الهيئــــة الوطنيــــه
للأمـــن السيبـــرانى
Nat onal 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 22nd of December to 28th of December. 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 ٢٢ ديسمبر إلى ٢٨ ديسمبر. 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
CVE-2024-52046	apache software foundation - Apache MINA	The ObjectSerializationDecoder in Apache MINA uses Java’s native deserialization protocol to process incoming serialized data but lacks the necessary security checks and defenses. This vulnerability allows attackers to exploit the deserialization process by sending specially crafted malicious serialized data, potentially leading to remote code execution (RCE) attacks. This issue affects MINA core versions 2.0.X, 2.1.X and 2.2.X, and will be fixed by the releases 2.0.27, 2.1.10 and 2.2.4. It's also important to note that an application using MINA core library will only be affected if the IoBuffer#getObject() method is called, and this specific method is potentially called when adding a ProtocolCodecFilter instance using the ObjectSerializationCodecFactory class in the filter chain. If your application is specifically using those classes, you have to upgrade to the latest version of MINA core library. Upgrading will not be enough: you also need to explicitly allow the classes the decoder will accept in the ObjectSerializationDecoder instance, using one of the three new methods: /** * Accept class names where the supplied ClassNameMatcher matches for * deserialization, unless they are otherwise rejected. * * @param classNameMatcher the matcher to use */ public void accept(ClassNameMatcher classNameMatcher) /** * Accept class names that match the supplied pattern for * deserialization, unless they are otherwise rejected. *	2024-12-25	10

		* @param pattern standard Java regexp */ public void accept(Pattern pattern) /** * Accept the wildcard specified classes for deserialization, * unless they are otherwise rejected. * * @param patterns Wildcard file name patterns as defined by * {@link org.apache.commons.io.FilenameUtils#wildcardMatch(String, String) FilenameUtils.wildcardMatch} */ public void accept(String... patterns) By default, the decoder will reject *all* classes that will be present in the incoming data. Note: The FtpServer, SSHd and Vysper sub-project are not affected by this issue.		
CVE-2024-45387	apache software foundation - Apache Traffic Control	An SQL injection vulnerability in Traffic Ops in Apache Traffic Control <= 8.0.1, >= 8.0.0 allows a privileged user with role "admin", "federation", "operations", "portal", or "steering" to execute arbitrary SQL against the database by sending a specially-crafted PUT request. Users are recommended to upgrade to version Apache Traffic Control 8.0.2 if you run an affected version of Traffic Ops.	2024-12-23	9.9
CVE-2024-43441	apache software foundation - Apache HugeGraph-Server	Authentication Bypass by Assumed-Immutable Data vulnerability in Apache HugeGraph-Server. This issue affects Apache HugeGraph-Server: from 1.0.0 before 1.5.0. Users are recommended to upgrade to version 1.5.0, which fixes the issue.	2024-12-24	9.8
CVE-2020-9236	huawei - FusionCompute	There is an improper interface design vulnerability in Huawei product. A module interface of the impated product does not deal with some operations properly. Attackers can exploit this vulnerability to perform malicious operatation to compromise module service. (Vulnerability ID: HWPSIRT-2020-05010) This vulnerability has been assigned a Common Vulnerabilities and Exposures (CVE) ID: CVE-2020-9236.	2024-12-27	8.8
CVE-2024-51540	dell - ECS	Dell ECS, versions prior to 3.8.1.3 contains an arithmetic overflow vulnerability exists in retention period handling of ECS. An authenticated user with bucket or object-level access and the necessary privileges could potentially exploit this vulnerability to bypass retention policies and delete objects.	2024-12-26	8.1
CVE-2023-7300	huawei - HarmonyOS AILife Solution 8.0	Huawei Home Music System has a path traversal vulnerability. Successful exploitation of this vulnerability may cause the music host file to be deleted or the file permission to be changed.(Vulnerability ID:HWPSIRT-2023-60613)	2024-12-26	8
CVE-2024-47978	dell - NativeEdge	Dell NativeEdge, version(s) 2.1.0.0, contain(s) an Execution with Unnecessary Privileges vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2024-12-25	7.8
