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 4th of June to 11th of June. 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 National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 4 يونيو إلى 11 يونيو. 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-2023-33532	netgear - r6250_firmware	There is a command injection vulnerability in the Netgear R6250 router with Firmware Version 1.0.4.48. If an attacker gains web management privileges, they can inject commands into the post request parameters, thereby gaining shell privileges.	2023-06-06	9.8	Critical
CVE-2023-20887	vmware - vrealize_network_insight	Aria Operations for Networks contains a command injection vulnerability. A malicious actor with network access to VMware Aria Operations for Networks may be able to perform a command injection attack resulting in remote code execution.	2023-06-07	9.8	Critical
CVE-2023-31116	samsung - exynos_5123_firmware	An issue was discovered in the Shannon RCS component in Samsung Exynos Modem 5123 and 5300. An incorrect default permission can cause unintended querying of RCS capability via a crafted application.	2023-06-07	9.8	Critical
CVE-2023-23482	ibm - multiple products	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 245891.	2023-06-08	9.6	Critical
CVE-2023-31114	samsung - exynos_5123_firmware	An issue was discovered in the Shannon RCS component in Samsung Exynos Modem 5123 and 5300. Incorrect resource transfer between spheres can cause unintended querying of the SIM status via a crafted application.	2023-06-07	9.1	Critical
CVE-2013-10027	wordpress - blogger_importer	A vulnerability was found in Blogger Importer Plugin up to 0.5 on WordPress. It has been classified as problematic. Affected is the function start/restart of the file blogger-importer.php. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. Upgrading to version 0.6 is able to address this issue. The name of the patch is b83fa4f862b0f19a54cfee76060ec9c2e7f7ca70. It is recommended to upgrade the affected component. VDB-230658 is the identifier assigned to this vulnerability.	2023-06-04	8.8	High
CVE-2023-0041	ibm - security_guardium	IBM Security Guardium 11.5 could allow a user to take over another user's session due to insufficient session expiration. IBM X-Force ID: 243657.	2023-06-05	8.8	High
CVE-2023-3079	google - chrome	Type confusion in V8 in Google Chrome prior to 114.0.5735.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-06-05	8.8	High
CVE-2023-33533	netgear - d6220_firmware	Netgear D6220 with Firmware Version 1.0.0.80, D8500 with Firmware Version 1.0.3.60, R6700 with Firmware Version 1.0.2.26, and R6900 with Firmware Version 1.0.2.26 are vulnerable to Command Injection. If an attacker gains web management privileges, they can inject commands into the post request parameters, gaining shell privileges.	2023-06-06	8.8	High
CVE-2023-33538	tp-link - tl-wr940n_firmware	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a command injection vulnerability via the component /userRpm/WlanNetworkRpm .	2023-06-07	8.8	High

CVE-2023-20888	vmware - vrealize_network_insight	Aria Operations for Networks contains an authenticated deserialization vulnerability. A malicious actor with network access to VMware Aria Operations for Networks and valid 'member' role credentials may be able to perform a deserialization attack resulting in remote code execution.	2023-06-07	8.8	High
CVE-2023-33536	tp-link - tl-wr940n_firmware	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/WlanMacFilterRpm.	2023-06-07	8.1	High
CVE-2023-33537	tp-link - tl-wr940n_firmware	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a buffer overflow via the component /userRpm/FixMapCfgRpm.	2023-06-07	8.1	High
CVE-2023-1388	trellix - agent	A heap-based overflow vulnerability in TA prior to version 5.7.9 allows a remote user to alter the page heap in the macmnsvc process memory block, resulting in the service becoming unavailable.	2023-06-07	8.1	High
CVE-2023-30576	apache - guacamole	Apache Guacamole 0.9.10 through 1.5.1 may continue to reference a freed RDP audio input buffer. Depending on timing, this may allow an attacker to execute arbitrary code with the privileges of the guacd process.	2023-06-07	8.1	High
