الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

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

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

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 2nd of July to 8th 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**

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 ٢ يوليو إلى ٨ 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**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-35797	apache - apache-airflow-providers-apache-hive	Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow Hive Provider. This issue affects Apache Airflow Apache Hive Provider: before 6.1.1. Before version 6.1.1 it was possible to bypass the security check to RCE via principal parameter. For this to be exploited it requires access to modifying the connection details. It is recommended updating provider version to 6.1.1 in order to avoid this vulnerability.	2023-07-03	9.8	Critical
CVE-2023-21631	qualcomm - 315_5g_firmware	Weak Configuration due to improper input validation in Modem while processing LTE security mode command message received from network.	2023-07-04	9.8	Critical
CVE-2021-46890	huawei - multiple products	Vulnerability of incomplete read and write permission verification in the GPU module. Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.	2023-07-05	9.8	Critical
CVE-2021-46891	huawei - multiple products	Vulnerability of incomplete read and write permission verification in the GPU module. Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.	2023-07-05	9.8	Critical
CVE-2021-46894	huawei - multiple products	Use After Free (UAF) vulnerability in the uinput module.Successful exploitation of this vulnerability may lead to kernel privilege escalation.	2023-07-06	9.8	Critical
CVE-2022-48510	huawei - multiple products	Input verification vulnerability in the AMS module. Successful exploitation of this vulnerability will cause unauthorized operations.	2023-07-06	9.8	Critical
CVE-2022-48511	huawei - multiple products	Use After Free (UAF) vulnerability in the audio PCM driver module under special conditions. Successful exploitation of this vulnerability may cause audio features to perform abnormally.	2023-07-06	9.8	Critical
CVE-2022-48512	huawei - multiple products	Use After Free (UAF) vulnerability in the Vdecoderservice service. Successful exploitation of this vulnerability may cause the image decoding feature to perform abnormally.	2023-07-06	9.8	Critical
CVE-2022-48513	huawei - multiple products	Vulnerability of identity verification being bypassed in the Gallery module. Successful exploitation of this vulnerability may cause out-of-bounds access.	2023-07-06	9.8	Critical
CVE-2023-37242	huawei - multiple products	Vulnerability of commands from the modem being intercepted in the atcmdserver module. Attackers may exploit this vulnerability to rewrite the non-volatile random-access memory (NVRAM), or facilitate the exploitation of other vulnerabilities.	2023-07-06	9.8	Critical
CVE-2023-29381	zimbra - multiple products	An issue in Zimbra Collaboration (ZCS) v.8.8.15 and v.9.0 allows a remote attacker to escalate privileges and obtain sensitive information via the password and 2FA parameters.	2023-07-06	9.8	Critical
CVE-2023-29382	zimbra - multiple products	An issue in Zimbra Collaboration ZCS v.8.8.15 and v.9.0 allows an attacker to execute arbitrary code via the sfdc_preauth.jsp component.	2023-07-06	9.8	Critical
CVE-2023-3455	huawei - multiple products	Key management vulnerability on system. Successful exploitation of this vulnerability may affect service availability and integrity.	2023-07-05	9.1	Critical

CVE-2023-37240	huawei - multiple products	Vulnerability of missing input length verification in the distributed file system. Successful exploitation of this vulnerability may cause out-of-bounds read.	2023-07-06	9.1	Critical
CVE-2023-37245	huawei - multiple products	Buffer overflow vulnerability in the modem pinctrl module. Successful exploitation of this vulnerability may affect the integrity and availability of the modem.	2023-07-06	9.1	Critical
CVE-2023-34192	zimbra - multiple products	Cross Site Scripting vulnerability in Zimbra ZCS v.8.8.15 allows a remote authenticated attacker to execute arbitrary code via a crafted script to the /h/autoSaveDraft function.	2023-07-06	9	Critical
CVE-2023-3314	trellix - enterprise_security_manager	A vulnerability arises out of a failure to comprehensively sanitize the processing of a zip file(s). Incomplete neutralization of external commands used to control the process execution of the .zip application allows an authorized user to obtain control of the .zip application to execute arbitrary commands or obtain elevation of system privileges.	2023-07-03	8.8	High
