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.

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 31st of December to 6th of January 2024. 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**

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

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 ٣١ ديسمبر إلى ٦ يناير ٢٠٢٤. 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-2023-33025	qualcomm - ar8035_firmware	Memory corruption in Data Modem when a non-standard SDP body, during a VOLTE call.	2024-01-02	9.8	Critical
CVE-2023-48419	google - nest_audio_firmware	An attacker in the wifi vicinity of a target Google Home can spy on the victim, resulting in Elevation of Privilege	2024-01-02	9.8	Critical
CVE-2023-6339	google - nest_wifi_pro_firmware	Google Nest WiFi Pro root code-execution & user-data compromise	2024-01-02	9.8	Critical
CVE-2023-51784	apache - inlong	Improper Control of Generation of Code ('Code Injection') vulnerability in Apache InLong.This issue affects Apache InLong: from 1.5.0 through 1.9.0, which could lead to Remote Code Execution. Users are advised to upgrade to Apache InLong's 1.10.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/9329	2024-01-03	9.8	Critical
CVE-2024-0222	google - chrome	Use after free in ANGLE in Google Chrome prior to 120.0.6099.199 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-01-04	8.8	High
CVE-2024-0223	google - chrome	Heap buffer overflow in ANGLE in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-01-04	8.8	High
CVE-2024-0224	google - chrome	Use after free in WebAudio in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-01-04	8.8	High
CVE-2024-0225	google - chrome	Use after free in WebGPU in Google Chrome prior to 120.0.6099.199 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-01-04	8.8	High
CVE-2023-41287	qnap - video_station	A SQL injection vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow users to inject malicious code via a network. We have already fixed the vulnerability in the following version: Video Station 5.7.2 (2023/11/23) and later	2024-01-05	8.8	High
CVE-2023-41288	qnap - video_station	An OS command injection vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following version: Video Station 5.7.2 (2023/11/23) and later	2024-01-05	8.8	High
CVE-2023-41289	qnap - qcalagent	An OS command injection vulnerability has been reported to affect QcalAgent. If exploited, the vulnerability could allow authenticated users to execute commands via a network.	2024-01-05	8.8	High

		We have already fixed the vulnerability in the following version: QcalAgent 1.1.8 and later			
CVE-2023-47219	qnap - qumagie	A SQL injection vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: QuMagie 2.2.1 and later	2024-01-05	8.8	High
CVE-2023-47560	qnap - qumagie	An OS command injection vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following version: QuMagie 2.2.1 and later	2024-01-05	8.8	High
CVE-2023-28583	qualcomm - aqt1000_firmware	Memory corruption when IPv6 prefix timer object`s lifetime expires which are created while Netmgr daemon gets an IPv6 address.	2024-01-02	7.8	High
CVE-2023-33030	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in HLOS while running playready use-case.	2024-01-02	7.8	High
CVE-2023-33032	qualcomm - 9205_lte_modem_firmware	Memory corruption in TZ Secure OS while requesting a memory allocation from TA region.	2024-01-02	7.8	High
CVE-2023-33033	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in Audio during playback with speaker protection.	2024-01-02	7.8	High
CVE-2023-33038	qualcomm - 315_5g_iot_modem_firmware	Memory corruption while receiving a message in Bus Socket Transport Server.	2024-01-02	7.8	High
CVE-2023-33085	qualcomm - ar8035_firmware	Memory corruption in wearables while processing data from AON.	2024-01-02	7.8	High
CVE-2023-33094	qualcomm - ar8035_firmware	Memory corruption while running VK synchronization with KASAN enabled.	2024-01-02	7.8	High
CVE-2023-33108	qualcomm - qam8255p_firmware	Memory corruption in Graphics Driver when destroying a context with KGSL_GPU_AUX_COMMAND_TIMELINE objects queued.	2024-01-02	7.8	High
CVE-2023-33113	qualcomm - ar8035_firmware	Memory corruption when resource manager sends the host kernel a reply message with multiple fragments.	2024-01-02	7.8	High
CVE-2023-33114	qualcomm - 315_5g_iot_modem_firmware	Memory corruption while running NPU, when NETWORK_UNLOAD and (NETWORK_UNLOAD or NETWORK_EXECUTE_V2) commands are submitted at the same time.	2024-01-02	7.8	High
CVE-2023-33117	qualcomm - ar8035_firmware	Memory corruption when HLOS allocates the response payload buffer to copy the data received from ADSP in response to AVCS_LOAD_MODULE command.	2024-01-02	7.8	High
CVE-2023-33118	qualcomm - ar8035_firmware	Memory corruption while processing Listen Sound Model client payload buffer when there is a request for Listen Sound session get parameter from ST HAL.	2024-01-02	7.8	High
CVE-2023-33120	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in Audio when memory map command is executed consecutively in ADSP.	2024-01-02	7.8	High
CVE-2023-43514	qualcomm - ar8035_firmware	Memory corruption while invoking IOCTLs calls from user space for internal mem MAP and internal mem UNMAP.	2024-01-02	7.8	High
CVE-2023-48418	google - pixel_watch_firmware	In checkDebuggingDisallowed of DeviceVersionFragment.java, there is a possible way to access adb before SUW completion due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation	2024-01-02	7.8	High
CVE-2023-6338	lenovo - universal_device_client	Uncontrolled search path vulnerabilities were reported in the Lenovo Universal Device Client (UDC) that could allow an attacker with local access to execute code with elevated privileges.	2024-01-03	7.8	High
CVE-2023-32889	google - multiple products	In Modem IMS Call UA, there is a possible out of bounds write 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. Patch ID: MOLY01161825; Issue ID: MOLY01161825 (MSV-895).	2024-01-02	7.5	High
CVE-2023-26157	gnu - libredwg	Versions of the package libredwg before 0.12.5.6384 are vulnerable to Denial of Service (DoS) due to an out-of-bounds read involving section->num_pages in decode_r2007.c.	2024-01-02	7.5	High
CVE-2023-33040	qualcomm - 315_5g_iot_modem_firmware	Transient DOS in Data Modem during DTLS handshake.	2024-01-02	7.5	High
CVE-2023-33062	qualcomm - 315_5g_iot_modem_firmware	Transient DOS in WLAN Firmware while parsing a BTM request.	2024-01-02	7.5	High

