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

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ١٩ مارس إلى ٢٦ مارس. ويتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) from 19 March to 26 March. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-25684	ibm - multiple products	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 247597.	2023-03-21	9.8	Critical
CVE-2023-1529	google - chrome	Out of bounds memory access in WebHID in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a malicious HID device. (Chromium security severity: High)	2023-03-21	9.8	Critical
CVE-2023-26497	samsung - exynos_modem_5300_firmware	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute.	2023-03-21	9.8	Critical
CVE-2023-25589	arubanetworks - multiple products	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to create arbitrary users on the platform. A successful exploit allows an attacker to achieve total cluster compromise.	2023-03-22	9.8	Critical
CVE-2023-26498	samsung - exynos_modem_5300_firmware	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module.	2023-03-23	9.8	Critical
CVE-2023-26496	samsung - exynos_modem_5300_firmware	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module.	2023-03-23	9.8	Critical
CVE-2023-27078	tp-link - tl-mr3020_firmware	A command injection issue was found in TP-Link MR3020 v.1_150921 that allows a remote attacker to execute arbitrary commands via a crafted request to the tftp endpoint.	2023-03-23	9.8	Critical
CVE-2023-26359	adobe - multiple products	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction.	2023-03-23	9.8	Critical
CVE-2023-26360	adobe - multiple products	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by an Improper Access Control vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction.	2023-03-23	9.8	Critical
CVE-2022-20532	google - android	In parseTrackFragmentRun() of MPEG4Extractor.cpp, there is a possible out of bounds read due to an integer overflow. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for	2023-03-24	9.8	Critical

		exploitation.Product: AndroidVersions: Android-13Android ID: A-232242894			
CVE-2022-42498	google - android	In Pixel cellular firmware, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-240662453References: N/A	2023-03-24	9.8	Critical
CVE-2022-42499	google - android	In sms_SendMmCpErrMsg of sms_MmConManagement.c, there is a possible out of bounds 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-242001391References: N/A	2023-03-24	9.8	Critical
CVE-2023-20951	google - multiple products	In gatt_process_prep_write_rsp of gatt_cl.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258652631	2023-03-24	9.8	Critical
CVE-2023-20954	google - multiple products	In SDP_AddAttribute of sdp_db.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261867748	2023-03-24	9.8	Critical
CVE-2023-21057	google - android	In ProfSixDecomTcpSACKoption of RohcPacketCommon, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244450646References: N/A	2023-03-24	9.8	Critical
CVE-2023-21058	google - android	In lcsm_SendRrAcquiAssist of lcsm_bcm_assist.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-246169606References: N/A	2023-03-24	9.8	Critical
CVE-2023-25664	google - tensorflow	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, there is a heap buffer overflow in TAvgPoolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1.	2023-03-25	9.8	Critical
CVE-2023-25668	google - tensorflow	TensorFlow is an open source platform for machine learning. Attackers using Tensorflow prior to 2.12.0 or 2.11.1 can access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and will also cherrypick this commit on TensorFlow version 2.11.1.	2023-03-25	9.8	Critical
CVE-2022-36413	zohocorp - multiple products	Zoho ManageEngine ADSelfService Plus through 6203 is vulnerable to a brute-force attack that leads to a password reset on IDM applications.	2023-03-23	9.1	Critical
CVE-2023-27980	schneider-electric - multiple products	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior)	2023-03-21	8.8	High
CVE-2023-27982	schneider-electric - multiple products	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).	2023-03-21	8.8	High
CVE-2023-27981	schneider-electric - multiple products	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).	2023-03-21	8.8	High
CVE-2023-27984	schneider-electric -	A CWE-20: Improper Input Validation vulnerability exists in Custom Reports that could cause a macro to be executed, potentially leading to remote code execution when a user opens	2023-03-21	8.8	High