CVE-2023-37201	mozilla - multiple products	An attacker could have triggered a use-after-free condition when creating a WebRTC connection over HTTPS. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13.	2023-07-05	8.8	High
CVE-2023-37202	mozilla - multiple products	Cross-compartment wrappers wrapping a scripted proxy could have caused objects from other compartments to be stored in the main compartment resulting in a use-after-free. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13.	2023-07-05	8.8	High
CVE-2023-37209	mozilla - firefox	A use-after-free condition existed in `NotifyOnHistoryReload` where a `LoadingSessionHistoryEntry` object was freed and a reference to that object remained. This resulted in a potentially exploitable condition when the reference to that object was later reused. This vulnerability affects Firefox < 115.	2023-07-05	8.8	High
CVE-2023-37211	mozilla - multiple products	Memory safety bugs present in Firefox 114, Firefox ESR 102.12, and Thunderbird 102.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13.	2023-07-05	8.8	High
CVE-2023-37212	mozilla - firefox	Memory safety bugs present in Firefox 114. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 115.	2023-07-05	8.8	High
CVE-2023-34193	zimbra - multiple products	File Upload vulnerability in Zimbra ZCS 8.8.15 allows an authenticated privileged user to execute arbitrary code and obtain sensitive information via the ClientUploader function.	2023-07-06	8.8	High
CVE-2023-2974	redhat - build_of_quarkus	A vulnerability was found in quarkus-core. This vulnerability occurs because the TLS protocol configured with quarkus.http.ssl.protocols is not enforced, and the client can force the selection of the weaker supported TLS protocol.	2023-07-04	8.1	High
CVE-2023-35975	arubanetworks - multiple products	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system.	2023-07-05	8.1	High
CVE-2023-3313	trellix - enterprise_security_manager	An OS common injection vulnerability exists in the ESM certificate API, whereby incorrectly neutralized special elements may have allowed an unauthorized user to execute system command injection for the purpose of privilege escalation or to execute arbitrary commands.	2023-07-03	7.8	High
CVE-2023-3438	trellix - move	An unquoted Windows search path vulnerability existed in the install the MOVE 4.10.x and earlier Windows install service (mvagtsce.exe). The misconfiguration allowed an unauthorized local user to insert arbitrary code into the unquoted service path to obtain privilege escalation and stop antimalware services.	2023-07-03	7.8	High
CVE-2023-20773	google - multiple products	In vow, there is a possible escalation of privilege 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. Patch ID: ALPS07611449; Issue ID: ALPS07441735.	2023-07-04	7.8	High
CVE-2023-21633	qualcomm - apq8064au_firmware	Memory Corruption in Linux while processing QcRilRequestImsRegisterMultiIdentityMessage request.	2023-07-04	7.8	High
CVE-2023-21635	qualcomm - aqt1000_firmware	Memory Corruption in Data Network Stack & Connectivity when sim gets detected on telephony.	2023-07-04	7.8	High
CVE-2023-21637	qualcomm - aqt1000_firmware	Memory corruption in Linux while calling system configuration APIs.	2023-07-04	7.8	High
CVE-2023-21638	qualcomm - aqt1000_firmware	Memory corruption in Video while calling APIs with different instance ID than the one received in initialization.	2023-07-04	7.8	High

CVE-2023-21639	qualcomm - aqt1000_firmware	Memory corruption in Audio while processing sva_model_serializer using memory size passed by HIDL client.	2023-07-04	7.8	High
CVE-2023-21640	qualcomm - fastconnect_6900_firmware	Memory corruption in Linux when the file upload API is called with parameters having large buffer.	2023-07-04	7.8	High
CVE-2023-21641	qualcomm - fastconnect_6900_firmware	An app with non-privileged access can change global system brightness and cause undesired system behavior.	2023-07-04	7.8	High
CVE-2023-21672	qualcomm - fastconnect_6700_firmware	Memory corruption in Audio while running concurrent tunnel playback or during concurrent audio tunnel recording sessions.	2023-07-04	7.8	High
CVE-2023-22386	qualcomm - ar8035_firmware	Memory Corruption in WLAN HOST while processing WLAN FW request to allocate memory.	2023-07-04	7.8	High
CVE-2023-22387	qualcomm - 315_5g_iot_firmware	Arbitrary memory overwrite when VM gets compromised in TX write leading to Memory Corruption.	2023-07-04	7.8	High