CVE-2023-33109	qualcomm - 315_5g_iot_modem_firmware	Transient DOS while processing a WMI P2P listen start command (0xD00A) sent from host.	2024-01-02	7.5	High
CVE-2023-33112	qualcomm - ar8035_firmware	Transient DOS when WLAN firmware receives "reassoc response" frame including RIC_DATA element.	2024-01-02	7.5	High
CVE-2023-33116	qualcomm - ar8035_firmware	Transient DOS while parsing ieee80211_parse_mscs_ie in WIN WLAN driver.	2024-01-02	7.5	High
CVE-2023-43511	qualcomm - 315_5g_iot_modem_firmware	Transient DOS while parsing IPv6 extension header when WLAN firmware receives an IPv6 packet that contains `IPPROTO_NONE` as the next header.	2024-01-02	7.5	High
CVE-2023-43512	qualcomm - qcn7606_firmware	Transient DOS while parsing GATT service data when the total amount of memory that is required by the multiple services is greater than the actual size of the services buffer.	2024-01-02	7.5	High
CVE-2023-51785	apache - inlong	Deserialization of Untrusted Data vulnerability in Apache InLong.This issue affects Apache InLong: from 1.7.0 through 1.9.0, the attackers can make a arbitrary file read attack using mysql driver. Users are advised to upgrade to Apache InLong's 1.10.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/9331	2024-01-03	7.5	High
CVE-2023-6540	lenovo - multiple products	A vulnerability was reported in the Lenovo Browser Mobile and Lenovo Browser HD Apps for Android that could allow an attacker to craft a payload that could result in the disclosure of sensitive information.	2024-01-03	7.5	High
CVE-2023-39296	qnap - multiple products	A prototype pollution vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to override existing attributes with ones that have incompatible type, which may lead to a crash via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later	2024-01-05	7.5	High
CVE-2023-39294	qnap - multiple products	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later	2024-01-05	7.2	High
CVE-2023-45039	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	2024-01-05	7.2	High
CVE-2023-45040	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	2024-01-05	7.2	High
CVE-2023-45041	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	2024-01-05	7.2	High
CVE-2023-45042	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	2024-01-05	7.2	High
CVE-2023-45043	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions:	2024-01-05	7.2	High

		QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later			
CVE-2023-45044	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.4.2596 build 20231128 and later QuTS hero h5.1.4.2596 build 20231128 and later	2024-01-05	7.2	High
CVE-2023-51441	apache - axis	** UNSUPPORTED WHEN ASSIGNED ** Improper Input Validation vulnerability in Apache Axis allowed users with access to the admin service to perform possible SSRF This issue affects Apache Axis: through 1.3. As Axis 1 has been EOL we recommend you migrate to a different SOAP engine, such as Apache Axis 2/Java. Alternatively you could use a build of Axis with the patch from https://github.com/apache/axis-axis1-java/commit/685c309febc64aa393b2d64a05f90e7eb9f73e06 applied. The Apache Axis project does not expect to create an Axis 1.x release fixing this problem, though contributors that would like to work towards this are welcome.	2024-01-06	7.2	High
CVE-2023-33110	qualcomm - snapdragon_425_mobile_platform_firmware	The session index variable in PCM host voice audio driver initialized before PCM open, accessed during event callback from ADSP and reset during PCM close may lead to race condition between event callback - PCM close and reset session index causing memory corruption.	2024-01-02	7	High
CVE-2023-6270	linux - linux_kernel	A flaw was found in the ATA over Ethernet (AoE) driver in the Linux kernel. The aoecmd_cfg_pkts() function improperly updates the refcnt on `struct net_device`, and a use-after-free can be triggered by racing between the free on the struct and the access through the `skbtxq` global queue. This could lead to a denial of service condition or potential code execution.	2024-01-04	7	High
CVE-2023-33014	qualcomm - ar8035_firmware	Information disclosure in Core services while processing a Diag command.	2024-01-02	6.8	Medium
CVE-2023-32872	google - multiple products	In keyInstall, 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: ALPS08308607; Issue ID: ALPS08308607.	2024-01-02	6.7	Medium
CVE-2023-32877	google - multiple products	In battery, 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: ALPS08308070; Issue ID: ALPS08308070.	2024-01-02	6.7	Medium
CVE-2023-32879	google - multiple products	In battery, 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: ALPS08308070; Issue ID: ALPS08308064.	2024-01-02	6.7	Medium
CVE-2023-32882	google - multiple products	In battery, there is a possible memory corruption 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: ALPS08308070; Issue ID: ALPS08308616.	2024-01-02	6.7	Medium
CVE-2023-32883	google - multiple products	In Engineer Mode, 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: ALPS08282249; Issue ID: ALPS08282249.	2024-01-02	6.7	Medium
CVE-2023-32884	google - multiple products	In netdagent, there is a possible information disclosure due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07944011; Issue ID: ALPS07944011.	2024-01-02	6.7	Medium
CVE-2023-32885	google - multiple products	In display drm, there is a possible memory corruption 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: ALPS07780685; Issue ID: ALPS07780685.	2024-01-02	6.7	Medium
CVE-2023-32891	google - multiple products	In bluetooth service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07933038; Issue ID: MSV-559.	2024-01-02	6.7	Medium