CVE-2023-27285	ibm - multiple products	IBM Aspera Connect 4.2.5 and IBM Aspera Cargo 4.2.5 is vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow a buffer and execute arbitrary code on the system. IBM X-Force ID: 248625.	2023-06-05	7.8	High
CVE-2022-4569	lenovo - thinkpad_hybrid_usb-c_with_usb-a_dock_firmware	A local privilege escalation vulnerability in the ThinkPad Hybrid USB-C with USB-A Dock Firmware Update Tool could allow an attacker with local access to execute code with elevated privileges during the package upgrade or installation.	2023-06-05	7.8	High
CVE-2023-3111	linux - multiple products	A use after free vulnerability was found in prepare_to_relocate in fs/btrfs/relocation.c in btrfs in the Linux Kernel. This possible flaw can be triggered by calling btrfs_ioctl_balance() before calling btrfs_ioctl_defrag().	2023-06-05	7.8	High
CVE-2022-48181	lenovo - ideacentre_c5-14imb05_firmware	An ErrorMessage driver stack-based buffer overflow vulnerability in BIOS of some ThinkPad models could allow an attacker with local access to elevate their privileges and execute arbitrary code.	2023-06-05	7.8	High
CVE-2022-48188	lenovo - ideacentre_aio_3_21itl7_firmware	A buffer overflow vulnerability in the SecureBootDXE BIOS driver of some Lenovo Desktop and ThinkStation models could allow an attacker with local access to elevate their privileges to execute arbitrary code.	2023-06-05	7.8	High
CVE-2023-3027	redhat - multiple products	The grc-policy-propagator allows security escalation within the cluster. The propagator allows policies which contain some dynamically obtained values (instead of the policy apply a static manifest on a managed cluster) of taking advantage of cluster scoped access in a created policy. This feature does not restrict properly to lookup content from the namespace where the policy was created.	2023-06-05	7.8	High
CVE-2022-48390	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-06-06	7.8	High
CVE-2022-48392	google - multiple products	In dialer service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-06-06	7.8	High
CVE-2023-30863	google - android	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-06-06	7.8	High
CVE-2023-30864	google - android	In Connectivity Service, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges.	2023-06-06	7.8	High
CVE-2022-33224	qualcomm - aqt1000_firmware	Memory corruption in core due to buffer copy without check9ing the size of input while processing ioctl queries.	2023-06-06	7.8	High
CVE-2022-33226	qualcomm - aqt1000_firmware	Memory corruption due to buffer copy without checking the size of input in Core while processing ioctl commands from diag client applications.	2023-06-06	7.8	High
CVE-2022-33227	qualcomm - aqt1000_firmware	Memory corruption in Linux android due to double free while calling unregister provider after register call.	2023-06-06	7.8	High
CVE-2022-33230	qualcomm - aqt1000_firmware	Memory corruption in FM Host due to buffer copy without checking the size of input in FM Host	2023-06-06	7.8	High
CVE-2022-33240	qualcomm - qca6595_firmware	Memory corruption in Audio due to incorrect type cast during audio use-cases.	2023-06-06	7.8	High
CVE-2022-33263	qualcomm - aqt1000_firmware	Memory corruption due to use after free in Core when multiple DCI clients register and deregister.	2023-06-06	7.8	High
CVE-2022-33264	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in modem due to stack based buffer overflow while parsing OTASP Key Generation Request Message.	2023-06-06	7.8	High
CVE-2022-33267	qualcomm - aqt1000_firmware	Memory corruption in Linux while sending DRM request.	2023-06-06	7.8	High
CVE-2022-33307	qualcomm - aqt1000_firmware	Memory Corruption due to double free in automotive when a bad HLOS address for one of the lists to be mapped is passed.	2023-06-06	7.8	High

CVE-2022-40507	qualcomm - 315_5g_iot_modem_firmware	Memory corruption due to double free in Core while mapping HLOS address to the list.	2023-06-06	7.8	High
CVE-2022-40522	qualcomm - csr8811_firmware	Memory corruption in Linux Networking due to double free while handling a hyp-assign.	2023-06-06	7.8	High
CVE-2022-40529	qualcomm - aqt1000_firmware	Memory corruption due to improper access control in kernel while processing a mapping request from root process.	2023-06-06	7.8	High
CVE-2023-21628	qualcomm - apq8017_firmware	Memory corruption in WLAN HAL while processing WMI-UTF command or FTM TLV1 command.	2023-06-06	7.8	High
