was found in the Linux kernel's linux - multiple products Products A null pointer dereference was found in the Linux kernel's linux - multiple products A null pointer dereference was found in the Linux kernel's linux - multiple products A null pointer dereference was found in the Linux kernel's linux - multiple products A null pointer dereference was found in the Linux kernel's linux - multiple products A null pointer dereference was found in the Linux kernel's linux was discovered in the Linux kernel's linux - multiple products A null pointer dereference was found in the Linux kernel's linux was discovered in the Linux kernel's linux - multiple products A null pointer dereference was found in the Linux kernel's linux was discovered in the Linux kernel's linux was discovered in the Linux kernel brcm_nvram_parse in drivers/nvmem/brcm_nvram.c. Lacks for the check of the return value of kzalloc() can cause the NULL Pointer Dereference. Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user inp	CVF_2023_21237	google - android	·	2023-06-28	5.5	Medium
drivers/gpu/drm/msm/msm_gem_submit.code in the submit_lookup_cmds function, which falls because it lacks a check of the return value of kmalloci). This issue allows a local user to crash the system. A NULL pointed dereference flaw was found in the Linux kernel AMD Sensor Fusion Hub driver. This flaw allows a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A null pointer dereference was found in the Linux kernel's integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A null pointer dere	CVL-2023-21237	google - android		2023-00-28	5.5	Wiediaiii
Submit_lookup_cmds function, which fails because it lacks a check of the return value of kmalloc(). This issue allows a local user to crash the system. 2023-06-28 5.5 Medi			· ·			
linux - multiple products A NULL pointer dereference flaw was found in the Linux kernel AND Sensor Fusion Hub driver. This flaw allows a local user to crash the system. A null pointer dereference flaw was found in the Linux kernel AND Sensor Fusion Hub driver. This flaw allows a local user to crash the system. A null pointer dereference was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A null pointer dereference was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. A nissue was discovered in the Linux kernel brcm_nvram_parse in drivers/nvmem/brcm_nvram.c. Lacks for the check of the return value of kzalloc() can cause the NULL Pointer Dereference. 2023-06-28 5.5 Medi A ffected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. CVE-2023-32537 apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi CVE-2023-32537 Apex_central						
CVE-2023-3357		linux - multiple				
Ilinux - multiple products AMD Sensor Fusion Hub driver. This flaw allows a local user to crash the system. 2023-06-28 5.5 Medi	CVE-2023-3355	products	,	2023-06-28	5.5	Medium
CVE-2023-3357 products crash the system. A null pointer dereference was found in the Linux kernel's linux - multiple products user to crash the system. A null pointer dereference was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. An issue was discovered in the Linux kernel brcm_nvram_parse in drivers/nymem/brcm_nvram_parse in drivers/nymem/brcm_nvram_charse in drivers/nymem/brcm_nvram_charse in drivers/nymem/brcm_nvram_charse in drivers/nymem/brcm_nvram_charse in drivers/nymem/brcm_nvram_charse in drivers/nymem/brcm_nvram_charse in drivers/nymem/brcm_nvram_parse in drivers/nymem/brcm_nvram_charse in drivers/nymem/brcm_nvram_parse in drivers/nymem/brcm_nvram_charse in drivers/nymem/brcm_nvram_charse in drivers/nymem/brcm_nvram_charse in drivers/nymem/brcm_nvram_charse in drivers/nymem/brcm_nvram_parse in drivers/nymem/brcm_nvram_charse in			·			
A null pointer dereference was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. An issue was discovered in the Linux kernel brcm_nvram_parse in drivers/nvmem/brcm_nvram_c. Lacks for the check of the return value of kzalloc() can cause the NULL Pointer Dereference. Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32537. Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32536. This is similar to, but not identical to CVE-2023-32536. An Its good and the control of th	CVE 2022 22E7	•		2022 06 28		Madium
Inix - multiple products Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system. 2023-06-28 5.5 Medi	CVE-2023-3357	products	•	2023-06-28	5.5	iviedium
CVE-2023-3358 products user to crash the system. 2023-06-28 5.5 Medi		linux - multiple	·			
An issue was discovered in the Linux kernel brcm_nvram_parse in drivers/nvmem/brcm_nvram.c. Lacks for the check of the return value of kzalloc() can cause the NULL Pointer Dereference. Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32537. 2023-06-26 5.4 Medi Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32537. 2023-06-26 5.4 Medi vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability.	CVE-2023-3358	·		2023-06-28	5.5	Medium
CVE-2023-3359 products value of kzalloc() can cause the NULL Pointer Dereference. 2023-06-28 5.5 Medi		·	·			
Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi		•	_			
vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32537. Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi	CVE-2023-3359	products		2023-06-28	5.5	Medium
(XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi			· · · · · · · · · · · · · · · · · · ·			
Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32537. 2023-06-26 Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi			, , ,			
CVE-2023-32536 trendmicro - apex_central Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi CVE-2023-32537 This is similar to, but not identical to CVE-2023-32536.			(NSS) accounts due to discrimput validation and samuzation issues.			