	multiple products	a malicious report file planted by an attacker. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).			
CVE-2023-27874	ibm - multiple products	IBM Aspera Faspex 4.4.2 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote authenticated attacker could exploit this vulnerability to execute arbitrary commands. IBM X-Force ID: 249845.	2023-03-21	8.8	High
CVE-2022-37337	netgear - rbs750_firmware	A command execution vulnerability exists in the access control functionality of Netgear Orbi Router RBR750 4.6.8.5. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2023-03-21	8.8	High
CVE-2022-38452	netgear - rbs750_firmware	A command execution vulnerability exists in the hidden telnet service functionality of Netgear Orbi Router RBR750 4.6.8.5. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a network request to trigger this vulnerability.	2023-03-21	8.8	High
CVE-2023-1528	google - chrome	Use after free in Passwords in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-03-21	8.8	High
CVE-2023-1530	google - chrome	Use after free in PDF in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-03-21	8.8	High
CVE-2023-1531	google - chrome	Use after free in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-03-21	8.8	High
CVE-2023-1532	google - chrome	Out of bounds read in GPU Video in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-03-21	8.8	High
CVE-2023-1533	google - chrome	Use after free in WebProtect in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-03-21	8.8	High
CVE-2023-1534	google - chrome	Out of bounds read in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-03-21	8.8	High
CVE-2023-25069	trendmicro - txone_stellarone	TXOne StellarOne has an improper access control privilege escalation vulnerability in every version before V2.0.1160 that could allow a malicious, falsely authenticated user to escalate his privileges to administrator level. With these privileges, an attacker could perform actions they are not authorized to. Please note: an attacker must first obtain a low-privileged authenticated user's profile on the target system in order to exploit this vulnerability.	2023-03-22	8.8	High
CVE-2023-25594	arubanetworks - multiple products	A vulnerability in the web-based management interface of ClearPass Policy Manager allows an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of this vulnerability allows an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform.	2023-03-22	8.8	High
CVE-2023-25924	ibm - multiple products	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to perform actions that they should not have access to due to improper authorization. IBM X-Force ID: 247630.	2023-03-22	8.8	High
CVE-2023-20055	cisco - multiple products	A vulnerability in the management API of Cisco DNA Center could allow an authenticated, remote attacker to elevate privileges in the context of the web-based management interface on an affected device. This vulnerability is due to the unintended exposure of sensitive information. An attacker could exploit this vulnerability by inspecting the responses from the API. Under certain circumstances, a successful exploit could allow the attacker to access the API with the privileges of a higher-level user account. To successfully exploit this vulnerability, the attacker would need at least valid Observer credentials.	2023-03-23	8.8	High
CVE-2023-20960	google - multiple products	In launchDeepLinkIntentToRight of SettingsHomepageActivity.java, there is a possible way to launch arbitrary activities due to improper input validation. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product:	2023-03-24	8.8	High

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

CVE-2023-26426	adobe - multiple products	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-22	7.8	High
CVE-2023-0386	linux - multiple products	A flaw was found in the Linux kernel, where unauthorized access to the execution of the setuid file with capabilities was found in the Linux kernel's OverlayFS subsystem in how a user copies a capable file from a nosuid mount into another mount. This uid mapping bug allows a local user to escalate their privileges on the system.	2023-03-22	7.8	High
CVE-2023-28759	veritas - netbackup	An issue was discovered in Veritas NetBackup before 10.0. A vulnerability in the way NetBackup validates the path to a DLL prior to loading may allow a lower level user to elevate privileges and compromise the system.	2023-03-23	7.8	High
CVE-2023-28772	linux - linux_kernel	An issue was discovered in the Linux kernel before 5.13.3. lib/seq_buf.c has a seq_buf_putmem_hex buffer overflow.	2023-03-23	7.8	High
CVE-2023-20035	cisco - ios_xe_sd-wan	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.	2023-03-23	7.8	High
CVE-2023-20065	cisco - multiple products	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.	2023-03-23	7.8	High
CVE-2023-1252	linux - linux_kernel	A use-after-free flaw was found in the Linux kernel's Ext4 File System in how a user triggers several file operations simultaneously with the overlay FS usage. This flaw allows a local user to crash or potentially escalate their privileges on the system. Only if patch 9a2544037600 ("ovl: fix use after free in struct ovl_aio_req") not applied yet, the kernel could be affected.	2023-03-23	7.8	High
CVE-2022-38745	apache - openoffice	Apache OpenOffice versions before 4.1.14 may be configured to add an empty entry to the Java class path. This may lead to run arbitrary Java code from the current directory.	2023-03-24	7.8	High
CVE-2022-47502	apache - openoffice	Apache OpenOffice documents can contain links that call internal macros with arbitrary arguments. Several URI Schemes are defined for this purpose. Links can be activated by clicks, or by automatic document events. The execution of such links must be subject to user approval. In the affected versions of OpenOffice, approval for certain links is not requested; when activated, such links could therefore result in arbitrary script execution.	2023-03-24	7.8	High
CVE-2022-20542	google - android	In parseParamsBlob of types.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-238083570	2023-03-24	7.8	High
CVE-2023-20906	google - multiple products	In onPackageAddedInternal of PermissionManagerService.java, there is a possible way to silently grant a permission after a Target SDK update due to a permissions bypass. This could lead to local escalation of privilege after updating an app to a higher Target SDK with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-221040577	2023-03-24	7.8	High
CVE-2023-20911	google - multiple products	In addPermission of PermissionManagerServiceImpl.java , there is a possible failure to persist permission settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242537498	2023-03-24	7.8	High