CVE-2023-21632	qualcomm - apq8064au_firmware	Memory corruption in Automotive GPU while querying a gsl memory node.	2023-06-06	7.8	High
CVE-2023-21656	qualcomm - ar8035_firmware	Memory corruption in WLAN HOST while receiving an WMI event from firmware.	2023-06-06	7.8	High
CVE-2023-21657	qualcomm - csra6620_firmware	Memoru corruption in Audio when ADSP sends input during record use case.	2023-06-06	7.8	High
CVE-2023-21670	qualcomm - 315_5g_iot_modem_firmware	Memory Corruption in GPU Subsystem due to arbitrary command execution from GPU in privileged mode.	2023-06-06	7.8	High
CVE-2023-0976	trellix - agent	A command Injection Vulnerability in TA for mac-OS prior to version 5.7.9 allows local users to place an arbitrary file into the /Library/Trellix/Agent/bin/ folder. The malicious file is executed by running the TA deployment feature located in the System Tree.	2023-06-07	7.8	High
CVE-2023-1709	siemens - multiple products	Datalogics Library APDFLThe v18.0.4PlusP1e and prior contains a stack-based buffer overflow due to documents containing corrupted fonts, which could allow an attack that causes an unhandled crash during the rendering process.	2023-06-07	7.8	High
CVE-2019-16283	hp - softpaq_installer	A potential security vulnerability has been identified with a version of the HP Softpaq installer that can lead to arbitrary code execution.	2023-06-09	7.8	High
CVE-2023-22862	ibm - multiple products	IBM Aspera Connect 4.2.5 and IBM Aspera Cargo 4.2.5 transmits authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. IBM X-Force ID: 244107.	2023-06-05	7.5	High
CVE-2022-22060	qualcomm - 315_5g_iot_modem_firmware	Assertion occurs while processing Reconfiguration message due to improper validation	2023-06-06	7.5	High
CVE-2022-33251	qualcomm - 315_5g_iot_modem_firmware	Transient DOS due to reachable assertion in Modem because of invalid network configuration.	2023-06-06	7.5	High
CVE-2022-40521	qualcomm - 315_5g_iot_modem_firmware	Transient DOS due to improper authorization in Modem	2023-06-06	7.5	High
CVE-2022-40536	qualcomm - 315_5g_iot_modem_firmware	Transient DOS due to improper authentication in modem while receiving plain TLB OTA request message from network.	2023-06-06	7.5	High
CVE-2022-40538	qualcomm - ar8035_firmware	Transient DOS due to reachable assertion in modem while processing sib with incorrect values from network.	2023-06-06	7.5	High
CVE-2023-21658	qualcomm - ar8035_firmware	Transient DOS in WLAN Firmware while processing the received beacon or probe response frame.	2023-06-06	7.5	High
CVE-2023-21659	qualcomm - 315_5g_iot_modem_firmware	Transient DOS in WLAN Firmware while processing frames with missing header fields.	2023-06-06	7.5	High
CVE-2023-21660	qualcomm - csr8811_firmware	Transient DOS in WLAN Firmware while parsing FT Information Elements.	2023-06-06	7.5	High
CVE-2023-21661	qualcomm - ar8035_firmware	Transient DOS while parsing WLAN beacon or probe-response frame.	2023-06-06	7.5	High
CVE-2023-21669	qualcomm - aqt1000_firmware	Information Disclosure in WLAN HOST while sending DPP action frame to peer with an invalid source address.	2023-06-06	7.5	High
CVE-2023-30575	apache - guacamole	Apache Guacamole 1.5.1 and older may incorrectly calculate the lengths of instruction elements sent during the Guacamole protocol handshake, potentially allowing an attacker to inject Guacamole instructions during the handshake through specially-crafted data.	2023-06-07	7.5	High
CVE-2023-20889	vmware - vrealize_network_insight	Aria Operations for Networks contains an information disclosure vulnerability. A malicious actor with network access to VMware Aria Operations for Networks may be able to perform a command injection attack resulting in information disclosure.	2023-06-07	7.5	High
CVE-2023-31115	samsung - exynos_5123_firmware	An issue was discovered in the Shannon RCS component in Samsung Exynos Modem 5123 and 5300. Incorrect resource transfer between spheres can cause changes to the activation mode of RCS via a crafted application.	2023-06-07	7.5	High
CVE-2023-29344	microsoft - multiple products	Microsoft Office Remote Code Execution Vulnerability	2023-06-05	7.3	High
CVE-2023-3141	linux - linux_kernel	A use-after-free flaw was found in r592_remove in drivers/memstick/host/r592.c in media access in the Linux Kernel. This flaw allows a local attacker to crash the system at device disconnect, possibly leading to a kernel information leak.	2023-06-09	7.1	High

