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 ٢٥ يونيو إلى ١ يوليو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 25th of June to 1st of July. 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-2023-32557	trendmicro - multiple products	A path traversal vulnerability in the Trend Micro Apex One and Apex One as a Service could allow an unauthenticated attacker to upload an arbitrary file to the Management Server which could lead to remote code execution with system privileges.	2023-06-26	9.8	Critical
CVE-2023-27866	ibm - multiple products	IBM Informix JDBC Driver 4.10 and 4.50 is susceptible to remote code execution attack via JNDI injection when driver code or the application using the driver do not verify supplied LDAP URL in Connect String. IBM X-Force ID: 249511.	2023-06-28	9.8	Critical
CVE-2023-21066	google - android	In cd_CodeMsg of cd_codec.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-250100597References: N/A	2023-06-28	9.8	Critical
CVE-2023-21517	samsung - exynos	Heap out-of-bound write vulnerability in Exynos baseband prior to SMR Jun-2023 Release 1 allows remote attacker to execute arbitrary code.	2023-06-28	9.8	Critical
CVE-2023-35175	hp - laserjet_pro_mfp_m478-m479_w1a75a_firmware	Certain HP LaserJet Pro print products are potentially vulnerable to Potential Remote Code Execution and/or Elevation of Privilege via Server-Side Request Forgery (SSRF) using the Web Service Eventing model.	2023-06-30	9.8	Critical
CVE-2023-32521	trendmicro - mobile_security	A path traversal exists in a specific service dll of Trend Micro Mobile Security (Enterprise) 9.8 SP5 which could allow an unauthenticated remote attacker to delete arbitrary files.	2023-06-26	9.1	Critical
CVE-2023-3420	google - chrome	Type Confusion in V8 in Google Chrome prior to 114.0.5735.198 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-06-26	8.8	High
CVE-2023-3421	google - chrome	Use after free in Media in Google Chrome prior to 114.0.5735.198 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-06-26	8.8	High
CVE-2023-3422	google - chrome	Use after free in Guest View in Google Chrome prior to 114.0.5735.198 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-06-26	8.8	High
CVE-2023-32523	trendmicro - mobile_security	Affected versions of Trend Micro Mobile Security (Enterprise) 9.8 SP5 contain some widgets that would allow a remote user to bypass authentication and potentially chain with other vulnerabilities. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit these vulnerabilities. This is similar to, but not identical to CVE-2023-32524.	2023-06-26	8.8	High

CVE-2023-32524	trendmicro - mobile_security	Affected versions of Trend Micro Mobile Security (Enterprise) 9.8 SP5 contain some widgets that would allow a remote user to bypass authentication and potentially chain with other vulnerabilities. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit these vulnerabilities. This is similar to, but not identical to CVE-2023-32523.	2023-06-26	8.8	High
CVE-2023-32527	trendmicro - mobile_security	Trend Micro Mobile Security (Enterprise) 9.8 SP5 contains vulnerable .php files that could allow a remote attacker to execute arbitrary code on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32528.	2023-06-26	8.8	High
CVE-2023-32528	trendmicro - mobile_security	Trend Micro Mobile Security (Enterprise) 9.8 SP5 contains vulnerable .php files that could allow a remote attacker to execute arbitrary code on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32527.	2023-06-26	8.8	High
CVE-2023-32529	trendmicro - apex_central	Vulnerable modules of Trend Micro Apex Central (on-premise) contain vulnerabilities which would allow authenticated users to perform a SQL injection that could lead to remote code execution. Please note: an attacker must first obtain authentication on the target system in order to exploit these vulnerabilities. This is similar to, but not identical to CVE-2023-32530.	2023-06-26	8.8	High
CVE-2023-32530	trendmicro - apex_central	Vulnerable modules of Trend Micro Apex Central (on-premise) contain vulnerabilities which would allow authenticated users to perform a SQL injection that could lead to remote code execution. Please note: an attacker must first obtain authentication on the target system in order to exploit these vulnerabilities. This is similar to, but not identical to CVE-2023-32529.	2023-06-26	8.8	High
CVE-2022-26899	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-06-29	8.8	High
CVE-2023-22886	apache - apache-airflow-providers-jdbc	Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow JDBC Provider. Airflow JDBC Provider Connection's [Connection URL] parameters had no restrictions, which made it possible to implement RCE attacks via different type JDBC drivers, obtain airflow server permission. This issue affects Apache Airflow JDBC Provider: before 4.0.0.	2023-06-29	8.8	High
CVE-2023-35176	hp - laserjet_pro_mfp_m478-m479_w1a75a_firmware	Certain HP LaserJet Pro print products are potentially vulnerable to Buffer Overflow and/or Denial of Service when using the backup & restore feature through the embedded web service on the device.	2023-06-30	8.8	High