CVE-2023-20917	google - multiple products	In onTargetSelected of ResolverActivity.java, there is a possible way to share a wrong file due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242605257	2023-03-24	7.8	High
CVE-2023-20931	google - multiple products	In avdt_scb_hdl_write_req of avdt_scb_act.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242535997	2023-03-24	7.8	High
CVE-2023-20936	google - multiple products	In bta_av_rc_disc_done of bta_av_act.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-226927612	2023-03-24	7.8	High
CVE-2023-20947	google - multiple products	In getGroupState of GrantPermissionsViewModel.kt, there is a possible way to keep a one-time permission granted due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-237405974	2023-03-24	7.8	High
CVE-2023-20953	google - android	In onPrimaryClipChanged of ClipboardListener.java, there is a possible way to bypass factory reset protection due to incorrect UI being shown prior to setup completion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-251778420	2023-03-24	7.8	High
CVE-2023-20955	google - multiple products	In onPrepareOptionsMenu of AppInfoDashboardFragment.java, there is a possible way to bypass admin restrictions and uninstall applications for all users due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258653813	2023-03-24	7.8	High
CVE-2023-20957	google - multiple products	In onAttach of SettingsPreferenceFragment.java, there is a possible bypass of Factory Reset Protections due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-258422561	2023-03-24	7.8	High
CVE-2023-20959	google - android	In AddSupervisedUserActivity, guest users are not prevented from starting the activity due to missing permissions checks. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-249057848	2023-03-24	7.8	High
CVE-2023-20963	google - multiple products	In WorkSource, there is a possible parcel mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-220302519	2023-03-24	7.8	High
CVE-2023-20964	google - multiple products	In multiple functions of MediaSessionRecord.java, there is a possible Intent rebroadcast due to a confused deputy. This could lead to local denial of service or escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-238177121	2023-03-24	7.8	High
CVE-2023-20966	google - multiple products	In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242299736	2023-03-24	7.8	High
CVE-2023-20971	google - android	In updatePermissionTreeSourcePackage of PermissionManagerServiceImpl.java, there is a possible way to obtain dangerous permission without the user's consent due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-225880325	2023-03-24	7.8	High
CVE-2023-20975	google - android	In getAvailabilityStatus of EnableContentCapturePreferenceController.java, there is a possible way to bypass DISALLOW_CONTENT_CAPTURE due to a permissions bypass. This could lead to local escalation of	2023-03-24	7.8	High

		privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-250573776			
CVE-2023-20985	google - android	In BTA_GATTS_HandleValueIndication of bta_gatts_api.cc, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-245915315	2023-03-24	7.8	High
CVE-2023-20993	google - android	In multiple functions of SnoozeHelper.java, there is a possible failure to persist settings due to an uncaught exception. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261588851	2023-03-24	7.8	High
CVE-2023-20995	google - android	In captureImage of CustomizedSensor.cpp, there is a possible way to bypass the fingerprint unlock due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-241910279	2023-03-24	7.8	High
CVE-2023-21000	google - android	In MediaCodec.cpp, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-194783918	2023-03-24	7.8	High
CVE-2023-21001	google - android	In onContextItemSelected of NetworkProviderSettings.java, there is a possible way for users to change the Wi-Fi settings of other users due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-237672190	2023-03-24	7.8	High
CVE-2023-21002	google - android	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193935	2023-03-24	7.8	High
CVE-2023-21003	google - android	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193711	2023-03-24	7.8	High
CVE-2023-21004	google - android	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193664	2023-03-24	7.8	High
CVE-2023-21005	google - android	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193946	2023-03-24	7.8	High
CVE-2023-21015	google - android	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-244569778	2023-03-24	7.8	High
CVE-2023-21017	google - android	In InstallStart of InstallStart.java, there is a possible way to change the installer package name due to an improper input validation. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-236687884	2023-03-24	7.8	High
CVE-2023-21021	google - android	In isTargetSdkLessThanQOrPrivileged of WifiServiceImpl.java, there is a possible way for the guest user to change admin user network settings due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255537598	2023-03-24	7.8	High
CVE-2023-21022	google - android	In BufferBlock of Suballocation.cpp, there is a possible out of bounds write due to memory corruption. This could lead to local escalation of privilege with no additional execution privileges	2023-03-24	7.8	High