CVE-2023-32536 trendmicro - apex_central Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi CVE-2023-32537 This is similar to, but not identical to CVE-2023-32536.						
CVE-2023-32536 trendmicro - apex_central Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi CVE-2023-32537 This is similar to, but not identical to CVE-2023-32536.						
trendmicro - apex_central This is similar to, but not identical to CVE-2023-32537. 2023-06-26 5.4 Medi Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi			·			
CVE-2023-32536 apex_central This is similar to, but not identical to CVE-2023-32537. 2023-06-26 5.4 Medi Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi			Central on the target system in order to exploit this vulnerability.			
CVE-2023-32536 apex_central This is similar to, but not identical to CVE-2023-32537. 2023-06-26 5.4 Medi Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi						
CVE-2023-32536 apex_central This is similar to, but not identical to CVE-2023-32537. 2023-06-26 5.4 Medi Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi		trendmicro -				
Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi	CVE-2023-32536		This is similar to, but not identical to CVE-2023-32537.	2023-06-26	5.4	Medium
vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi		1				20.0.11
Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi						
Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi			(XSS) attacks due to user input validation and sanitization issues.			
Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi						
Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi						
Central on the target system in order to exploit this vulnerability. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi			Please note: an attacker must first obtain authentication to Anex			
trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. trendmicro - apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi			·			
CVE-2023-32537 apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi			, , , , , , , , , , , , , , , , , , , ,			
<u>CVE-2023-32537</u> apex_central This is similar to, but not identical to CVE-2023-32536. 2023-06-26 5.4 Medi						
	CVE-2023-32537	apex_central		2023-06-26	5.4	Medium
Affected versions Trend Micro Apex Central (on-premise) are			, , , , ,			
vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues.						
(1.05) actacks and to aser input validation and samitzation issues.			(1.55) accused and to user input validation and samuzation issues.			
Please note: an attacker must first obtain authentication to Apex			·			
Central on the target system in order to exploit this vulnerability.			Central on the target system in order to exploit this vulnerability.			
trandmicro		trandmissa				
trendmicro - <u>CVE-2023-32604</u> apex_central This is similar to, but not identical to CVE-2023-32605. 2023-06-26 5.4 Medi	CVF-2023-32604		This is similar to but not identical to CVF-2023-32605	2023-06-26	5 /	Medium
Affected versions Trend Micro Apex Central (on-premise) are	312 2023 32004	арел_сепиа		_023 00 20	J. T	Medialii
trendmicro - vulnerable to potential authenticated reflected cross-site scripting			, , , ,			
CVE-2023-32605 apex_central (XSS) attacks due to user input validation and sanitization issues. 2023-06-26 5.4 Medi		trendmicro -	vulnerable to potential authenticated reflected cross-site scripting			l

		Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability.			
CVE-2023-26274 CVE-2023-20028 CVE-2021-34506	ibm - multiple products cisco - multiple products microsoft - edge_chromium	This is similar to, but not identical to CVE-2023-32604. IBM QRadar SIEM 7.5.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 248144. Multiple vulnerabilities in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager; Cisco Secure Email Gateway, formerly Cisco Email Security Appliance (ESA); and Cisco Secure Web Appliance, formerly Cisco Web Security Appliance (WSA), could allow a remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory. Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability An Improper access control vulnerability in Trend Micro Apex One and Apex One as a Service could allow an unauthenticated user	2023-06-27 2023-06-28 2023-07-01	5.4 5.4	Medium Medium Medium
CVE-2023-32552	trendmicro - multiple products	and Apex One as a Service could allow an unauthenticated user under certain circumstances to disclose sensitive information on agents. This is similar to, but not identical to CVE-2023-32553 An Improper access control vulnerability in Trend Micro Apex One and Apex One as a Service could allow an unauthenticated user under certain circumstances to disclose sensitive information on agents.	2023-06-26	5.3	Medium
CVE-2023-32553	trendmicro - multiple products	This is similar to, but not identical to CVE-2023-32552. In btm_acl_encrypt_change of btm_acl.cc, there is a possible way for a remote device to turn off encryption without resulting in a terminated connection due to an unusual root cause. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for	2023-06-26	5.3	Medium
CVE-2023-21190	google - android	exploitation.Product: AndroidVersions: Android-13Android ID: A-251436534	2023-06-28	5	Medium
	cisco - sf200-	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need to have valid credentials to access the web-based management interface of the affected device. Cisco has not released software updates to			
CVE-2023-20188	24_firmware	address this vulnerability. Reflected cross site scripting (XSS) vulnerability was discovered in	2023-06-28	4.8	Medium
CVE-2023-33336	sophos - web_appliance linux - multiple	Sophos Web Appliance v4.3.9.1 that allows for arbitrary code to be inputted via the double quotes. A flaw was found in the MCTP protocol in the Linux kernel. The function mctp_unregister() reclaims the device's relevant resource when a netcard detaches. However, a running routine may be unaware of this and cause the use-after-free of the mdev->addrs	2023-06-30	4.8	Medium
CVE-2023-3439	products microsoft -	object, potentially leading to a denial of service.	2023-06-28	4.7	Medium
CVE-2022-23264	edge_chromium proofpoint - insider_threat_man	Microsoft Edge (Chromium-based) Spoofing Vulnerability A missing authorization check in multiple SOAP endpoints of the Insider Threat Management Server enables an attacker on an adjacent network to read and write unauthorized objects.	2023-06-29	4.7	Medium
CVE-2023-35998	agement_server	Successful exploitation requires an attacker to first obtain a valid	2023-06-27	4.6	Medium

		agent authentication token. All versions before 7.14.3 are			
		affected.			