CVE-2023-20723	google - multiple products	In Bluetooth, 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: ALPS07843845; Issue ID: ALPS07843845.	2023-06-06	6.7	Medium
CVE-2023-20724	google - multiple products	In Bluetooth, 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: ALPS07843845; Issue ID: ALPS07843841.	2023-06-06	6.7	Medium
CVE-2023-20739	google - multiple products	In vcu, there is a possible memory corruption 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: ALPS07559819; Issue ID: ALPS07559819.	2023-06-06	6.7	Medium
CVE-2023-20749	google - android	In swpm, 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: ALPS07780926; Issue ID: ALPS07780926.	2023-06-06	6.7	Medium
CVE-2023-20751	google - multiple products	In keymange, 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: ALPS07825502; Issue ID: ALPS07825502.	2023-06-06	6.7	Medium
CVE-2023-20752	google - multiple products	In keymange, 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: ALPS07826586; Issue ID: ALPS07826586.	2023-06-06	6.7	Medium
CVE-2023-27989	zyxel - lte7480-m804_firmware	A buffer overflow vulnerability in the CGI program of the Zyxel NR7101 firmware versions prior to V1.00(ABUV.8)C0 could allow a remote authenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device.	2023-06-05	6.5	Medium
CVE-2023-2253	redhat - multiple products	A flaw was found in the \`/v2/_catalog\` endpoint in distribution/distribution, which accepts a parameter to control the maximum number of records returned (query string: \`n\`). This vulnerability allows a malicious user to submit an unreasonably large value for \`n,\` causing the allocation of a massive string array, possibly causing a denial of service through excessive use of memory.	2023-06-06	6.5	Medium
CVE-2023-33848	ibm - multiple products	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could allow a privileged user to obtain highly sensitive information by enabling debug mode. IBM X-Force ID: 257104.	2023-06-07	6.5	Medium
CVE-2023-2183	grafana - multiple products	Grafana is an open-source platform for monitoring and observability. The option to send a test alert is not available from the user panel UI for users having the Viewer role. It is still possible for a user with the Viewer role to send a test alert using the API as the API does not check access to this function. This might enable malicious users to abuse the functionality by sending multiple alert messages to e-mail and Slack, spamming users, prepare Phishing attack or block SMTP server. Users may upgrade to version 9.5.3, 9.4.12, 9.3.15, 9.2.19 and 8.5.26 to receive a fix.	2023-06-06	6.4	Medium
CVE-2023-29345	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2023-06-07	6.1	Medium
CVE-2023-27861	ibm - multiple products	IBM Maximo Application Suite - Manage Component 8.8.0 and 8.9.0 transmits sensitive information in cleartext that could be intercepted by an attacker using man in the middle techniques. IBM X-Force ID: 249208.	2023-06-05	5.9	Medium
CVE-2022-48391	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-06-06	5.5	Medium
CVE-2022-48440	google - multiple products	In dialer service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-06-06	5.5	Medium
CVE-2022-48441	google - multiple products	In dialer service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-06-06	5.5	Medium
CVE-2022-48442	google - multiple products	In dialer service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-06-06	5.5	Medium

CVE-2022-48443	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-06-06	5.5	Medium
CVE-2022-48444	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-06-06	5.5	Medium
CVE-2022-48445	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-06-06	5.5	Medium
CVE-2022-48446	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-06-06	5.5	Medium
CVE-2022-48447	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-06-06	5.5	Medium
CVE-2022-48448	google - multiple products	In telephony service, there is a possible missing permission check. This could lead to local denial of service with no additional execution privileges.	2023-06-06	5.5	Medium
CVE-2023-30865	google - multiple products	In dialer service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-06-06	5.5	Medium