CVE-2024-0193	linux - linux_kernel	A use-after-free flaw was found in the netfilter subsystem of the Linux kernel. If the catchall element is garbage-collected when the pipapo set is removed, the element can be deactivated twice. This can cause a use-after-free issue on an NFT_CHAIN object or NFT_OBJECT object, allowing a local unprivileged user with CAP_NET_ADMIN capability to escalate their privileges on the system.	2024-01-02	6.7	Medium
CVE-2024-20803	samsung - multiple products	Improper authentication vulnerability in Bluetooth pairing process prior to SMR Jan-2024 Release 1 allows remote attackers to establish pairing process without user interaction.	2024-01-04	6.5	Medium
CVE-2023-6944	redhat - red_hat_developer_hub	A flaw was found in the Red Hat Developer Hub (RHDH). The catalog-import function leaks GitLab access tokens on the frontend when the base64 encoded GitLab token includes a newline at the end of the string. The sanitized error can display on the frontend, including the raw access token. Upon gaining access to this token and depending on permissions, an attacker could push malicious code to repositories, delete resources in Git, revoke or generate new keys, and sign code illegitimately.	2024-01-04	5.7	Medium
CVE-2023-33036	qualcomm - aqt1000_firmware	Permanent DOS in Hypervisor while untrusted VM without PSCI support makes a PSCI call.	2024-01-02	5.5	Medium
CVE-2023-33037	qualcomm - ar8035_firmware	Cryptographic issue in Automotive while unwrapping the key secs2d and verifying with RPMB data.	2024-01-02	5.5	Medium
CVE-2023-4164	google - android	There is a possible information disclosure due to a missing permission check. This could lead to local information disclosure of health data with no additional execution privileges needed.	2024-01-02	5.5	Medium
CVE-2024-20802	samsung - dex	Improper access control vulnerability in Samsung DeX prior to SMR Jan-2024 Release 1 allows owner to access other users&#39; notification in a multi-user environment.	2024-01-04	5.5	Medium
CVE-2024-20804	samsung - multiple products	Path traversal vulnerability in FileUriConverter of MyFiles prior to SMR Jan-2024 Release 1 in Android 11 and Android 12, and version 14.5.00.21 in Android 13 allows attackers to write arbitrary file.	2024-01-04	5.5	Medium
CVE-2024-20805	samsung - multiple products	Path traversal vulnerability in ZipCompressor of MyFiles prior to SMR Jan-2024 Release 1 in Android 11 and Android 12, and version 14.5.00.21 in Android 13 allows attackers to write arbitrary file.	2024-01-04	5.5	Medium
CVE-2024-20806	samsung - multiple products	Improper access control in Notification service prior to SMR Jan-2024 Release 1 allows local attacker to access notification data.	2024-01-04	5.5	Medium
CVE-2024-20808	samsung - nearby_device_scanning	Improper access control vulnerability in Nearby device scanning prior version 11.1.14.7 allows local attacker to access data.	2024-01-04	5.5	Medium
CVE-2024-20809	samsung - nearby_device_scanning	Improper access control vulnerability in Nearby device scanning prior version 11.1.14.7 allows local attacker to access data.	2024-01-04	5.5	Medium
CVE-2023-47559	qnap - qumagie	A cross-site scripting (XSS) vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: QuMagie 2.2.1 and later	2024-01-05	5.4	Medium
CVE-2023-34324	linux - multiple products	Closing of an event channel in the Linux kernel can result in a deadlock. This happens when the close is being performed in parallel to an unrelated Xen console action and the handling of a Xen console interrupt in an unprivileged guest. The closing of an event channel is e.g. triggered by removal of a paravirtual device on the other side. As this action will cause console messages to be issued on the other side quite often, the chance of triggering the deadlock is not neglectable. Note that 32-bit Arm-guests are not affected, as the 32-bit Linux kernel on Arm doesn't use queued-RW-locks, which are required to trigger the issue (on Arm32 a waiting writer doesn't block further readers to get the lock).	2024-01-05	4.9	Medium
CVE-2017-20188	zimbra - zm-ajax	A vulnerability has been found in Zimbra zm-ajax up to 8.8.1 and classified as problematic. Affected by this vulnerability is the function XFormItem.prototype.setError of the file WebRoot/js/ajax/dwt/xforms/XFormItem.js. The manipulation of the argument message leads to cross site scripting. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. Upgrading to version 8.8.2 is able to address this issue. The identifier of the patch is 8d039d6efe80780adc40c6f670c06d21de272105. It is	2024-01-02	4.7	Medium

		recommended to upgrade the affected component. The identifier VDB-249421 was assigned to this vulnerability.			
CVE-2023-32875	google - multiple products	In keyInstall, there is a possible information disclosure 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: ALPS08308607; Issue ID: ALPS08304217.	2024-01-02	4.4	Medium
CVE-2023-32876	google - multiple products	In keyInstall, there is a possible information disclosure 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: ALPS08308612; Issue ID: ALPS08308612.	2024-01-02	4.4	Medium
CVE-2023-32878	google - multiple products	In battery, there is a possible information disclosure 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: ALPS08308070; Issue ID: ALPS08307992.	2024-01-02	4.4	Medium
CVE-2023-32880	google - multiple products	In battery, there is a possible information disclosure 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: ALPS08308070; Issue ID: ALPS08308076.	2024-01-02	4.4	Medium
CVE-2023-32881	google - multiple products	In battery, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08308070; Issue ID: ALPS08308080.	2024-01-02	4.4	Medium
CVE-2023-7192	linux - linux_kernel	A memory leak problem was found in ctnetlink_create_conntrack in net/netfilter/nf_conntrack_netlink.c in the Linux Kernel. This issue may allow a local attacker with CAP_NET_ADMIN privileges to cause a denial of service (DoS) attack due to a refcount overflow.	2024-01-02	4.4	Medium
CVE-2024-20807	samsung - email	Implicit intent hijacking vulnerability in Samsung Email prior to version 6.1.90.16 allows attacker to get sensitive information.	2024-01-04	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.