		In btm_ble_periodic_adv_sync_tx_rcvd of btm_ble_gap.cc, there is a possible out of bounds read due to an incorrect bounds check.			
		This could lead to local information disclosure over Bluetooth, if			
		the firmware were compromised with System execution privileges			
CVE 2022 2440E	l accele coducid	needed. User interaction is not needed for exploitation.Product:	2022 06 20	4.5	N 4 = ali
CVE-2023-21195	google - android	AndroidVersions: Android-13Android ID: A-233879420 In btm_delete_stored_link_key_complete of btm_devctl.cc, there	2023-06-28	4.5	Medium
		is a 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 needed for exploitation. Product: Android Versions: Android-			
CVE-2023-21202	google - android	13Android ID: A-260568359	2023-06-28	4.5	Medium
		In BuildSetConfig of protocolimsbuilder.cpp, there is a possible out			
		of bounds read due to a missing null check. This could lead to local			
		information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product:			
		AndroidVersions: Android kernelAndroid ID: A-			
CVE-2023-21148	google - android	263783657References: N/A	2023-06-28	4.4	Medium
		In handle_set_parameters_ctrl of hal_socket.c, 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			
CVE-2023-21150	google andreid	exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-267312009References: N/A	2023-06-28	4.4	Medium
CAT-5052-51120	google - android	In StoreAdbSerialNumber of protocolmiscbuilder.cpp, there is a	ZUZ3-UU-ZŎ	4.4	ivicululli
		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: AndroidVersions: Android kernelAndroid ID:			
CVE-2023-21154	google - android	A-263783910References: N/A	2023-06-28	4.4	Medium
		In BuildGetRadioNode of protocolmiscbulider.cpp, there is a			
		possible out of bounds read due to improper input validation. This could lead to local information disclosure from the modem with			
		System execution privileges needed. User interaction is not			
0.45 0000 04456		needed for exploitation.Product: AndroidVersions: Android			
CVE-2023-21156	google - android	kernelAndroid ID: A-264540759References: N/A In encode of miscdata.cpp, there is a possible out of bounds read	2023-06-28	4.4	Medium
		due to a heap buffer overflow. This could lead to local information			
		disclosure with System execution privileges needed. User			
		interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-			
CVE-2023-21158	google - android	263783635References: N/A	2023-06-28	4.4	Medium
		In inviteInternal 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 needed. User interaction is not needed for exploitation.Product:			
CVE-2023-21169	google - android	AndroidVersions: Android-13Android ID: A-274443441	2023-06-28	4.4	Medium
		In executeSetClientTarget of ComposerCommandEngine.h, 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			
CVE 2022 24172	and the second second	exploitation.Product: AndroidVersions: Android-13Android ID: A-	2022 06 22	4.4	N 4 = -1*
CVE-2023-21170	google - android	252764410 In list_key_entries of utils.rs, there is a possible way to disable user	2023-06-28	4.4	Medium
		credentials due to resource exhaustion. This could lead to local			
		denial of service with System execution privileges needed. User			
CVE-2023-21176	google - android	interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-222287335	2023-06-28	4.4	Medium
<u> </u>	Soogic analola	In btm_ble_update_inq_result of btm_ble_gap.cc, there is a	2023 00 20	ਾ. ਾ	iviculalii
		possible out of bounds read due to a heap buffer overflow. This			
		could lead to local information disclosure with System execution privileges needed. User interaction is not needed for			
		exploitation.Product: AndroidVersions: Android-13Android ID: A-			
CVE-2023-21181	google - android	264880969	2023-06-28	4.4	Medium
		In Exynos_parsing_user_data_registered_itu_t_t35 of			
		VendorVideoAPI.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:			
CVE-2023-21182	google - android	AndroidVersions: Android-13Android ID: A-252764175	2023-06-28	4.4	Medium
		In btm_ble_update_inq_result of btm_ble_gap.cc, there is a possible out of bounds read due to a heap buffer overflow. This			
		could lead to local information disclosure with System execution			
		privileges needed. User interaction is not needed for			
CVE-2023-21188	google - android	exploitation.Product: AndroidVersions: Android-13Android ID: A-264624283	2023-06-28	4.4	Medium
CAF 7072-51100	Boogic allululu	20 1027203	2023 00-20	7.7	IVICUIUIII