CVE-2023-35177	hp - laserjet_pro_mfp_m478-m479_w1a75a_firmware	Certain HP LaserJet Pro print products are potentially vulnerable to a stack-based buffer overflow related to the compact font format parser.	2023-06-30	8.8	High
CVE-2023-35178	hp - laserjet_pro_mfp_m478-m479_w1a75a_firmware	Certain HP LaserJet Pro print products are potentially vulnerable to Buffer Overflow when performing a GET request to scan jobs.	2023-06-30	8.8	High
CVE-2021-31982	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2023-07-01	8.8	High
CVE-2021-34475	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-07-01	8.8	High
CVE-2022-29146	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-06-29	8.3	High
CVE-2021-31937	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-06-28	8.2	High
CVE-2023-34418	lenovo - xclarity_administrator	A valid, authenticated LXCA user may be able to gain unauthorized access to events and other data stored in LXCA due to a SQL injection vulnerability in a specific web API.	2023-06-26	8.1	High
CVE-2023-32522	trendmicro - mobile_security	A path traversal exists in a specific dll of Trend Micro Mobile Security (Enterprise) 9.8 SP5 which could allow an authenticated remote attacker to delete arbitrary files. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2023-06-26	8.1	High
CVE-2023-28929	trendmicro - multiple products	Trend Micro Security 2021, 2022, and 2023 (Consumer) are vulnerable to a DLL Hijacking vulnerability which could allow an attacker to use a specific executable file as an execution and/or persistence mechanism which could execute a malicious program each time the executable file is started.	2023-06-26	7.8	High
CVE-2023-34144	trendmicro - multiple products	An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34145.	2023-06-26	7.8	High
CVE-2023-34145	trendmicro - multiple products	An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34144.	2023-06-26	7.8	High
CVE-2023-34146	trendmicro - multiple products	An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to specific Trend Micro agent subkeys on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34147 and CVE-2023-34148.	2023-06-26	7.8	High
CVE-2023-34147	trendmicro - multiple products	An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges and write an arbitrary value to	2023-06-26	7.8	High

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

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

		and 0e388fce7aec40992eadee654193cad345d62663 for 5.15 stable).			
CVE-2023-21518	samsung - searchwidget	Improper access control vulnerability in SearchWidget prior to version 3.3 in China models allows untrusted applications to start arbitrary activity.	2023-06-28	7.8	High
CVE-2023-3390	linux - linux_kernel	A use-after-free vulnerability was found in the Linux kernel's netfilter subsystem in net/netfilter/nf_tables_api.c. Mishandled error handling with NFT_MSG_NEWRULE makes it possible to use a dangling pointer in the same transaction causing a use-after-free vulnerability. This flaw allows a local attacker with user access to cause a privilege escalation issue. We recommend upgrading past commit 1240eb93f0616b21c675416516ff3d74798fdc97.	2023-06-28	7.8	High
CVE-2023-3117	linux - multiple products	A use-after-free flaw was found in the Netfilter subsystem of the Linux kernel when processing named and anonymous sets in batch requests, which can lead to performing arbitrary reads and writes in kernel memory. This flaw allows a local user with CAP_NET_ADMIN capability to crash or potentially escalate their privileges on the system.	2023-06-30	7.8	High
CVE-2023-20192	cisco - telepresence_video_communication_server	Multiple vulnerabilities in Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated attacker with Administrator-level read-only credentials to elevate their privileges to Administrator with read-write credentials on an affected system. Note: "Cisco Expressway Series" refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices. For more information about these vulnerabilities, see the Details section of this advisory.	2023-06-28	7.7	High
CVE-2023-2992	lenovo - nextscale_n1200_enclosure_firmware	An unauthenticated denial of service vulnerability exists in the SMM v1, SMM v2, and FPC management web server which can be triggered under crafted conditions. Rebooting SMM or FPC will restore access to the management web server.	2023-06-26	7.5	High
CVE-2023-3113	lenovo - xclarity_administrator	An unauthenticated XML external entity injection (XXE) vulnerability exists in LXCA's Common Information Model (CIM) server that could result in read-only access to specific files.	2023-06-26	7.5	High
CVE-2023-35695	trendmicro - mobile_security	A remote attacker could leverage a vulnerability in Trend Micro Mobile Security (Enterprise) 9.8 SP5 to download a particular log file which may contain sensitive information regarding the product.	2023-06-26	7.5	High
CVE-2023-26276	ibm - multiple products	IBM QRadar SIEM 7.5.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 248147.	2023-06-27	7.5	High
CVE-2023-30993	ibm - cloud_pak_for_security	IBM Cloud Pak for Security (CP4S) 1.9.0.0 through 1.9.2.0 could allow an attacker with a valid API key for one tenant to access data from another tenant's account. IBM X-Force ID: 254136.	2023-06-27	7.5	High
CVE-2023-20006	cisco - multiple products	A vulnerability in the hardware-based SSL/TLS cryptography functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series Appliances could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to an implementation error within the cryptographic functions for SSL/TLS traffic processing when they are offloaded to the hardware. An attacker could exploit this vulnerability by sending a crafted stream of SSL/TLS traffic to an affected device. A successful exploit could allow the attacker to cause an unexpected error in the hardware-based cryptography engine, which could cause the device to reload.	2023-06-28	7.5	High
CVE-2023-21180	google - android	In xmlParseTryOrFinish of parser.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261365944	2023-06-28	7.5	High
CVE-2023-21186	google - android	In LogResponse of Dns.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261079188	2023-06-28	7.5	High
CVE-2023-21193	google - android	In VideoFrame of VideoFrame.h, there is a possible abort due to an integer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-233006499	2023-06-28	7.5	High
CVE-2023-21197	google - android	In btm_acl_process_sca_cmpl_pkt of btm_acl.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure with no additional	2023-06-28	7.5	High