CVE-2023-22667	qualcomm - 315_5g_iot_firmware	Memory Corruption in Audio while allocating the ion buffer during the music playback.	2023-07-04	7.8	High
CVE-2023-24851	qualcomm - ar8035_firmware	Memory Corruption in WLAN HOST while parsing QMI response message from firmware.	2023-07-04	7.8	High
CVE-2023-24854	qualcomm - ar8035_firmware	Memory Corruption in WLAN HOST while parsing QMI WLAN Firmware response message.	2023-07-04	7.8	High
CVE-2023-28541	qualcomm - aqt1000_firmware	Memory Corruption in Data Modem while processing DMA buffer release event about CFR data.	2023-07-04	7.8	High
CVE-2023-28542	qualcomm - 315_5g_iot_firmware	Memory Corruption in WLAN HOST while fetching TX status information.	2023-07-04	7.8	High
CVE-2023-37208	mozilla - multiple products	When opening Diagcab files, Firefox did not warn the user that these files may contain malicious code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13.	2023-07-05	7.8	High
CVE-2023-37203	mozilla - firefox	Insufficient validation in the Drag and Drop API in conjunction with social engineering, may have allowed an attacker to trick end-users into creating a shortcut to local system files. This could have been leveraged to execute arbitrary code. This vulnerability affects Firefox < 115.	2023-07-05	7.8	High
CVE-2023-31248	linux - linux_kernel	Linux Kernel nftables Use-After-Free Local Privilege Escalation Vulnerability; `nft_chain_lookup_byid()` failed to check whether a chain was active and CAP_NET_ADMIN is in any user or network namespace	2023-07-05	7.8	High
CVE-2023-35001	linux - linux_kernel	Linux Kernel nftables Out-Of-Bounds Read/Write Vulnerability; nft_byteorder poorly handled vm register contents when CAP_NET_ADMIN is in any user or network namespace	2023-07-05	7.8	High
CVE-2023-30644	samsung - multiple products	Stack out of bound write vulnerability in CdmaSmsParser of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code.	2023-07-06	7.8	High
CVE-2023-30645	samsung - multiple products	Heap out of bound write vulnerability in IpcRxIncomingCBMsg of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code.	2023-07-06	7.8	High
CVE-2023-30646	samsung - multiple products	Heap out of bound write vulnerability in BroadcastSmsConfig of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code.	2023-07-06	7.8	High
CVE-2023-30647	samsung - multiple products	Heap out of bound write vulnerability in IpcRxUsimPhoneBookCapa of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code.	2023-07-06	7.8	High
CVE-2023-30649	samsung - multiple products	Heap out of bound write vulnerability in RmtUimNeedApdu of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code.	2023-07-06	7.8	High
CVE-2023-30650	samsung - multiple products	Out of bounds read and write in callrunTspCmd of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code.	2023-07-06	7.8	High
CVE-2023-30651	samsung - multiple products	Out of bounds read and write in callgetTspsysfs of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code.	2023-07-06	7.8	High
CVE-2023-30652	samsung - multiple products	Out of bounds read and write in callrunTspCmdNoRead of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code.	2023-07-06	7.8	High
CVE-2023-30653	samsung - multiple products	Out of bounds read and write in enableTspDevice of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code.	2023-07-06	7.8	High
CVE-2023-30655	samsung - multiple products	Improper input validation vulnerability in SCEPProfile prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities.	2023-07-06	7.8	High
CVE-2023-30656	samsung - multiple products	Improper input validation vulnerability in LSOItemData prior to SMR Jul-2023 Release 1 allows attackers to launch certain activities.	2023-07-06	7.8	High
CVE-2023-30657	samsung - multiple products	Improper input validation vulnerability in EnhancedAttestationResult prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities.	2023-07-06	7.8	High

CVE-2023-30658	samsung - multiple products	Improper input validation vulnerability in DataProfile prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities.	2023-07-06	7.8	High
CVE-2023-30659	samsung - multiple products	Improper input validation vulnerability in Transaction prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities.	2023-07-06	7.8	High
CVE-2023-30663	samsung - multiple products	Improper input validation vulnerability in OemPersonalizationSetLock in libsec-ril prior to SMR Jul-2023 Release 1 allows local attackers to cause an Out-Of-Bounds write.	2023-07-06	7.8	High