CVE-2020-9080	huawei - multiple products	There is an improper privilege management vulnerability in Huawei smart phone product. A local, authenticated attacker could craft a specific input to exploit this vulnerability. Successful exploitation may lead to local privilege escalation. (Vulnerability ID: HWPSIRT-2020-05272) This vulnerability has been assigned a Common Vulnerabilities and Exposures (CVE) ID: CVE-2020-9080.	2024-12-27	7.8
CVE-2021-37000	huawei - HarmonyOS	Some Huawei wearables have a permission management vulnerability.	2024-12-28	7.7
CVE-2024-53291	dell - NativeEdge	Dell NativeEdge, version(s) 2.1.0.0, contain(s) an Exposure of Sensitive Information Through Metadata vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	2024-12-25	7.5
CVE-2021-22484	huawei - HarmonyOS	Some Huawei wearables have a vulnerability of not verifying the actual data size when reading data. Successful exploitation of this vulnerability may cause a server out of memory (OOM).	2024-12-28	7.5
CVE-2023-7266	huawei - multiple products	Some Huawei home routers have a connection hijacking vulnerability. Successful exploitation of this vulnerability may cause DoS or information leakage.(Vulnerability ID:HWPSIRT-2023-76605) This vulnerability has been assigned a (CVE)ID:CVE-2023-7266	2024-12-28	7.5
CVE-2024-53961	adobe - ColdFusion	ColdFusion versions 2023.11, 2021.17 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access files or directories that are outside of the restricted directory set by the application. This could lead to the disclosure of sensitive information or the manipulation of system data.	2024-12-23	7.4

CVE-2023-7263	huawei - HarmonyOS AILife Solution 8.0	Some Huawei home music system products have a path traversal vulnerability. Successful exploitation of this vulnerability may cause unauthorized file deletion or file permission change.(Vulnerability ID:HWPSIRT-2023-53450) This vulnerability has been assigned a (CVE)ID:CVE-2023-7263	2024-12-28	7.3
CVE-2024-12582	red hat - Red Hat Service Interconnect 1	A flaw was found in the skupper console, a read-only interface that renders cluster network, traffic details, and metrics for a network application that a user sets up across a hybrid multi-cloud environment. When the default authentication method is used, a random password is generated for the "admin" user and is persisted in either a Kubernetes secret or a podman volume in a plaintext file. This authentication method can be manipulated by an attacker, leading to the reading of any user-readable file in the container filesystem, directly impacting data confidentiality. Additionally, the attacker may induce skupper to read extremely large files into memory, resulting in resource exhaustion and a denial of service attack.	2024-12-24	7.1
CVE-2024-52535	dell - multiple products	Dell SupportAssist for Home PCs versions 4.6.1 and prior and Dell SupportAssist for Business PCs versions 4.5.0 and prior, contain a symbolic link (symlink) attack vulnerability in the software remediation component. A low-privileged authenticated user could potentially exploit this vulnerability, gaining privileges escalation, leading to arbitrary deletion of files and folders from the system.	2024-12-25	7.1
CVE-2020-9222	huawei - FusionCompute	There is a privilege escalation vulnerability in Huawei FusionCompute product. Due to insufficient verification on specific files that need to be deserialized, local attackers can exploit this vulnerability to elevate permissions. (Vulnerability ID: HWPSIRT-2020-05241) This vulnerability has been assigned a Common Vulnerabilities and Exposures (CVE) ID: CVE-2020-9222.	2024-12-27	7
CVE-2024-12986	draytek - multiple products	A vulnerability, which was classified as critical, has been found in DrayTek Vigor2960 and Vigor300B 1.5.1.3/1.5.1.4. This issue affects some unknown processing of the file /cgi-bin/mainfunction.cgi/apmcfgupptim of the component Web Management Interface. The manipulation of the argument session leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.5.1.5 is able to address this issue. It is recommended to upgrade the affected component.	2024-12-27	6.9
CVE-2024-12987	draytek - multiple products	A vulnerability, which was classified as critical, was found in DrayTek Vigor2960 and Vigor300B 1.5.1.4. Affected is an unknown function of the file /cgi-bin/mainfunction.cgi/apmcfgupload of the component Web Management Interface. The manipulation of the argument session leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.5.1.5 is able to address this issue. It is recommended to upgrade the affected component.	2024-12-27	6.9