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

		vulnerability. This is similar to, but not identical to CVE-2023-32554.			
CVE-2023-1295	linux - linux_kernel	A time-of-check to time-of-use issue exists in io_uring subsystem's IORING_OP_CLOSE operation in the Linux kernel's versions 5.6 - 5.11 (inclusive), which allows a local user to elevate their privileges to root. Introduced in b5dba59e0cf7e2cc4d3b3b1ac5fe81ddf21959eb, patched in 9eac1904d3364254d622bf2c771c4f85cd435fc2, backported to stable in 788d0824269bef539fe31a785b1517882eafed93.	2023-06-28	7	High
CVE-2023-21513	samsung - multiple products	Improper privilege management vulnerability in CC Mode prior to SMR Jun-2023 Release 1 allows physical attackers to manipulate device to operate in way that results in unexpected behavior in CC Mode under specific condition.	2023-06-28	6.8	Medium
CVE-2023-2290	lenovo - thinkpad_e14_firmware	A potential vulnerability in the LenovoFlashDeviceInterface SMI handler may allow an attacker with local access and elevated privileges to execute arbitrary code.	2023-06-26	6.7	Medium
CVE-2023-21146	google - android	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-239867994References: N/A	2023-06-28	6.7	Medium
CVE-2023-21151	google - android	In the Google BMS kernel module, 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-265149414References: N/A	2023-06-28	6.7	Medium
CVE-2023-21153	google - android	In Do_AIMS_SET_CALL_WAITING of imsservice.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-264259730References: N/A	2023-06-28	6.7	Medium
CVE-2023-21157	google - android	In encode of wlandata.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-263783137References: N/A	2023-06-28	6.7	Medium
CVE-2023-21159	google - android	In Parse of simdata.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-263783565References: N/A	2023-06-28	6.7	Medium
CVE-2023-21161	google - android	In Parse of simdata.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-263783702References: N/A	2023-06-28	6.7	Medium
CVE-2023-21171	google - android	In verifyInputEvent of InputDispatcher.cpp, there is a possible way to conduct click fraud due to side channel information disclosure. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261085213	2023-06-28	6.7	Medium
CVE-2023-21203	google - android	In startWpsPbcInternal of sta_iface.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262246082	2023-06-28	6.7	Medium
CVE-2023-21207	google - android	In initiateTdlsSetupInternal of sta_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236670	2023-06-28	6.7	Medium
CVE-2023-21209	google - android	In multiple functions of sta_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. 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-262236273	2023-06-28	6.7	Medium
CVE-2023-21222	google - android	In load_dt_data of storage.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:	2023-06-28	6.7	Medium