CVE-2023-30664	samsung - multiple products	Improper input validation vulnerability in RegisteredMSISDN prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities.	2023-07-06	7.8	High
CVE-2023-30666	samsung - multiple products	Improper input validation vulnerability in DoOemImeiSetPreconfig in libsec-ril prior to SMR Jul-2023 Release 1 allows local attackers to cause an Out-Of-Bounds write.	2023-07-06	7.8	High
CVE-2023-30668	samsung - multiple products	Out-of-bounds Write in BuildOemSecureSimLockResponse of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code.	2023-07-06	7.8	High
CVE-2023-30669	samsung - multiple products	Out-of-bounds Write in DoOemFactorySendFactoryTestResult of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code.	2023-07-06	7.8	High
CVE-2023-30670	samsung - multiple products	Out-of-bounds Write in BuildIpcFactoryDeviceTestEvent of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code.	2023-07-06	7.8	High
CVE-2021-46893	huawei - multiple products	Vulnerability of unstrict data verification and parameter check. Successful exploitation of this vulnerability may affect integrity.	2023-07-05	7.5	High
CVE-2023-3089	redhat - openshift_container_platform	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated.	2023-07-05	7.5	High
CVE-2023-35979	arubanetworks - multiple products	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller.	2023-07-05	7.5	High
CVE-2021-46892	huawei - multiple products	Encryption bypass vulnerability in Maintenance mode. Successful exploitation of this vulnerability may affect service confidentiality.	2023-07-06	7.5	High
CVE-2022-48507	huawei - multiple products	Vulnerability of identity verification being bypassed in the storage module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-07-06	7.5	High
CVE-2022-48508	huawei - multiple products	Inappropriate authorization vulnerability in the system apps. Successful exploitation of this vulnerability may affect service integrity.	2023-07-06	7.5	High
CVE-2022-48514	huawei - harmonyos	The Sepolicy module has inappropriate permission control on the use of Netlink.Successful exploitation of this vulnerability may affect confidentiality.	2023-07-06	7.5	High
CVE-2022-48515	huawei - multiple products	Vulnerability of inappropriate permission control in Nearby. Successful exploitation of this vulnerability may affect service confidentiality.	2023-07-06	7.5	High
CVE-2022-48516	huawei - multiple products	Vulnerability that a unique value can be obtained by a third-party app in the DSoftBus module. Successful exploitation of this vulnerability will affect confidentiality.	2023-07-06	7.5	High
CVE-2022-48517	huawei - multiple products	Unauthorized service access vulnerability in the DSoftBus module. Successful exploitation of this vulnerability will affect availability.	2023-07-06	7.5	High
CVE-2022-48519	huawei - multiple products	Unauthorized access vulnerability in the SystemUI module. Successful exploitation of this vulnerability may affect confidentiality.	2023-07-06	7.5	High
CVE-2022-48520	huawei - multiple products	Unauthorized access vulnerability in the SystemUI module. Successful exploitation of this vulnerability may affect confidentiality.	2023-07-06	7.5	High
CVE-2023-1691	huawei - multiple products	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally.	2023-07-06	7.5	High
CVE-2023-1695	huawei - multiple products	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally.	2023-07-06	7.5	High
CVE-2023-34164	huawei - multiple products	Vulnerability of incomplete input parameter verification in the communication framework module. Successful exploitation of this vulnerability may affect availability.	2023-07-06	7.5	High
CVE-2023-37239	huawei - multiple products	Format string vulnerability in the distributed file system. Attackers who bypass the selinux permission can exploit this vulnerability to crash the program.	2023-07-06	7.5	High
CVE-2023-37241	huawei - multiple products	Input verification vulnerability in the WMS API. Successful exploitation of this vulnerability may cause the device to restart.	2023-07-06	7.5	High
CVE-2023-20899	vmware - sd-wan_edge_firmware	VMware SD-WAN (Edge) contains a bypass authentication vulnerability. An unauthenticated attacker can download the Diagnostic bundle of the application under VMware SD-WAN Management.	2023-07-06	7.5	High

CVE-2023-35972	arubanetworks - multiple products	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.	2023-07-05	7.2	High
CVE-2023-35973	arubanetworks - multiple products	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	2023-07-05	7.2	High
CVE-2023-35974	arubanetworks - multiple products	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	2023-07-05	7.2	High