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

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

CVE-2023-25667	google - tensorflow	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, integer overflow occurs when `2^31 <= num_frames * height * width * channels < 2^32`, for example Full HD screencast of at least 346 frames. A fix is included in TensorFlow version 2.12.0 and version 2.11.1.	2023-03-25	7.5	High
CVE-2023-25669	google - tensorflow	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, if the stride and window size are not positive for `tf.raw_ops.AvgPoolGrad`, it can give a floating point exception. A fix is included in TensorFlow version 2.12.0 and version 2.11.1.	2023-03-25	7.5	High
CVE-2023-25670	google - tensorflow	TensorFlow is an open source platform for machine learning. Versions prior to 2.12.0 and 2.11.1 have a null point error in QuantizedMatMulWithBiasAndDequantize with MKL enabled. A fix is included in TensorFlow version 2.12.0 and version 2.11.1.	2023-03-25	7.5	High
CVE-2023-25671	google - tensorflow	TensorFlow is an open source platform for machine learning. There is out-of-bounds access due to mismatched integer type sizes. A fix is included in TensorFlow version 2.12.0 and version 2.11.1.	2023-03-25	7.5	High
CVE-2023-25672	google - tensorflow	TensorFlow is an open source platform for machine learning. The function `tf.raw_ops.LookupTableImportV2` cannot handle scalars in the `values` parameter and gives an NPE. A fix is included in TensorFlow version 2.12.0 and version 2.11.1.	2023-03-25	7.5	High
CVE-2023-25673	google - tensorflow	TensorFlow is an open source platform for machine learning. Versions prior to 2.12.0 and 2.11.1 have a Floating Point Exception in TensorListSplit with XLA. A fix is included in TensorFlow version 2.12.0 and version 2.11.1.	2023-03-25	7.5	High
CVE-2023-25674	google - tensorflow	TensorFlow is an open source machine learning platform. Versions prior to 2.12.0 and 2.11.1 have a null pointer error in RandomShuffle with XLA enabled. A fix is included in TensorFlow 2.12.0 and 2.11.1.	2023-03-25	7.5	High
CVE-2023-27579	google - tensorflow	TensorFlow is an end-to-end open source platform for machine learning. Constructing a tflite model with a paramater `filter_input_channel` of less than 1 gives a FPE. This issue has been patched in version 2.12. TensorFlow will also cherrypick the fix commit on TensorFlow 2.11.1.	2023-03-25	7.5	High
CVE-2023-20976	google - android	In getConfirmationMessage of DefaultAutofillPicker.java, there is a possible way to mislead the user to select default autofill application due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-216117246	2023-03-24	7.3	High
CVE-2022-36429	netgear - rbs750_firmware	A command execution vulnerability exists in the ubus backend communications functionality of Netgear Orbi Satellite RBS750 4.6.8.5. A specially-crafted JSON object can lead to arbitrary command execution. An attacker can send a sequence of malicious packets to trigger this vulnerability.	2023-03-21	7.2	High
CVE-2022-43863	ibm - multiple products	IBM QRadar SIEM 7.4 and 7.5 is vulnerable to privilege escalation, allowing a user with some admin capabilities to gain additional admin capabilities. IBM X-Force ID: 239425.	2023-03-22	7.2	High
CVE-2023-21054	google - android	In EUTRAN_LCS_ConvertLCS_MOLRReq of LPP_CommonUtil.c, there is a possible out of bounds write due to a logic error in the code. This could lead to remote code execution with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244556535References: N/A	2023-03-24	7.2	High
CVE-2023-28685	jenkins - absint_a3	Jenkins AbsInt a³ Plugin 1.1.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2023-03-22	7.1	High
CVE-2023-28758	veritas - netbackup	An issue was discovered in Veritas NetBackup before 8.3.0.2. BPCD allows an unprivileged user to specify a log file path when executing a NetBackup command. This can be used to overwrite existing NetBackup log files.	2023-03-23	7.1	High
CVE-2023-20958	google - android	In read_paint of ttcolr.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254803162	2023-03-24	7.1	High
CVE-2023-28005	trendmicro - trend_micro_endpoint_encryption	A vulnerability in Trend Micro Endpoint Encryption Full Disk Encryption version 6.0.0.3204 and below could allow an attacker with physical access to an affected device to bypass Microsoft Windows? Secure Boot process in an attempt to execute other attacks to obtain access to the contents of the device. An attacker must first obtain physical access to the target system in order to exploit this vulnerability. It is also important to note that the contents of the drive(s) encrypted with TMEE FDE would still be protected and would NOT be accessible by the attacker by exploitation of this vulnerability alone.	2023-03-22	6.8	Medium