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

		Administrator user, including the creation and deletion of user labels.			
CVE-2023-2993	lenovo - nextscale_n1200_enclosure_firmware	A valid, authenticated user with limited privileges may be able to use specifically crafted web management server API calls to execute a limited number of commands on SMM v1, SMM v2, and FPC that the user does not normally have sufficient privileges to execute.	2023-06-26	6.3	Medium
CVE-2023-32531	trendmicro - apex_central	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. This is similar to, but not identical to CVE-2023-32532 through 32535.	2023-06-26	6.1	Medium
CVE-2023-32532	trendmicro - apex_central	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. This is similar to, but not identical to CVE-2023-32531 through 32535.	2023-06-26	6.1	Medium
CVE-2023-32533	trendmicro - apex_central	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. This is similar to, but not identical to CVE-2023-32531 through 32535.	2023-06-26	6.1	Medium
CVE-2023-32534	trendmicro - apex_central	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. This is similar to, but not identical to CVE-2023-32531 through 32535.	2023-06-26	6.1	Medium
CVE-2023-32535	trendmicro - apex_central	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. This is similar to, but not identical to CVE-2023-32531 through 32534.	2023-06-26	6.1	Medium
CVE-2023-32339	ibm - multiple products	IBM Business Automation Workflow is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 255587.	2023-06-27	6.1	Medium
CVE-2023-20119	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager; Cisco Secure Email Gateway, formerly Cisco Email Security Appliance (ESA); and Cisco Secure Web Appliance, formerly Cisco Web Security Appliance (WSA), could allow a remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory.	2023-06-28	6.1	Medium
CVE-2023-20120	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager; Cisco Secure Email Gateway, formerly Cisco Email Security Appliance (ESA); and Cisco Secure Web Appliance, formerly Cisco Web Security Appliance (WSA), could allow a remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. For more information about these vulnerabilities, see the Details section of this advisory.	2023-06-28	6.1	Medium
CVE-2023-20116	cisco - multiple products	A vulnerability in the Administrative XML Web Service (AXL) API of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of user-supplied	2023-06-28	5.7	Medium

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

		privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-245517503			
CVE-2023-21200	google - android	In on_remove_iso_data_path of btm_iso_impl.h, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-236688764	2023-06-28	5.5	Medium
CVE-2023-21205	google - android	In startWpsPinDisplayInternal of sta_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262245376	2023-06-28	5.5	Medium
CVE-2023-21211	google - android	In multiple files, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262235998	2023-06-28	5.5	Medium
CVE-2023-21237	google - android	In applyRemoteView of NotificationContentInflater.java, there is a possible way to hide foreground service notification due to misleading or insufficient UI. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-251586912	2023-06-28	5.5	Medium
CVE-2023-3355	linux - multiple products	A NULL pointer dereference flaw was found in the Linux kernel's drivers/gpu/drm/msm/msm_gem_submit.c code in the submit_lookup_cmds function, which fails because it lacks a check of the return value of kmalloc(). This issue allows a local user to crash the system.	2023-06-28	5.5	Medium
CVE-2023-3357	linux - multiple products	A NULL pointer dereference flaw was found in the Linux kernel AMD Sensor Fusion Hub driver. This flaw allows a local user to crash the system.	2023-06-28	5.5	Medium
CVE-2023-3358	linux - multiple products	A null pointer dereference was found in the Linux kernel's Integrated Sensor Hub (ISH) driver. This issue could allow a local user to crash the system.	2023-06-28	5.5	Medium
CVE-2023-3359	linux - multiple products	An issue was discovered in the Linux kernel brcm_nvram_parse in drivers/nvmem/brcm_nvram.c. Lacks for the check of the return value of kzalloc() can cause the NULL Pointer Dereference.	2023-06-28	5.5	Medium
CVE-2023-32536	trendmicro - apex_central	Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32537.	2023-06-26	5.4	Medium
CVE-2023-32537	trendmicro - apex_central	Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32536.	2023-06-26	5.4	Medium
CVE-2023-32604	trendmicro - apex_central	Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues. Please note: an attacker must first obtain authentication to Apex Central on the target system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32605.	2023-06-26	5.4	Medium
CVE-2023-32605	trendmicro - apex_central	Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validation and sanitization issues.	2023-06-26	5.4	Medium