CVE-2023-30643	samsung - multiple products	Missing authentication vulnerability in Galaxy Themes Service prior to SMR Jul-2023 Release 1 allows local attackers to delete arbitrary non-preloaded applications.	2023-07-06	7.1	High
CVE-2023-21629	qualcomm - 315_5g_firmware	Memory Corruption in Modem due to double free while parsing the PKCS15 sim files.	2023-07-04	6.8	Medium
CVE-2023-20753	google - multiple products	In rpmb, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07460390; Issue ID: ALPS07588667.	2023-07-04	6.7	Medium
CVE-2023-20754	google - multiple products	In keyinstall, 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. Patch ID: ALPS07563028; Issue ID: ALPS07588343.	2023-07-04	6.7	Medium
CVE-2023-20755	google - multiple products	In keyinstall, 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. Patch ID: ALPS07510064; Issue ID: ALPS07509605.	2023-07-04	6.7	Medium
CVE-2023-20756	google - multiple products	In keyinstall, 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. Patch ID: ALPS07510064; Issue ID: ALPS07549928.	2023-07-04	6.7	Medium
CVE-2023-20757	google - multiple products	In cmdq, 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. Patch ID: ALPS07636133; Issue ID: ALPS07636133.	2023-07-04	6.7	Medium
CVE-2023-20760	google - multiple products	In apu, 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. Patch ID: ALPS07629578; Issue ID: ALPS07629578.	2023-07-04	6.7	Medium
CVE-2023-20761	google - multiple products	In ril, 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. Patch ID: ALPS07628604; Issue ID: ALPS07628582.	2023-07-04	6.7	Medium
CVE-2023-20766	google - multiple products	In gps, 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. Patch ID: ALPS07573237; Issue ID: ALPS07573202.	2023-07-04	6.7	Medium
CVE-2023-20767	google - multiple products	In pqframework, 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. Patch ID: ALPS07629585; Issue ID: ALPS07629584.	2023-07-04	6.7	Medium
CVE-2023-20768	google - multiple products	In ion, there is a possible out of bounds read due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560720; Issue ID: ALPS07559800.	2023-07-04	6.7	Medium
CVE-2023-20772	google - multiple products	In vow, there is a possible escalation of privilege 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. Patch ID: ALPS07441796; Issue ID: ALPS07441796.	2023-07-04	6.7	Medium
CVE-2023-20774	google - multiple products	In display, 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. Patch ID: ALPS07292228; Issue ID: ALPS07292228.	2023-07-04	6.7	Medium

CVE-2023-20775	google - multiple products	In display, 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. Patch ID: ALPS07978760; Issue ID: ALPS07363410.	2023-07-04	6.7	Medium
CVE-2023-37207	mozilla - multiple products	A website could have obscured the fullscreen notification by using a URL with a scheme handled by an external program, such as a mailto URL. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13.	2023-07-05	6.5	Medium
CVE-2023-37204	mozilla - firefox	A website could have obscured the fullscreen notification by using an option element by introducing lag via an expensive computational function. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 115.	2023-07-05	6.5	Medium
CVE-2023-37205	mozilla - firefox	The use of RTL Arabic characters in the address bar may have allowed for URL spoofing. This vulnerability affects Firefox < 115.	2023-07-05	6.5	Medium
CVE-2023-37206	mozilla - firefox	Uploading files which contain symlinks may have allowed an attacker to trick a user into submitting sensitive data to a malicious website. This vulnerability affects Firefox < 115.	2023-07-05	6.5	Medium
CVE-2023-37210	mozilla - firefox	A website could prevent a user from exiting full-screen mode via alert and prompt calls. This could lead to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 115.	2023-07-05	6.5	Medium
CVE-2023-3482	mozilla - firefox	When Firefox is configured to block storage of all cookies, it was still possible to store data in localstorage by using an iframe with a source of 'about:blank'. This could have led to malicious websites storing tracking data without permission. This vulnerability affects Firefox < 115.	2023-07-05	6.5	Medium
CVE-2023-35976	arubanetworks - multiple products	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level.	2023-07-05	6.5	Medium
CVE-2023-35977	arubanetworks - multiple products	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level.	2023-07-05	6.5	Medium