CVE-2023-20082	cisco - multiple products	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.	2023-03-23	6.8	Medium
CVE-2023-20926	google - multiple products	In onParentVisible of HeaderPrivacyIconsController.kt, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-253043058	2023-03-24	6.8	Medium
CVE-2023-25134	mcafee - total_protection	McAfee Total Protection prior to 16.0.50 may allow an adversary (with full administrative access) to modify a McAfee specific Component Object Model (COM) in the Windows Registry. This can result in the loading of a malicious payload.	2023-03-21	6.7	Medium
CVE-2022-42500	google - android	In OEM_OnRequest of sced.cpp, there is a possible shell command execution due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239701389References: N/A	2023-03-24	6.7	Medium
CVE-2023-20994	google - android	In _ufdt_output_property_to_fdt of ufdt_convert.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-259062118	2023-03-24	6.7	Medium
CVE-2023-21018	google - android	In UnwindingWorker of unwinding.cc, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-233338564	2023-03-24	6.7	Medium
CVE-2023-21020	google - android	In registerSignalHandlers of main.c, there is a possible local arbitrary code execution 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-13Android ID: A-256591441	2023-03-24	6.7	Medium
CVE-2023-21038	google - android	In cs40l2x_cp_trigger_queue_show of cs40l2x.c, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-224000736References: N/A	2023-03-24	6.7	Medium
CVE-2023-21042	google - android	In (TBD) of (TBD), there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239873326References: N/A	2023-03-24	6.7	Medium
CVE-2023-21043	google - android	In (TBD) of (TBD), there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239872581References: N/A	2023-03-24	6.7	Medium
CVE-2023-21050	google - android	In load_png_image of ExynosHWCHelper.cpp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244423702References: N/A	2023-03-24	6.7	Medium
CVE-2023-21051	google - android	In dwc3_exynos_clk_get of dwc3-exynos.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-259323322References: N/A	2023-03-24	6.7	Medium
CVE-2023-21052	google - android	In setToExternal of ril_external_client.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	2023-03-24	6.7	Medium

		needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-259063189References: N/A			
CVE-2023-21056	google - android	In lwis_slc_buffer_free of lwis_device_slc.c, there is a possible memory corruption due to type confusion. 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-245300559References: N/A	2023-03-24	6.7	Medium
CVE-2023-21062	google - android	In DoSetTempEcc of imsservice.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243376770References: N/A	2023-03-24	6.7	Medium
CVE-2023-21063	google - android	In ParseWithAuthType of simdata.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243129862References: N/A	2023-03-24	6.7	Medium
CVE-2023-21064	google - android	In DoSetPinControl of miscservice.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: AndroidVersions: Android kernelAndroid ID: A-243130078References: N/A	2023-03-24	6.7	Medium
CVE-2023-21065	google - android	In fdt_next_tag of fdt.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239630493References: N/A	2023-03-24	6.7	Medium
CVE-2023-21069	google - android	In wl_update_hidden_ap_ie of wl_cfgscan.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254029309References: N/A	2023-03-24	6.7	Medium
CVE-2023-21070	google - android	In add_roam_cache_list of wl_roam.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254028776References: N/A	2023-03-24	6.7	Medium
CVE-2023-21071	google - android	In dhd_prot_ioctcmplt_process of dhd_msgbuf.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254028518References: N/A	2023-03-24	6.7	Medium
CVE-2023-21072	google - android	In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257290781References: N/A	2023-03-24	6.7	Medium
CVE-2023-21073	google - android	In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257290396References: N/A	2023-03-24	6.7	Medium
CVE-2023-21075	google - android	In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857862References: N/A	2023-03-24	6.7	Medium
CVE-2023-21076	google - android	In createTransmitFollowupRequest of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857623References: N/A	2023-03-24	6.7	Medium
CVE-2023-21077	google - android	In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:	2023-03-24	6.7	Medium