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

		agent authentication token. All versions before 7.14.3 are affected.			
CVE-2023-21195	google - android	In btm_ble_periodic_adv_sync_tx_rcvd of btm_ble_gap.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure over Bluetooth, if the firmware were compromised with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-233879420	2023-06-28	4.5	Medium
CVE-2023-21202	google - android	In btm_delete_stored_link_key_complete 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 over Bluetooth with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568359	2023-06-28	4.5	Medium
CVE-2023-21148	google - android	In BuildSetConfig of protocolimsbuilder.cpp, there is a possible out of bounds read due to a missing null check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-263783657References: N/A	2023-06-28	4.4	Medium
CVE-2023-21150	google - android	In handle_set_parameters_ctrl of hal_socket.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-267312009References: N/A	2023-06-28	4.4	Medium
CVE-2023-21154	google - android	In StoreAdbSerialNumber of protocolmiscbuilder.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-263783910References: N/A	2023-06-28	4.4	Medium
CVE-2023-21156	google - android	In BuildGetRadioNode of protocolmiscbulider.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure from the modem with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-264540759References: N/A	2023-06-28	4.4	Medium
CVE-2023-21158	google - android	In encode of miscdata.cpp, 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 kernelAndroid ID: A-263783635References: N/A	2023-06-28	4.4	Medium
CVE-2023-21169	google - android	In inviteInternal of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-274443441	2023-06-28	4.4	Medium
CVE-2023-21170	google - android	In executeSetClientTarget of ComposerCommandEngine.h, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-252764410	2023-06-28	4.4	Medium
CVE-2023-21176	google - android	In list_key_entries of utils.rs, there is a possible way to disable user credentials due to resource exhaustion. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-222287335	2023-06-28	4.4	Medium
CVE-2023-21181	google - android	In btm_ble_update_inq_result of btm_ble_gap.cc, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-264880969	2023-06-28	4.4	Medium
CVE-2023-21182	google - android	In Exynos_parsing_user_data_registered_itu_t_t35 of VendorVideoAPI.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-252764175	2023-06-28	4.4	Medium
CVE-2023-21188	google - android	In btm_ble_update_inq_result of btm_ble_gap.cc, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-264624283	2023-06-28	4.4	Medium

CVE-2023-21194	google - android	In gatt_dbg_op_name of gatt_utils.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-260079141	2023-06-28	4.4	Medium
CVE-2023-21196	google - android	In btm_ble_batchscan_filter_track_adv_vse_cback of btm_ble_batchscan.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-261857395	2023-06-28	4.4	Medium
CVE-2023-21199	google - android	In btu_ble_proc_ltk_req 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-254445961	2023-06-28	4.4	Medium
CVE-2023-21204	google - android	In multiple files, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wifi server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262246231	2023-06-28	4.4	Medium
CVE-2023-21206	google - android	In initiateVenueUrlAnqpQueryInternal of sta_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262245630	2023-06-28	4.4	Medium
CVE-2023-21208	google - android	In setCountryCodeInternal of sta_iface.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262245254	2023-06-28	4.4	Medium
CVE-2023-21210	google - android	In initiateHs20IconQueryInternal of sta_iface.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236331	2023-06-28	4.4	Medium
CVE-2023-21212	google - android	In multiple files, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wifi server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236031	2023-06-28	4.4	Medium
CVE-2023-21213	google - android	In initiateTdlsTeardownInternal of sta_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the wifi server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262235951	2023-06-28	4.4	Medium
CVE-2023-21214	google - android	In addGroupWithConfigInternal of p2p_iface.cpp, there is a possible out of bounds read due to unsafe deserialization. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262235736	2023-06-28	4.4	Medium
CVE-2023-35798	apache - multiple products	Input Validation vulnerability in Apache Software Foundation Apache Airflow ODBC Provider, Apache Software Foundation Apache Airflow MSSQL Provider.This vulnerability is considered low since it requires DAG code to use `get_sqlalchemy_connection` and someone with access to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provider: before 3.4.1. It is recommended to upgrade to a version that is not affected	2023-06-27	4.3	Medium
CVE-2023-36002	proofpoint - insider_threat_management_server	A missing authorization check in multiple URL validation endpoints of the Insider Threat Management Server enables an anonymous attacker on an adjacent network to smuggle content via DNS lookups. All versions before 7.14.3 are affected.	2023-06-27	4.3	Medium
CVE-2023-26273	ibm - multiple products	IBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. IBM X-Force ID: 248134.	2023-06-27	4.3	Medium
CVE-2021-42307	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2023-07-01	4.3	Medium
CVE-2023-21178	google - android	In installKey of KeyUtil.cpp, there is a possible failure of file encryption due to a race condition. This could lead to local	2023-06-28	4.1	Medium

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

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

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