CVE-2023-30674	samsung - internet	Improper configuration in Samsung Internet prior to version 21.0.0.41 allows attacker to bypass SameSite Cookie.	2023-07-06	6.5	Medium
CVE-2023-20771	google - android	In display, there is a possible memory corruption 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. Patch ID: ALPS07671046; Issue ID: ALPS07671046.	2023-07-04	6.4	Medium
CVE-2023-35971	arubanetworks - multiple products	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	2023-07-05	6.1	Medium
CVE-2023-35978	arubanetworks - multiple products	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.	2023-07-05	6.1	Medium
CVE-2023-33335	sophos - iview	Cross Site Scripting (XSS) in Sophos Sophos iView (The EOL was December 31st 2020) in grpname parameter that allows arbitrary script to be executed.	2023-07-05	6.1	Medium
CVE-2022-48509	huawei - multiple products	Race condition vulnerability due to multi-thread access to mutually exclusive resources in Huawei Share. Successful exploitation of this vulnerability may cause the program to exit abnormally.	2023-07-06	5.9	Medium
CVE-2023-21624	qualcomm - fastconnect_6700_firmware	Information disclosure in DSP Services while loading dynamic module.	2023-07-04	5.5	Medium
CVE-2023-30642	samsung - multiple products	Improper privilege management vulnerability in Galaxy Themes Service prior to SMR Jul-2023 Release 1 allows local attackers to call privilege function.	2023-07-06	5.5	Medium
CVE-2023-30648	samsung - multiple products	Stack out-of-bounds write vulnerability in IpcRxImeiUpdateImeiNoti of RILD priro to SMR Jul-2023 Release 1 cause a denial of service on the system.	2023-07-06	5.5	Medium
CVE-2023-30660	samsung - multiple products	Exposure of Sensitive Information vulnerability in getDefaultChipId in UwbAospAdapterService prior to SMR Jul-2023 Release 1 allows local attackers to access the UWB chipset Identifier.	2023-07-06	5.5	Medium
CVE-2023-30661	samsung - multiple products	Exposure of Sensitive Information vulnerability in getChipInfos in UwbAospAdapterService prior to SMR Jul-2023 Release 1 allows local attackers to access the UWB chipset Identifier.	2023-07-06	5.5	Medium

CVE-2023-30662	samsung - multiple products	Exposure of Sensitive Information vulnerability in getChipIds in UwbAospAdapterService prior to SMR Jul-2023 Release 1 allows local attackers to access the UWB chipset Identifier.	2023-07-06	5.5	Medium
CVE-2023-30671	samsung - multiple products	Logic error in package installation via adb command prior to SMR Jul-2023 Release 1 allows local attackers to downgrade installed application.	2023-07-06	5.5	Medium
CVE-2023-30672	samsung - smart_switch_pc	Improper privilege management vulnerability in Samsung Smart Switch for Windows Installer prior to version 4.3.23043_3 allows attackers to cause permanent DoS via directory junction.	2023-07-06	5.5	Medium
CVE-2023-30673	samsung - smart_switch_pc	Improper validation of integrity check vulnerability in Smart Switch PC prior to version 4.3.23052_1 allows local attackers to delete arbitrary directory using directory junction.	2023-07-06	5.5	Medium
CVE-2023-30675	samsung - pass	Improper authentication in Samsung Pass prior to version 4.2.03.1 allows local attacker to access stored account information when Samsung Wallet is not installed.	2023-07-06	5.5	Medium
CVE-2023-30678	samsung - calendar	Potential zip path traversal vulnerability in Calendar application prior to version 12.4.07.15 in Android 13 allows attackers to write arbitrary file.	2023-07-06	5.5	Medium
CVE-2022-48518	huawei - multiple products	Vulnerability of signature verification in the iaware system being initialized later than the time when the system broadcasts are sent. Successful exploitation of this vulnerability may cause malicious apps to start upon power-on by spoofing the package names of apps in the startup trustlist, which affects system performance.	2023-07-06	5.5	Medium
CVE-2023-37454	linux - linux_kernel	An issue was discovered in the Linux kernel through 6.4.2. A crafted UDF filesystem image causes a use-after-free write operation in the udf_put_super and udf_close_lvid functions in fs/udf/super.c.	2023-07-06	5.5	Medium
CVE-2023-35890	ibm - multiple products	IBM WebSphere Application Server 8.5 and 9.0 could provide weaker than expected security, caused by the improper encoding in a local configuration file. IBM X-Force ID: 258637.	2023-07-07	5.5	Medium
CVE-2023-34197	zohocorp - multiple products	Zoho ManageEngine ServiceDesk Plus before 14202, ServiceDesk Plus MSP before 14300, and SupportCenter Plus before 14300 have a privilege escalation vulnerability in the Release module that allows unprivileged users to access the Reminders of a release ticket and make modifications.	2023-07-07	5.4	Medium