		AndroidVersions: Android kernelAndroid ID: A-257289560References: N/A			
CVE-2023-21078	google - android	In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254840211References: N/A	2023-03-24	6.7	Medium
CVE-2023-21079	google - android	In rtt_unpack_xtlv_cbfn of dhd_rtt.c, 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-254839721References: N/A	2023-03-24	6.7	Medium
CVE-2023-27873	ibm - multiple products	IBM Aspera Faspex 4.4.2 could allow a remote authenticated attacker to obtain sensitive credential information using specially crafted XML input. IBM X-Force ID: 249654.	2023-03-21	6.5	Medium
CVE-2023-25591	arubanetworks - multiple products	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow a remote attacker authenticated with low privileges to access sensitive information. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further privileges on the ClearPass instance.	2023-03-22	6.5	Medium
CVE-2023-20059	cisco - multiple products	A vulnerability in the implementation of the Cisco Network Plug-and-Play (PnP) agent of Cisco DNA Center could allow an authenticated, remote attacker to view sensitive information in clear text. The attacker must have valid low-privileged user credentials. This vulnerability is due to improper role-based access control (RBAC) with the integration of PnP. An attacker could exploit this vulnerability by authenticating to the device and sending a query to an internal API. A successful exploit could allow the attacker to view sensitive information in clear text, which could include configuration files.	2023-03-23	6.5	Medium
CVE-2023-20066	cisco - multiple products	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.	2023-03-23	6.5	Medium
CVE-2023-20861	vmware - multiple products	In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.	2023-03-23	6.5	Medium
CVE-2023-21055	google - android	In dit_hal_ioctl of dit.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244301523References: N/A	2023-03-24	6.4	Medium
CVE-2023-25592	arubanetworks - multiple products	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	2023-03-22	6.1	Medium
CVE-2023-25593	arubanetworks - multiple products	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	2023-03-22	6.1	Medium
CVE-2022-38458	netgear - rbs750_firmware	A cleartext transmission vulnerability exists in the Remote Management functionality of Netgear Orbi Router RBR750 4.6.8.5. A specially-crafted man-in-the-middle attack can lead to a disclosure of sensitive information.	2023-03-21	5.9	Medium
CVE-2023-20081	cisco - multiple products	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload,	2023-03-23	5.9	Medium

		resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.			
CVE-2023-25686	ibm - multiple products	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 247601.	2023-03-21	5.5	Medium
CVE-2023-25595	arubanetworks - multiple products	A vulnerability exists in the ClearPass OnGuard Ubuntu agent that allows for an attacker with local Ubuntu instance access to potentially obtain sensitive information. Successful Exploitation of this vulnerability allows an attacker to retrieve information that is of a sensitive nature to the ClearPass/OnGuard environment.	2023-03-22	5.5	Medium
CVE-2023-25862	adobe - multiple products	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-22	5.5	Medium
CVE-2023-20056	cisco - wireless_lan_controller_software	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.	2023-03-23	5.5	Medium
CVE-2023-1249	linux - linux_kernel	A use-after-free flaw was found in the Linux kernel's core dump subsystem. This flaw allows a local user to crash the system. Only if patch 390031c94211 ("coredump: Use the vma snapshot in fill_files_note") not applied yet, then kernel could be affected.	2023-03-23	5.5	Medium
CVE-2023-20859	vmware - multiple products	In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token.	2023-03-23	5.5	Medium
CVE-2020-36691	linux - linux_kernel	An issue was discovered in the Linux kernel before 5.8. lib/nlattr.c allows attackers to cause a denial of service (unbounded recursion) via a nested Netlink policy with a back reference.	2023-03-24	5.5	Medium
CVE-2022-20467	google - multiple products	In isBluetoothShareUri of BluetoothOppUtility.java, there is a possible incorrect file read due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-225880741	2023-03-24	5.5	Medium
CVE-2022-20499	google - multiple products	In validateForCommonR1andR2 of PasspointConfiguration.java, uncaught errors in parsing stored configs could lead to local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-246539931	2023-03-24	5.5	Medium
CVE-2022-42528	google - android	In ffa_mrd_prot of shared_mem.c, there is a possible ID due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-242203672References: N/A	2023-03-24	5.5	Medium
CVE-2023-20910	google - multiple products	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920	2023-03-24	5.5	Medium
CVE-2023-20929	google - android	In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-234442700	2023-03-24	5.5	Medium
CVE-2023-20952	google - multiple products	In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-186803518	2023-03-24	5.5	Medium
CVE-2023-20962	google - android	In getSliceEndItem of MediaVolumePreferenceController.java, there is a possible way to start foreground activity from the background due to an unsafe PendingIntent. This could lead to local information disclosure with no additional execution	2023-03-24	5.5	Medium

		privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256590210			
CVE-2023-20972	google - android	In btm_vendor_specific_evt of btm_devctl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255304665	2023-03-24	5.5	Medium
CVE-2023-20973	google - android	In btm_create_conn_cancel_complete of btm_sec.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568245	2023-03-24	5.5	Medium
CVE-2023-20974	google - android	In btm_ble_add_resolving_list_entry_complete of btm_ble_privacy.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260078907	2023-03-24	5.5	Medium
CVE-2023-20979	google - android	In BtaAvCo::GetNextSourceDataPacket of bta_av_co.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-259939364	2023-03-24	5.5	Medium
CVE-2023-20980	google - android	In btu_ble_ll_conn_param_upd_evt of btu_hcif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260230274	2023-03-24	5.5	Medium
CVE-2023-20996	google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749764	2023-03-24	5.5	Medium
CVE-2023-20997	google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749702	2023-03-24	5.5	Medium
CVE-2023-20998	google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936	2023-03-24	5.5	Medium
CVE-2023-20999	google - android	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467	2023-03-24	5.5	Medium
CVE-2023-21016	google - android	In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213905884	2023-03-24	5.5	Medium
CVE-2023-21019	google - android	In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242379731	2023-03-24	5.5	Medium
CVE-2023-21026	google - android	In updateInputChannel of WindowManagerService.java, there is a possible way to set a touchable region beyond its own SurfaceControl due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254681548	2023-03-24	5.5	Medium
CVE-2023-21029	google - android	In register of UidObserverController.java, there is a missing permission check. This could lead to local information disclosure of app usage with User execution privileges needed. User	2023-03-24	5.5	Medium

		interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-217934898			
CVE-2023-21033	google - android	In addNetwork of WifiManager.java, there is a possible way to trigger a persistent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-244713323	2023-03-24	5.5	Medium
CVE-2023-21036	google - android	In BitmapExport.java, there is a possible failure to truncate images due to a logic error in the code.Product: AndroidVersions: Android kernelAndroid ID: A-264261868References: N/A	2023-03-24	5.5	Medium
CVE-2023-1583	linux - multiple products	A NULL pointer dereference was found in io_file_bitmap_get in io_uring/filetable.c in the io_uring sub-component in the Linux Kernel. When fixed files are unregistered, some context information (file_alloc_{start,end} and alloc_hint) is not cleared. A subsequent request that has auto index selection enabled via IORING_FILE_INDEX_ALLOC can cause a NULL pointer dereference. An unprivileged user can use the flaw to cause a system crash.	2023-03-24	5.5	Medium
CVE-2023-28083	hp - integrated_lights-out_4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out.	2023-03-22	5.4	Medium
CVE-2023-21615	adobe - multiple products	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-03-22	5.4	Medium
CVE-2023-21616	adobe - multiple products	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-03-22	5.4	Medium
CVE-2023-22252	adobe - multiple products	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-03-22	5.4	Medium
CVE-2023-22253	adobe - multiple products	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-03-22	5.4	Medium
CVE-2023-22254	adobe - multiple products	Experience Manager versions 6.5.15.0 (and earlier) are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-03-22	5.4	Medium
CVE-2023-22256	adobe - multiple products	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Medium
CVE-2023-22257	adobe - multiple products	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Medium
CVE-2023-22258	adobe - multiple products	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Medium
CVE-2023-22259	adobe - multiple products	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Medium
CVE-2023-22260	adobe - multiple products	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction.	2023-03-22	5.4	Medium
CVE-2023-22261	adobe - multiple products	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could	2023-03-22	5.4	Medium