CVE-2024-12988	netgear - multiple products	A vulnerability has been found in Netgear R6900P and R7000P 1.3.3.154 and classified as critical. Affected by this vulnerability is the function sub_16C4C of the component HTTP Header Handler. The manipulation of the argument Host leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-12-27	6.9
CVE-2020-9210	huawei - Myna	There is an insufficient integrity vulnerability in Huawei products. A module does not perform sufficient integrity check in a specific scenario. Attackers can exploit the vulnerability by physically install malware. This could compromise normal service of the affected device. (Vulnerability ID: HWPSIRT-2020-00145) This vulnerability has been assigned a Common Vulnerabilities and Exposures (CVE) ID: CVE-2020-9210.	2024-12-27	6.8
CVE-2024-52543	dell - NativeEdge	Dell NativeEdge, version(s) 2.1.0.0, contain(s) a Creation of Temporary File With Insecure Permissions vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2024-12-25	6.5
CVE-2020-9211	huawei - HUAWEI Mate 30	There is an out-of-bound read and write vulnerability in Huawei smartphone. A module dose not verify the input sufficiently. Attackers can exploit this vulnerability by modifying some configuration to cause out-of-bound read and write, causing denial of service. (Vulnerability ID: HWPSIRT-2020-05103) This vulnerability has been assigned a Common Vulnerabilities and Exposures (CVE) ID: CVE-2020-9211.	2024-12-27	6.4
CVE-2023-52718	huawei - multiple products	A connection hijacking vulnerability exists in some Huawei home routers. Successful exploitation of this vulnerability may cause DoS or information leakage.(Vulnerability ID:HWPSIRT-2023-34408) This vulnerability has been assigned a (CVE)ID:CVE-2023-52718	2024-12-28	6.4
CVE-2020-9253	huawei - Lion-AL00C	There is a stack overflow vulnerability in some Huawei smart phone. An attacker can craft specific packet to exploit this vulnerability. Due to insufficient verification, this could be exploited to tamper with the information to affect the availability. (Vulnerability ID: HWPSIRT-2019-11030) This vulnerability has been assigned a Common Vulnerabilities and Exposures (CVE) ID: CVE-2020-9253.	2024-12-27	6.3
CVE-2024-39727	ibm - Engineering Insights	IBM Engineering Lifecycle Optimization - Engineering Insights 7.0.2 and 7.0.3 uses a web link with untrusted references to an external site. A remote attacker could exploit this vulnerability to expose sensitive information or perform unauthorized actions on the victims' web browser.	2024-12-25	6.1
CVE-2024-23945	apache software foundation - multiple products	Signing cookies is an application security feature that adds a digital signature to cookie data to verify its authenticity and integrity. The signature helps prevent malicious actors from modifying the cookie value, which can lead to security vulnerabilities and exploitation. Apache Hive's service component accidentally exposes the signed cookie to the end user when there is a mismatch in signature between the current and expected cookie. Exposing the correct cookie signature can lead to further exploitation. The vulnerable CookieSigner logic was introduced in Apache Hive by HIVE-9710 (1.2.0) and in Apache	2024-12-23	5.9

		Spark by SPARK-14987 (2.0.0). The affected components are the following: * org.apache.hive:hive-service * org.apache.spark:spark-hive-thriftserver_2.11 * org.apache.spark:spark-hive-thriftserver_2.12		
CVE-2024-47102	ibm - AIX	IBM AIX 7.2, 7.3, VIOS 3.1, and 4.1 could allow a non-privileged local user to exploit a vulnerability in the AIX perfstat kernel extension to cause a denial of service.	2024-12-25	5.5
CVE-2024-52906	ibm - AIX	IBM AIX 7.2, 7.3, VIOS 3.1, and 4.1 could allow a non-privileged local user to exploit a vulnerability in the TCP/IP kernel extension to cause a denial of service.	2024-12-25	5.5
CVE-2024-52534	dell - ECS	Dell ECS, version(s) prior to ECS 3.8.1.3, contain(s) an Authentication Bypass by Capture-replay vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Session theft.	2024-12-25	5.4
CVE-2024-39725	ibm - Engineering Insights	IBM Engineering Lifecycle Optimization - Engineering Insights 7.0.2 and 7.0.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.	2024-12-25	5.3
CVE-2020-9085	huawei - HUAWEI 4G Router B612	There is a NULL pointer dereference vulnerability in some Huawei products. An attacker may send specially crafted POST messages to the affected products. Due to insufficient validation of some parameter in the message, successful exploit may cause some process abnormal. (Vulnerability ID: HWPSIRT-2017-10105) This vulnerability has been assigned a Common Vulnerabilities and Exposures (CVE) ID: CVE-2020-9085.	2024-12-27	5.3