CVE-2023-37308	zohocorp - multiple products	Zoho ManageEngine ADAudit Plus before 7100 allows XSS via the username field.	2023-07-07	5.4	Medium
CVE-2021-39014	ibm - multiple products	IBM Cloud Object System 3.15.8.97 is vulnerable to stored 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: 213650.	2023-07-07	5.4	Medium
CVE-2023-34150	apache - any23	** UNSUPPPORTED WHEN ASSIGNED ** ** UNSUPPORTED WHEN ASSIGNED ** Use of TikaEncodingDetector in Apache Any23 can cause excessive memory usage.	2023-07-05	5.3	Medium
CVE-2023-37238	huawei - multiple products	Vulnerability of apps' permission to access a certain API being incompletely verified in the wireless projection module. Successful exploitation of this vulnerability may affect some wireless projection features.	2023-07-06	5.3	Medium
CVE-2023-3456	huawei - multiple products	Vulnerability of kernel raw address leakage in the hang detector module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-07-06	5.3	Medium
CVE-2023-33008	apache - johnzon	Deserialization of Untrusted Data vulnerability in Apache Software Foundation Apache Johnzon. A malicious attacker can craft up some JSON input that uses large numbers (numbers such as 1e20000000) that Apache Johnzon will deserialize into BigDecimal and maybe use numbers too large which may result in a slow conversion (Denial of service risk). Apache Johnzon 1.2.21 mitigates this by setting a scale limit of 1000 (by default) to the BigDecimal. This issue affects Apache Johnzon: through 1.2.20.	2023-07-07	5.3	Medium
CVE-2023-35786	zohocorp - multiple products	Zoho ManageEngine ADManager Plus before 7183 allows admin users to exploit an XXE issue to view files.	2023-07-05	4.9	Medium
CVE-2023-3497	google - chrome	Out of bounds read in Google Security Processor firmware in Google Chrome on Chrome OS prior to 114.0.5735.90 allowed a local attacker to perform denial of service via physical access to the device. (Chromium security severity: Medium)	2023-07-03	4.6	Medium
CVE-2023-30676	samsung - pass	Improper access control vulnerability in Samsung Pass prior to version 4.2.03.1 allows physical attackers to access data of Samsung Pass.	2023-07-06	4.6	Medium
CVE-2023-30677	samsung - pass	Improper access control vulnerability in Samsung Pass prior to version 4.2.03.1 allows physical attackers to access data of Samsung Pass on a certain state of an unlocked device.	2023-07-06	4.6	Medium

CVE-2023-37453	linux - linux_kernel	An issue was discovered in the USB subsystem in the Linux kernel through 6.4.2. There is an out-of-bounds and crash in read_descriptors in drivers/usb/core/sysfs.c.	2023-07-06	4.6	Medium
CVE-2023-20748	google - multiple products	In display, 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. Patch ID: ALPS07536951; Issue ID: ALPS07536951.	2023-07-04	4.4	Medium
CVE-2023-20758	google - multiple products	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07636130.	2023-07-04	4.4	Medium
CVE-2023-20759	google - multiple products	In cmdq, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07636133; Issue ID: ALPS07634601.	2023-07-04	4.4	Medium
CVE-2023-30665	samsung - multiple products	Improper input validation vulnerability in OnOemServiceMode in libsec-ril prior to SMR Jul-2023 Release 1 allows local attackers to cause an Out-Of-Bounds read.	2023-07-06	4.4	Medium
CVE-2023-30641	samsung - multiple products	Improper access control vulnerability in Settings prior to SMR Jul-2023 Release 1 allows physical attacker to use restricted user profile to access device owner&#39;s google account data.	2023-07-06	4.3	Medium
CVE-2020-8934	google - site_kit	The Site Kit by Google plugin for WordPress is vulnerable to Sensitive Information Disclosure in versions up to, and including, 1.8.0 This is due to the lack of capability checks on the admin_enqueue_scripts action which displays the connection key. This makes it possible for authenticated attackers with any level of access obtaining owner access to a site in the Google Search Console. We recommend upgrading to V1.8.1 or above.	2023-07-07	4.3	Medium
CVE-2023-30640	samsung - multiple products	Improper access control vulnerability in PersonaManagerService prior to SMR Jul-2023 Release 1 allows local attackers to change confiugration.	2023-07-06	3.3	Low
CVE-2023-30667	samsung - multiple products	Improper access control in Audio system service prior to SMR Jul-2023 Release 1 allows attacker to send broadcast with system privilege.	2023-07-06	3.3	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.