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

		Description was not properly sanitized. An attacker needs to have control over the Graphite data source in order to manipulate a function description and a Grafana admin needs to configure the data source, later a Grafana user needs to select a tampered function and hover over the description. Users may upgrade to version 8.5.22, 9.2.15 and 9.3.11 to receive a fix.			
CVE-2023-0590	linux - multiple products	A use-after-free flaw was found in qdisc_graft in net/sched/sch_api.c in the Linux Kernel due to a race problem. This flaw leads to a denial of service issue. If patch ebda44da44f6 ("net: sched: fix race condition in qdisc_graft()") not applied yet, then kernel could be affected.	2023-03-23	4.7	Medium
CVE-2023-21031	google - android	In Display::setPowerMode of HWC2.cpp, there is a possible out of bounds read due to a race condition. 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-242688355	2023-03-24	4.7	Medium
CVE-2023-20987	google - android	In btm_read_link_quality_complete of btm_acl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure over Bluetooth with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260569414	2023-03-24	4.5	Medium
CVE-2023-20988	google - android	In btm_read_rssi_complete of btm_acl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260569232	2023-03-24	4.5	Medium
CVE-2023-20992	google - android	In on_iso_link_quality_read of btm_iso_impl.h, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568750	2023-03-24	4.5	Medium
CVE-2023-20956	google - multiple products	In Import of C2SurfaceSyncObj.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-240140929	2023-03-24	4.4	Medium
CVE-2023-20968	google - android	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262235935	2023-03-24	4.4	Medium
CVE-2023-20969	google - android	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236313	2023-03-24	4.4	Medium
CVE-2023-20970	google - android	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236005	2023-03-24	4.4	Medium
CVE-2023-20977	google - android	In btm_ble_read_remote_features_complete of btm_ble_gap.cc, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure if the firmware were compromised with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254445952	2023-03-24	4.4	Medium
CVE-2023-20981	google - android	In btu_ble_rc_param_req_evt of btu_hcif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256165737	2023-03-24	4.4	Medium
CVE-2023-20982	google - android	In btm_read_tx_power_complete of btm_acl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568083	2023-03-24	4.4	Medium
CVE-2023-20983	google - android	In btm_ble_rand_enc_complete of btm_sec.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	2023-03-24	4.4	Medium

		exploitation.Product: AndroidVersions: Android-13Android ID: A-260569449			
CVE-2023-20984	google - android	In ParseBqrLinkQualityEvt of btif_bqr.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242993878	2023-03-24	4.4	Medium
CVE-2023-20986	google - android	In btm_ble_clear_resolving_list_complete of btm_ble_privacy.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255304475	2023-03-24	4.4	Medium
CVE-2023-20989	google - android	In btm_ble_write_adv_enable_complete of btm_ble_gap.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568367	2023-03-24	4.4	Medium
CVE-2023-20990	google - android	In btm_read_local_oob_complete of btm_sec.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568354	2023-03-24	4.4	Medium
CVE-2023-20991	google - android	In btm_ble_process_periodic_adv_sync_lost_evt of ble_scanner_hci_interface.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255305114	2023-03-24	4.4	Medium
CVE-2023-21006	google - android	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257030027	2023-03-24	4.4	Medium
CVE-2023-21007	google - android	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029965	2023-03-24	4.4	Medium
CVE-2023-21008	google - android	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257030100	2023-03-24	4.4	Medium
CVE-2023-21009	google - android	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029925	2023-03-24	4.4	Medium
CVE-2023-21010	google - android	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029915	2023-03-24	4.4	Medium
CVE-2023-21011	google - android	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029912	2023-03-24	4.4	Medium
CVE-2023-21012	google - android	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029812	2023-03-24	4.4	Medium
CVE-2023-21013	google - android	In forceStaDisconnection of hostapd.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: AndroidVersions: Android-13Android ID: A-256818945	2023-03-24	4.4	Medium
CVE-2023-21014	google - android	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029326	2023-03-24	4.4	Medium
CVE-2023-21025	google - android	In ufdt_local_fixup_prop of ufdt_overlay.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	2023-03-24	4.4	Medium

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

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations and their impacts.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.