In signt_dig_c_p_name of jagl_upic_tance (in secular jack) and on the control of secular process of a missing bound research. This could lead to receive the process of the country of the		T				1
Social Information disclosure in the Bisectoth sever with System execution privilegal residue of exploitation in control in an artistic privilegal residue of the property of the privilegal residue o			In gatt_dbg_op_name of gatt_utils.cc, there is a possible out of			
execution privileges needed. User interaction is not seeded for proceedings of the process of th			_			
December 2003-21194 poogle - android December 2003-21196 patchiscan rich per is a possible out of bounds read due to missing bounds check. This could lead to local information disclosure in the Blustoche share with System securion privileges and an amising bounds check. This could lead to local information disclosure with System securion privileges and an amising bounds are all one of the period privileges and an amising bounds read due to a missing bound check. This could lead to be considered to be considered to the period privileges and the period			·			
in http://bib.phtchischam.phtm.ptd.phtchisch.ptd.phtchisch.ptd.phtchisch.ptd.phtchisch.ptd.phtchisch.ptd.phtchisch.ptd.phtchisch.ptd.phtchisch.ptd.phtchisch.ptd.phtchisch.ptd.phtchisch.ptd.ptd.phtchisch.ptd.ptd.ptd.phtchisch.ptd.ptd.ptd.ptd.ptd.ptd.ptd.ptd.ptd.ptd						
both, Bile, Batchescan, cc. there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Busicoth sever with System execution privileges receded. User interaction is not neceded for registration products. And old/busicores and road 13 Abundand 15: A 2018/37855 7023-06-78 4.4 Medium Interaction products and receives a possible out of bounds read due to interaction privileges receded. User interaction is not neceded for registration products. And road/busicores Androad 13 Abundand 15: A 2018/37856 7023-06-78 4.4 Medium Interaction products and receives a possible out of the products of the product	CVE-2023-21194	google - android		2023-06-28	4.4	Medium
company of the control of the control best of the control best of the control best of the control of the contro						
needed. User interaction is not needed for exploitation Product Androil/Versions. Annoted-13 Annoted id. P. A218357395 3123-96-28 4.4 Medium by poogle - android of he but, ble, proc., pit, pee of but, hef. fc., 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 medied. Liber interaction is not needed for exploitation Product. Androil/Versions. Antroid-13 Annoted in the A25847556. Over 2012-1109 google - android over 10 poogle - android over 2012-1109 google - android over 10 poogle - android over 2013-1109 google - android						
CVE-2023-21204 google - android Android/Versions: Android-13Android ID: A. 251857305 2023-06-28 4.4 Medium in the control of the			, , ,			
In thus ble proc. Ilk, read that, holicut, 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: Androidversions: Android-13/ndroid ID. A. 25/4459581. CVF-2073-21204 google - android Direction of the system of the system execution privileges in multiple life, 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 readed to a missing bounds check. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. The could lead to loca	CVE 2022 21106	google android	·	2022 06 28	4.4	Madium
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: Android/versions: An	CVE-2023-21196	google - android		2023-06-28	4.4	Medium
needed. User Interaction is not needed for exploitation. Product: Admirable Septiments and College Septiments an						
CVE 2023 - 21204 google - android Android/Versions: Android 13 Android ID: A. 254445961 2023 - 06.28 4.4 Medium in multiple lifes, there is a possible out of bounds read due to a missing bounds cheek. This could lead to local information disclosure in the wiff server with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android-13 Android ID: A. 252426361 2023 - 06.28 4.4 Medium interactions are considered. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android-13 Android-			, , , ,			
In multiple files, there is a possible out of bounds read due to a missing bounds cheek. This could lead to local findmation of disclosure in the wfile server with system execution privileges needed. User interaction is not needed for exploitation. Product: (VE-2023-21204 google - android CVE-2023-21206 google - android (VE-2023-21206 google - android (VE-2023-21210 google - android (V	CVE 2022 24400	la dan'd	·	2022 06 20	4.4	na.d.