CVE-2023-30866	google - android	In telephony service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-06-06	5.5	Medium
CVE-2023-30914	google - multiple products	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-06-06	5.5	Medium
CVE-2023-30915	google - multiple products	In email service, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed.	2023-06-06	5.5	Medium
CVE-2022-22076	qualcomm - 315_5g_iot_modem_firmware	information disclosure due to cryptographic issue in Core during RPMB read request.	2023-06-06	5.5	Medium
CVE-2022-33303	qualcomm - wcn685x-5_firmware	Transient DOS due to uncontrolled resource consumption in Linux kernel when malformed messages are sent from the Gunyah Resource Manager message queue.	2023-06-06	5.5	Medium
CVE-2022-40523	qualcomm - 9205_lte_modem_firmware	Information disclosure in Kernel due to indirect branch misprediction.	2023-06-06	5.5	Medium
CVE-2022-40525	qualcomm - csr8811_firmware	Information disclosure in Linux Networking Firmware due to unauthorized information leak during side channel analysis.	2023-06-06	5.5	Medium
CVE-2022-40533	qualcomm - csra6620_firmware	Transient DOS due to untrusted Pointer Dereference in core while sending USB QMI request.	2023-06-06	5.5	Medium
CVE-2023-33846	ibm - txseries_for_multiplatform	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 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: 257100.	2023-06-08	5.4	Medium
CVE-2023-23480	ibm - multiple products	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 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: 245885.	2023-06-08	5.4	Medium
CVE-2023-23481	ibm - multiple products	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 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: 245889.	2023-06-08	5.4	Medium
CVE-2023-32334	ibm - multiple products	IBM Maximo Asset Management 7.6.1.2, 7.6.1.3 and IBM Maximo Application Suite 8.8.0 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 255074.	2023-06-05	5.3	Medium
CVE-2023-2801	grafana - multiple products	Grafana is an open-source platform for monitoring and observability. Using public dashboards users can query multiple distinct data sources using mixed queries. However such query has a possibility of crashing a Grafana instance. The only feature that uses mixed queries at the moment is public dashboards, but it's also possible to cause this by calling the query API directly. This might enable malicious users to crash Grafana instances through that endpoint.	2023-06-06	5.3	Medium

		Users may upgrade to version 9.4.12 and 9.5.3 to receive a fix.			
CVE-2023-27126	tp-link - tapo_c200_firmware	The AES Key-IV pair used by the TP-Link TAPO C200 camera V3 (EU) on firmware version 1.1.22 Build 220725 is reused across all cameras. An attacker with physical access to a camera is able to extract and decrypt sensitive data containing the Wifi password and the TP-LINK account credential of the victim.	2023-06-06	4.6	Medium
CVE-2022-48438	google - multiple products	In cp_dump driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-06-06	4.4	Medium
CVE-2022-48439	google - multiple products	In cp_dump driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2023-06-06	4.4	Medium
CVE-2023-20741	google - multiple products	In ril, 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: ALPS07628591; Issue ID: ALPS07628606.	2023-06-06	4.4	Medium
CVE-2023-20742	google - multiple products	In ril, 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: ALPS07628591; Issue ID: ALPS07628540.	2023-06-06	4.4	Medium
CVE-2023-20750	google - android	In swpm, there is a possible out of bounds write due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07780926; Issue ID: ALPS07780928.	2023-06-06	4.1	Medium
CVE-2023-33849	ibm - multiple products	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 could transmit sensitive information in query parameters that could be intercepted using man in the middle techniques. IBM X-Force ID: 257105.	2023-06-07	3.7	Low
CVE-2023-33847	ibm - txseries_for_multiplatform	IBM TXSeries for Multiplatforms 8.1, 8.2, 9.1, CICS TX Standard, 11.1, CICS TX Advanced 10.1, and 11.1 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 257102.	2023-06-08	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.