CVE-2020-9086	huawei - HUAWEI 4G Router B612	There is a buffer error vulnerability in some Huawei product. An unauthenticated attacker may send special UPNP message to the affected products. Due to insufficient input validation of some value, successful exploit may cause some service abnormal. (Vulnerability ID: HWPSIRT-2017-08234) This vulnerability has been assigned a Common Vulnerabilities and Exposures (CVE) ID: CVE-2020-9086.	2024-12-27	4.3
CVE-2022-48470	huawei - HarmonyOS AILife Solution 6.0	Huawei HiLink AI Life product has an identity authentication bypass vulnerability. Successful exploitation of this vulnerability may allow attackers to access restricted functions.(Vulnerability ID:HWPSIRT-2022-42291) This vulnerability has been assigned a (CVE)ID:CVE-2022-48470	2024-12-28	4
CVE-2020-1818	huawei - multiple products	There are multiple out of bounds (OOB) read vulnerabilities in the implementation of the Common Open Policy Service (COPS) protocol of some Huawei products. The specific decoding function may occur out-of-bounds read when processes an incoming data packet. Successful exploit of these vulnerabilities may disrupt service on the affected device. (Vulnerability ID: HWPSIRT-2018-12275,HWPSIRT-2018-12276,HWPSIRT-2018-12277,HWPSIRT-2018-12278,HWPSIRT-2018-12279,HWPSIRT-2018-12280 and HWPSIRT-2018-12289) The seven vulnerabilities have been assigned seven Common Vulnerabilities and Exposures (CVE) IDs: CVE-2020-1818, CVE-2020-1819, CVE-2020-1820, CVE-2020-1821, CVE-2020-1822, CVE-2020-1823 and CVE-2020-1824.	2024-12-27	3.7
CVE-2020-1819	huawei - multiple products	There are multiple out of bounds (OOB) read vulnerabilities in the implementation of the Common Open Policy Service (COPS) protocol of some Huawei products. The specific decoding function may occur out-of-bounds read when processes an incoming data packet. Successful exploit of these vulnerabilities may disrupt service on the affected device. (Vulnerability ID: HWPSIRT-2018-12275,HWPSIRT-2018-12276,HWPSIRT-2018-12277,HWPSIRT-2018-12278,HWPSIRT-2018-12279,HWPSIRT-2018-12280 and HWPSIRT-2018-12289) The seven vulnerabilities have been assigned seven Common Vulnerabilities and Exposures (CVE) IDs: CVE-2020-1818, CVE-2020-1819, CVE-2020-1820, CVE-2020-1821, CVE-2020-1822, CVE-2020-1823 and CVE-2020-1824.	2024-12-27	3.7
CVE-2020-1820	huawei - multiple products	There are multiple out of bounds (OOB) read vulnerabilities in the implementation of the Common Open Policy Service (COPS) protocol of some Huawei products. The specific decoding function may occur out-of-bounds read when processes an incoming data packet. Successful exploit of these vulnerabilities may disrupt service on the affected device. (Vulnerability ID: HWPSIRT-2018-12275,HWPSIRT-2018-12276,HWPSIRT-2018-12277,HWPSIRT-2018-12278,HWPSIRT-2018-12279,HWPSIRT-2018-12280 and HWPSIRT-2018-12289) The seven vulnerabilities have been assigned seven Common Vulnerabilities and Exposures (CVE) IDs: CVE-2020-1818, CVE-2020-1819, CVE-2020-1820, CVE-2020-1821, CVE-2020-1822, CVE-2020-1823 and CVE-2020-1824.	2024-12-28	3.7
CVE-2020-1821	huawei - multiple products	There are multiple out of bounds (OOB) read vulnerabilities in the implementation of the Common Open Policy Service (COPS) protocol of some Huawei products. The specific decoding function may occur out-of-bounds read when processes an incoming data packet. Successful exploit of these vulnerabilities may disrupt service on the affected device. (Vulnerability ID: HWPSIRT-2018-12275,HWPSIRT-2018-12276,HWPSIRT-2018-12277,HWPSIRT-2018-12278,HWPSIRT-2018-12279,HWPSIRT-2018-12280 and HWPSIRT-2018-12289) The seven vulnerabilities have been assigned seven Common Vulnerabilities and Exposures (CVE) IDs: CVE-2020-1818, CVE-2020-1819, CVE-2020-1820, CVE-2020-1821, CVE-2020-1822, CVE-2020-1823 and CVE-2020-1824.	2024-12-28	3.7
CVE-2020-1822	huawei - multiple products	There are multiple out of bounds (OOB) read vulnerabilities in the implementation of the Common Open Policy Service (COPS) protocol of some Huawei products. The specific decoding function may occur out-of-bounds read when processes an incoming data packet. Successful exploit of these	2024-12-28	3.7

		vulnerabilities may disrupt service on the affected device. (Vulnerability ID: HWPSIRT-2018-12275,HWPSIRT-2018-12276,HWPSIRT-2018-12277,HWPSIRT-2018-12278,HWPSIRT-2018-12279,HWPSIRT-2018-12280 and HWPSIRT-2018-12289) The seven vulnerabilities have been assigned seven Common Vulnerabilities and Exposures (CVE) IDs: CVE-2020-1818, CVE-2020-1819, CVE-2020-1820, CVE-2020-1821, CVE-2020-1822, CVE-2020-1823 and CVE-2020-1824.		