missing bounds check. This could lead to local Information disclosure in the wifi server with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versinos: Andr	CVE-2023-21199	google - android		2023-06-28	4.4	Medium
disclosure in the wifi server with System execution privileges needed. User internation is not needed for exploitation. Product. OVE 2023-21206 google - android OVE 2023-21206 google - android OVE 2023-21208 google - android OVE 2023-21209 google - android OVE 2023-21209 google - android OVE 2023-21210 google - android OVE 2023-21212 google - android OVE 2023-21213 google - android OVE 2023-21214 google - android OVE 2023-21214 google - android OVE 2023-21215 google - android OVE 2023-21215 google - android OVE 2023-21216 google - android OVE 2023-21217 google - android OVE 2023-21218 google - android OVE 2023-21219 google - android OVE 2023-21210 google - android OV						
CVE-2023-21204 google - android Android/Versions. Android-13Android ID. A-262246231 2023-06-28 4.4 Medium in initiate-Version in initiate-Version and initia						
In initiate/venueur/AnnypQueryInternal of stal face.opp. there is a possible out of bounds read due to unsafe describation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android-13Android ID: A-262245254 2023-06-28 4.4 Medium in initiate ID: Initiate I			·			
possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation Product: Android/Versions: Android-13Android ID: A-2023-06-28 Let 2023-21208 poogle - android products and of the product of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation privileges needed. User interaction is not needed for exploitation product: Android/Versions: Android-13Android ID: A-2023-06-28 Let 2023-06-28 Let 2	CVE-2023-21204	google - android		2023-06-28	4.4	Medium
could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure in the wife server with System execution privileges needed. User interaction is not needed for exploitation. Product. Android/Versions: Android-13Android ID: A-2023-06-28 4.4 Medium in hit in this could be a formation of the provileges needed. User interaction is not needed for exploitation. Product. Android/Versions: Android-13Android ID: A-2023-06-28 4.4 Medium for the privileges needed. User interaction is not needed for exploitation. Product. Android/Versions: Android-13Android ID: A-2023-06-28 4.4 Medium for the privileges needed. User interaction is not needed for exploitation. Product. Android/Versions: Android-13Android ID: A-2023-06-28 4.4 Medium for the privileges needed. User interaction is not needed for exploitation. Product. Android/Versions: Android-13Android ID: A-2023-06-28 4.4 Medium for the product of this provileges needed. User interaction is not needed for exploita			" ' ' = ' ' ' '			
privileges needed. User interaction is not needed for expolation Product: Android/Westons: Android-133/Android ID: A- 2023-06-28						
2023-06-28 4.4 Medium			privileges needed. User interaction is not needed for			
In setCountryCodeInternal of sta, frace.ppp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions.	CVE 2022 24225	goods and the		2022 00 20	A A	NA = -1.
of bounds read due to improper input validation. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13.Android ID: A-262245254 2023-06-28 4.4 Medium in initiate Validation of the possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android-Versions: Androi	CVE-2023-21206	googie - android		zuz3-Ub-28	4.4	ivieaium
to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android-Versions: Android-13 Android ID: A-262245254 In initiate/Hs20iconQueryinternal of sta_iface.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android-13 Android ID: A-26236313 In multiple flies, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wiff server with System execution privileges needed. User interaction is not needed for exploitation. Product: Android-13 Android-13 Android-10: A-26236031 CVE-2023-21212 google - android In initiate/Tell-Tell-Android-13 Android-13						
CVE-2023-21208 google - android AndroidVersions: Android-13Android ID: A-262245254 2023-06-28 4.4 Medium			to local information disclosure with System execution privileges			
In inititateNs2DiconQueryInternal of sta_Iface.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Products. Android/Versions: Android/V	0./= 0000 0.4000		·			
possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android-13Android ID: A-2623-06-28	CVE-2023-21208	google - android		2023-06-28	4.4	Medium
could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-13Android ID: A-26223-6321 google - android						
exploitation.Product: AndroidVersions: Android-13Android ID: A- 262236331 In multiple files, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wiff server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-26235631 2023-06-28 4.4 Medium In initiateTdIsTeardownInternal of sta_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wiff server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A- 262235951 CVE-2023-21213 google - android In addCrouptWithConfighternal of p2p_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A- 262235951 CVE-2023-21214 google - android In addCrouptWithConfighternal of p2p_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A- 262235736 Input Validation vulnerability in Apache Software Foundation Apache Airflow ODBC Provider, Phache Software Foundation Apache Airflow MSSQL Provider, This vulnerability is considered low since it requires DAG code to use get_sqlatchemy_connection and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 3.4.1. A missing authorization check in multiple URL validation endpoints of the Insider Threat Management Server enables an anonymous attacker on an adjacent network to smuggle content via DNS lookup						
Section CVE-2023-21210 google - android Z62236331 In multiple files, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wifi server with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-13Android ID: A-Z62235033 Z023-06-28 4.4 Medium Me			· -			