CVE-2020-1823	huawei - multiple products	There are multiple out of bounds (OOB) read vulnerabilities in the implementation of the Common Open Policy Service (COPS) protocol of some Huawei products. The specific decoding function may occur out-of-bounds read when processes an incoming data packet. Successful exploit of these vulnerabilities may disrupt service on the affected device. (Vulnerability ID: HWPSIRT-2018-12275,HWPSIRT-2018-12276,HWPSIRT-2018-12277,HWPSIRT-2018-12278,HWPSIRT-2018-12279,HWPSIRT-2018-12280 and HWPSIRT-2018-12289) The seven vulnerabilities have been assigned seven Common Vulnerabilities and Exposures (CVE) IDs: CVE-2020-1818, CVE-2020-1819, CVE-2020-1820, CVE-2020-1821, CVE-2020-1822, CVE-2020-1823 and CVE-2020-1824.	2024-12-28	3.7
CVE-2020-1824	huawei - multiple products	There are multiple out of bounds (OOB) read vulnerabilities in the implementation of the Common Open Policy Service (COPS) protocol of some Huawei products. The specific decoding function may occur out-of-bounds read when processes an incoming data packet. Successful exploit of these vulnerabilities may disrupt service on the affected device. (Vulnerability ID: HWPSIRT-2018-12275,HWPSIRT-2018-12276,HWPSIRT-2018-12277,HWPSIRT-2018-12278,HWPSIRT-2018-12279,HWPSIRT-2018-12280 and HWPSIRT-2018-12289) The seven vulnerabilities have been assigned seven Common Vulnerabilities and Exposures (CVE) IDs: CVE-2020-1818, CVE-2020-1819, CVE-2020-1820, CVE-2020-1821, CVE-2020-1822, CVE-2020-1823 and CVE-2020-1824.	2024-12-28	3.7
CVE-2020-9081	huawei - multiple products	There is an improper authorization vulnerability in some Huawei smartphones. An attacker could perform a series of operation in specific mode to exploit this vulnerability. Successful exploit could allow the attacker to bypass app lock. (Vulnerability ID: HWPSIRT-2019-12144) This vulnerability has been assigned a Common Vulnerabilities and Exposures (CVE) ID: CVE-2020-9081.	2024-12-27	3.5
CVE-2020-9082	huawei - HUAWEI Mate 20	There is an information disclosure vulnerability in several smartphones. The system has a logic judging error under certain scenario, the attacker should gain the permit to execute commands in ADB mode and then do a series of operation on the phone. Successful exploit could allow the attacker to gain certain information from certain apps locked by Applock. (Vulnerability ID: HWPSIRT-2019-07112) This vulnerability has been assigned a Common Vulnerabilities and Exposures (CVE) ID: CVE-2020-9082.	2024-12-27	3.5
CVE-2020-9089	huawei - HUAWEI P30 Pro	There is an information vulnerability in Huawei smartphones. A function in a module can be called without verifying the caller's access. Attackers with user access can exploit this vulnerability to obtain some information. This can lead to information leak. (Vulnerability ID: HWPSIRT-2019-12141) This vulnerability has been assigned a Common Vulnerabilities and Exposures (CVE) ID: CVE-2020-9089.	2024-12-27	3.3
CVE-2024-56512	apache software foundation - Apache NiFi	Apache NiFi 1.10.0 through 2.0.0 are missing fine-grained authorization checking for Parameter Contexts, referenced Controller Services, and referenced Parameter Providers, when creating new Process Groups. Creating a new Process Group can include binding to a Parameter Context, but in cases where the Process Group did not reference any Parameter values, the framework did not check user authorization for the bound Parameter Context. Missing authorization for a bound Parameter Context enabled clients to download non-sensitive Parameter values after creating the Process Group. Creating a new Process Group can also include referencing existing Controller Services or Parameter Providers. The framework did not check user authorization for referenced Controller Services or Parameter Providers, enabling clients to create Process Groups and use these components that were otherwise unauthorized. This vulnerability is limited in scope to authenticated users authorized to create Process Groups. The scope is further limited to deployments with component-based authorization policies. Upgrading to Apache NiFi 2.1.0 is the recommended mitigation, which includes authorization checking for Parameter and Controller Service references on Process Group creation.	2024-12-28	2.1

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.