In multiple files, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wiff server with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android-13Android ID: A-25235631 2023-06-28 4.4 Medium In initiateTdIsTeardownInternal of sta_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wiff server with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android-13Android ID: A-262235951 In addition-product: Android/Versions: Android-13Android ID: A-262235951 In addition-product: Android/Versions: Android-13Android ID: A-262235951 In addition-product: Android/Versions: Android-13Android ID: A-262235736 In addition-product In Android-13Android-13Android ID: A-262235736 In addition-product In Android-13Android-13Android ID: A-262235736 In addition-product In Android-13Android-13Android-13	CVE 2022 21210	google android	· ·	2022 06 29	4.4	Modium
missing bounds check. This could lead to local information disclosure in the wifi server with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android/-13Android ID: A-262236031 In initiaterIdisFeardowninternal of sta, Iface. copp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wifi server with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android-13Android ID: A-262335951 In addGroupWithConfighternal of p2p_Iface. cpp, there is a possible out of bounds read due to unsafe desertalization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android-13Android ID: A-26235951 In addGroupWithConfighternal of p2p_Iface. cpp, there is a possible out of bounds read due to unsafe desertalization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/versions: Android-13Android ID: A-2023-06-28 4.4 Medium Input Validation vulnerability in Apache Software Foundation Apache Airflow OBEC Provider. This vulnerability is considered low since it requires DAG code to use get_sqlatchemy_connection' and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow OBEC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. This issue affects Apache Airflow OBEC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. Is growing authorization check in multiple URL validation endpoints of the Insider Threat Management Server enables an anonymous attacker on an adjacent network to smuggle content via DNS cookups. All versions before 7.14.3 are affected. Imput Validation vulnerability in Apache Software Ended to the Apa	CVE-2023-21210	google - android		2023-06-28	4.4	Medium
needed. User interaction is not needed for exploitation. Product:			· · · · · · · · · · · · · · · · · · ·			
CVE-2023-21212 google - android Android/Versions: Android-13Android ID: A-262236031 2023-06-28 4.4 Medium			disclosure in the wifi server with System execution privileges			
In initiateTdIsTeardownInternal of sta_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wifi server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A- 262235951 In addGroupWithConfigInternal of p2p_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-13Android ID: A- 262235736 In addGroupWithConfigInternal of p2p_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-13Android ID: A- 262235736 Input Validation vulnerability in Apache Software Foundation Apache Airflow MSSQL Provider. Apache Software Foundation Apache Airflow MSSQL Provider. This vulnerability is considered low since it requires DAG code to use "get_sqlalchermy_connection" and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow	CVE 2022 24242	and a sudue!d	·	2022 06 20	4.4	0.4 a ali:
out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wifi server with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-13Android ID: A-262235951 In addGroupWithConfighternal of p2p_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-13Android ID: A-262235736 Input Validation vulnerability in Apache Software Foundation Apache Airflow OBEC Provider. Apache Software Foundation Apache Airflow MSSQL Provider. This vulnerability is considered low since it requires DAG code to use 'get_sqlatchemy_connection' and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. A missing authorization check in multiple URL validation endpoints of the Insider Threat Management Server enables an anonymous attacker on an adjacent network to smuggle content via DNS lookups. All versions before 7.14.3 are affected. VE-2023-36002 agement_server ibm - multiple products ibm - multiple products IBM X-Force ID: 248134. Medium Microsoft - Microsoft Edge (Chromium-based) Information Disclosure VVE-2021-42307 edge_chromium Vulnerability In installKey of KeyUtil.cpp, there is a possible failure of file	CVE-2023-21212	google - android		2023-06-28	4.4	Medium
to local information disclosure in the wifi server with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android-13Android ID: A-262235951 In addGroupWithConfighternal of p2p_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android/Versions: Android-13Android ID: A-262235736 Input Validation vulnerability in Apache Software Foundation Apache Airflow ODBC Provider. Apache Software Foundation Apache Airflow MSSQL Provider. This vulnerability is considered low since it requires DAG code to use 'get_sqlalchemy_connection' and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. **CVE-2023-35798** This is insue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. **A missing authorization check in multiple URL validation endpoints proofpoint insider_threat_man agament server enables an anonymous attacker on an adjacent network to smuggle content via DNS 2023-06-27						
exploitation.Product: AndroidVersions: Android-13Android ID: A- 262233951 In addGroupWithConfighternal of p2p_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A- 262235736 Input Validation vulnerability in Apache Software Foundation Apache Airflow OBSC Provider, Apache Software Foundation Apache Airflow MSSQL Provider.This vulnerability is considered low since it requires DAG code to use get_sqlachemy_connection* and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow OBSC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. This issue affects Apache Airflow OBSC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. It is recommended to upgrade to a version that is not affected proofpoint insider_threat_man agement_server lockups. All versions before 7.14.3 are affected. VE-2023-36002 IBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. BM X-Force ID: 248134. VE-2021-42307 VUE-2021-42307 VUE-2021-42307 In installKey of KeyUtil.cpp, there is a possible failure of file			to local information disclosure in the wifi server with System			
CVE-2023-21213 google - android 262235951						
In addGroupWithConfigInternal of p2p_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262235736 Input Validation vulnerability in Apache Software Foundation Apache Airflow ODBC Provider, Apache Software Foundation Apache Airflow MSSQL Provider. This vulnerability is considered low since it requires DAG code to use 'get_sqlalchemy_connection' and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. It is recommended to upgrade to a version that is not affected 2023-06-27 4.3 Medium Amissing authorization check in multiple URL validation endpoints of the Insider Threat Management Server enables an anonymous attacker on an adjacent network to smuggle content via DNS lookups. All versions before 7.14.3 are affected. 2023-06-27 4.3 Medium IBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. IBM X-Force ID: 248134. 2023-06-27 4.3 Medium VE-2023-26273 microsoft dege_chromium linistallKey of KeyUtil.cpp, there is a possible failure of file	CVF-2023-21213	google - android		2023-06-28	4.4	Medium
possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262235736 Input Validation vulnerability in Apache Software Foundation Apache Airflow ODBC Provider, Apache Software Foundation Apache Airflow MSSQL Provider. This vulnerability is considered low since it requires DAG code to use 'get_sqlalchemy_connection' and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. apache - multiple products proofpoint - insider_threat_man agement_server ibim - multiple products ibm	<u>CVL 2023 21213</u>	googie anaroid		2023 00 28	7.7	Wicalam
privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-2023-06-28 4.4 Medium CVE-2023-21214 google - android 262235736 2023-06-28 4.4 Medium			· · · · · · · · · · · · · · · · · · ·			
exploitation.Product: AndroidVersions: Android-13Android ID: A- 262235736 Input Validation vulnerability in Apache Software Foundation Apache Airflow ODBC Provider, Apache Software Foundation Apache Airflow MSSQL Provider.This vulnerability is considered low since it requires DAG code to use 'get_sqlalchemy_connection' and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. A missing authorization check in multiple URL validation endpoints of the Insider Threat Management Server enables an anonymous attacker on an adjacent network to smuggle content via DNS attacker on an adjacent network to smuggle content via DNS IBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. IBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. IBM X-Force ID: 248134. OUE-2021-42307 Microsoft Edge (Chromium-based) Information Disclosure Vulnerability Vulnerability Vulnerability Vulnerability August 2023-07-01 A.3 Medium In installKey of KeyUtil.cpp, there is a possible failure of file			· · · · · · · · · · · · · · · · · · ·			
CVE-2023-21214 google - android 262235736 2023-06-28 4.4 Medium Input Validation vulnerability in Apache Software Foundation Apache Airflow ODBC Provider, Apache Software Foundation Apache Airflow MSSQL Provider. This vulnerability is considered low since it requires DAG code to use 'get_sqlalchemy_connection' and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1.						
Input Validation vulnerability in Apache Software Foundation Apache Airflow ODBC Provider, Apache Software Foundation Apache Airflow MSSQL Provider. This vulnerability is considered low since it requires DAG code to use 'get_sqlalchemy_connection' and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. A missing authorization check in multiple URL validation endpoints of the Insider Threat Management Server enables an anonymous attacker on an adjacent network to smuggle content via DNS CVE-2023-36002 agement_server lookups. All versions before 7.14.3 are affected. 2023-06-27 4.3 Medium BM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. BM X-Force ID: 248134. 2023-06-27 4.3 Medium In installKey of KeyUtil.cpp, there is a possible failure of file	CVE-2023-21214	google - android		2023-06-28	4.4	Medium
Apache Airflow MSSQL Provider. This vulnerability is considered low since it requires DAG code to use 'get_sqlalchemy_connection' and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. Lit is recommended to upgrade to a version that is not affected proofpoint - insider_threat_man agement_server A missing authorization check in multiple URL validation endpoints of the Insider Threat Management Server enables an anonymous attacker on an adjacent network to smuggle content via DNS lookups. All versions before 7.14.3 are affected. CVE-2023-36002 IBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. IBM X-Force ID: 248134. Medium Microsoft - edge_chromium Microsoft Edge (Chromium-based) Information Disclosure 2023-07-01 4.3 Medium 4.		5 6 2 2				
low since it requires DAG code to use 'get_sqlalchemy_connection' and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. Lit is recommended to upgrade to a version that is not affected 2023-06-27 4.3 Medium A missing authorization check in multiple URL validation endpoints of the Insider Threat Management Server enables an anonymous attacker on an adjacent network to smuggle content via DNS lookups. All versions before 7.14.3 are affected. Lookups. All versions before 7.14.3 are affected. 2023-06-27 4.3 Medium BM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. Love-2023-26273 products BM X-Force ID: 248134. 2023-06-27 4.3 Medium microsoft dege_chromium Vulnerability Vulnerability 2023-07-01 4.3 Medium In installKey of KeyUtil.cpp, there is a possible failure of file			· · · · · · · · · · · · · · · · · · ·			
CVE-2023-35798productsIt is recommended to upgrade to a version that is not affected2023-06-274.3MediumCVE-2023-36002A missing authorization check in multiple insider_threat_man agement_serverIt were not agement_server100kups. All versions before 7.14.3 are affected.2023-06-274.3MediumCVE-2023-26273BM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation.2023-06-274.3MediumCVE-2021-42307Microsoft Edge (Chromium-based) Information Disclosure2023-07-014.3Medium			·			
connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. It is recommended to upgrade to a version that is not affected 2023-06-27 4.3 Medium A missing authorization check in multiple URL validation endpoints of the Insider Threat Management Server enables an anonymous attacker on an adjacent network to smuggle content via DNS lookups. All versions before 7.14.3 are affected. 2023-06-27 4.3 Medium CVE-2023-36002 IBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. CVE-2023-26273 products IBM X-Force ID: 248134. 2023-06-27 4.3 Medium microsoft - edge_chromium Vulnerability 2023-07-01 4.3 Medium In installKey of KeyUtil.cpp, there is a possible failure of file			· · · · · · · · · · · · · · · · · · ·			
exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. It is recommended to upgrade to a version that is not affected products A missing authorization check in multiple URL validation endpoints of the Insider Threat Management Server enables an anonymous attacker on an adjacent network to smuggle content via DNS lookups. All versions before 7.14.3 are affected. CVE-2023-36002 IBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. CVE-2023-26273 products IBM X-Force ID: 248134. Medium CVE-2021-42307 Microsoft - edge_chromium Microsoft Edge (Chromium-based) Information Disclosure Vulnerability In installKey of KeyUtil.cpp, there is a possible failure of file			· · · · · · · · · · · · · · · · · ·			
Apache Airflow MSSQL Provider: before 3.4.1. CVE-2023-35798 products			, , , ,			
Apache Airflow MSSQL Provider: before 3.4.1. CVE-2023-35798 products			This issue affects Anacha Airflant ODDS Dravidant by Surviva			
apache - multiple products						
CVE-2023-35798 products It is recommended to upgrade to a version that is not affected A missing authorization check in multiple URL validation endpoints of the Insider Threat Management Server enables an anonymous attacker on an adjacent network to smuggle content via DNS lookups. All versions before 7.14.3 are affected. CVE-2023-36002 IBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. CVE-2023-26273 products IBM X-Force ID: 248134. 2023-06-27 4.3 Medium microsoft - edge_chromium Vulnerability Vulnerability 2023-07-01 4.3 Medium In installKey of KeyUtil.cpp, there is a possible failure of file		apache - multiple	p.s.i.e / iii /			
proofpoint - insider_threat_man attacker on an adjacent network to smuggle content via DNS CVE-2023-36002 agement_server lookups. All versions before 7.14.3 are affected. 2023-06-27 4.3 Medium IBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. CVE-2023-26273 products IBM X-Force ID: 248134. 2023-06-27 4.3 Medium microsoft - Microsoft Edge (Chromium-based) Information Disclosure CVE-2021-42307 edge_chromium Vulnerability 2023-07-01 4.3 Medium In installKey of KeyUtil.cpp, there is a possible failure of file	CVE-2023-35798	products	· -	2023-06-27	4.3	Medium
insider_threat_man attacker on an adjacent network to smuggle content via DNS lookups. All versions before 7.14.3 are affected. IBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. CVE-2023-26273 products IBM X-Force ID: 248134. 2023-06-27 4.3 Medium microsoft - Microsoft Edge (Chromium-based) Information Disclosure Vulnerability 2023-07-01 4.3 Medium In installKey of KeyUtil.cpp, there is a possible failure of file			, , ,			
CVE-2023-36002agement_serverlookups. All versions before 7.14.3 are affected.2023-06-274.3MediumIBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation.2023-06-274.3MediumCVE-2023-26273productsIBM X-Force ID: 248134.2023-06-274.3MediumMicrosoft - edge_chromiumMicrosoft Edge (Chromium-based) Information Disclosure2023-07-014.3MediumCVE-2021-42307edge_chromiumVulnerability2023-07-014.3MediumIn installKey of KeyUtil.cpp, there is a possible failure of file		· ·	·			
IBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. CVE-2023-26273 products products IBM X-Force ID: 248134. 2023-06-27 4.3 Medium microsoft - edge_chromium Vulnerability 2023-07-01 4.3 Medium In installKey of KeyUtil.cpp, there is a possible failure of file	CVE-2023-36002		,	2023-06-27	4.3	Medium
CVE-2023-26273productsIBM X-Force ID: 248134.2023-06-274.3Mediummicrosoft - edge_chromiumMicrosoft Edge (Chromium-based) Information Disclosure Vulnerability2023-07-014.3MediumIn installKey of KeyUtil.cpp, there is a possible failure of fileMedium		<u> </u>	IBM QRadar SIEM 7.5.0 could allow an authenticated user to			
microsoft - dege_chromium	.	· ·				
CVE-2021-42307edge_chromiumVulnerability2023-07-014.3MediumIn installKey of KeyUtil.cpp, there is a possible failure of file	CVE-2023-26273	•		2023-06-27	4.3	Medium
In installKey of KeyUtil.cpp, there is a possible failure of file	CVF-2021-42307			2023-07-01	4.3	Medium
	<u> </u>		,	2020 07 01		caiaiii
· · · · · · · · · · · · · · · · · · ·	CVE-2023-21178	google - android		2023-06-28	4.1	Medium

		information disclosure with System execution privileges needed.			
		User interaction is not needed for exploitation.Product:			
		AndroidVersions: Android-13Android ID: A-140762419			
		Improper Knox ID validation logic in notification framework prior			
	samsung - multiple	to SMR Jun-2023 Release 1 allows local attackers to read work			
CVE-2023-21512	products	profile notifications without proper access permission.	2023-06-28	3.3	Low
	microsoft -				
CVE-2022-29147	edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2023-06-29	3.1	Low

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's الله الثغرات كما تم نشرها من قبل NIST's المناسبة. NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.