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

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 11 فبراير إلى 17 فبراير. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 11th of February to 17th of February. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- **Critical: CVSS base score of 9.0-10.0**
- **High: CVSS base score of 7.0-8.9**
- **Medium: CVSS base score 4.0-6.9**
- **Low: CVSS base score 0.0-3.9**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2024-21401	microsoft - entra_jira_sso_plugin	Microsoft Entra Jira Single-Sign-On Plugin Elevation of Privilege Vulnerability	2024-02-13	9.8	Critical
CVE-2024-21413	microsoft - multiple products	Microsoft Outlook Remote Code Execution Vulnerability	2024-02-13	9.8	Critical
CVE-2024-23113	fortinet - multiple products	A use of externally-controlled format string in Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, FortiPAM versions 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiSwitchManager versions 7.2.0 through 7.2.3, 7.0.0 through 7.0.3 allows attacker to execute unauthorized code or commands via specially crafted packets.	2024-02-15	9.8	Critical
CVE-2024-23476	solarwinds - access_rights_manager	The SolarWinds Access Rights Manager (ARM) was found to be susceptible to a Directory Traversal Remote Code Execution Vulnerability. If exploited, this vulnerability allows an unauthenticated user to achieve the Remote Code Execution.	2024-02-15	9.6	Critical
CVE-2024-23477	solarwinds - access_rights_manager	The SolarWinds Access Rights Manager (ARM) was found to be susceptible to a Directory Traversal Remote Code Execution Vulnerability. If exploited, this vulnerability allows an unauthenticated user to achieve a Remote Code Execution.	2024-02-15	9.6	Critical
CVE-2024-23479	solarwinds - access_rights_manager	SolarWinds Access Rights Manager (ARM) was found to be susceptible to a Directory Traversal Remote Code Execution Vulnerability. If exploited, this vulnerability allows an unauthenticated user to achieve a Remote Code Execution.	2024-02-15	9.6	Critical
CVE-2024-20719	adobe - multiple products	Adobe Commerce versions 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into every admin page. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field, that could be leveraged to gain admin access.	2024-02-15	9.1	Critical
CVE-2024-20720	adobe - multiple products	Adobe Commerce versions 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead in arbitrary code execution by an attacker. Exploitation of this issue does not require user interaction.	2024-02-15	9.1	Critical
CVE-2023-40057	solarwinds - access_rights_manager	The SolarWinds Access Rights Manager was found to be susceptible to a Remote Code Execution Vulnerability. If exploited, this vulnerability allows an authenticated user to abuse a SolarWinds service resulting in remote code execution.	2024-02-15	9	Critical
CVE-2024-21372	microsoft - multiple products	Windows OLE Remote Code Execution Vulnerability	2024-02-13	8.8	High
CVE-2024-22024	ivanti - multiple products	An XML external entity or XXE vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x) and ZTA gateways which allows an attacker to access certain restricted resources without authentication.	2024-02-13	8.3	High
CVE-2024-21395	microsoft - dynamics_365	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2024-02-13	8.2	High

CVE-2024-23478	solarwinds - access_rights_manager	SolarWinds Access Rights Manager (ARM) was found to be susceptible to a Remote Code Execution Vulnerability. If exploited, this vulnerability allows an authenticated user to abuse a SolarWinds service, resulting in remote code execution.	2024-02-15	8	High
CVE-2024-0164	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contain an OS Command Injection Vulnerability in its svc_topstats utility. An authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary commands with elevated privileges.	2024-02-12	7.8	High
CVE-2024-0165	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_acldb_dump utility. An authenticated attacker could potentially exploit this vulnerability, leading to execution of arbitrary operating system commands with root privileges.	2024-02-12	7.8	High
CVE-2024-0166	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_tcpdump utility. An authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands with elevated privileges.	2024-02-12	7.8	High
CVE-2024-0167	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in the svc_topstats utility. An authenticated attacker could potentially exploit this vulnerability, leading to the ability to overwrite arbitrary files on the file system with root privileges.	2024-02-12	7.8	High
CVE-2024-0168	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains a Command Injection Vulnerability in svc_oscheck utility. An authenticated attacker could potentially exploit this vulnerability, leading to the ability to inject arbitrary operating system commands. This vulnerability allows an authenticated attacker to execute commands with root privileges.	2024-02-12	7.8	High
CVE-2024-0170	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_cava utility. An authenticated attacker could potentially exploit this vulnerability, escaping the restricted shell and execute arbitrary operating system commands with root privileges.	2024-02-12	7.8	High
CVE-2024-22222	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability within its svc_udoctor utility. An authenticated malicious user with local access could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application.	2024-02-12	7.8	High
CVE-2024-22223	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability within its svc_cbr utility. An authenticated malicious user with local access could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application.	2024-02-12	7.8	High
CVE-2024-22224	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_nas utility. An authenticated attacker could potentially exploit this vulnerability, escaping the restricted shell and execute arbitrary operating system commands with root privileges.	2024-02-12	7.8	High
CVE-2024-22225	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_supportassist utility. An authenticated attacker could potentially exploit this vulnerability, leading to execution of arbitrary operating system commands with root privileges.	2024-02-12	7.8	High
CVE-2024-22227	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_dc utility. An authenticated attacker could potentially exploit this vulnerability, leading to the ability execute commands with root privileges.	2024-02-12	7.8	High
CVE-2024-22228	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains an OS Command Injection Vulnerability in its svc_cifssupport utility. An authenticated attacker could potentially exploit this vulnerability, escaping the restricted shell and execute arbitrary operating system commands with root privileges.	2024-02-12	7.8	High
CVE-2024-23795	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected application	2024-02-13	7.8	High

		contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process.			
CVE-2024-23796	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	High
CVE-2024-23797	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected applications contain a stack overflow vulnerability while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	High
CVE-2024-23798	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected applications contain a stack overflow vulnerability while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	High
CVE-2024-23802	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	High
CVE-2024-23803	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions), Tecnomatix Plant Simulation V2302 (All versions < V2302.0007). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	High
CVE-2024-23804	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0012), Tecnomatix Plant Simulation V2302 (All versions < V2302.0006). The affected applications contain a stack overflow vulnerability while parsing specially crafted PSOBJ files. This could allow an attacker to execute code in the context of the current process.	2024-02-13	7.8	High
CVE-2024-20673	microsoft - multiple products	Microsoft Office Remote Code Execution Vulnerability	2024-02-13	7.8	High
CVE-2024-21338	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2024-02-13	7.8	High
CVE-2024-21384	microsoft - multiple products	Microsoft Office OneNote Remote Code Execution Vulnerability	2024-02-13	7.8	High
CVE-2024-20723	adobe - substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by a Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	High
CVE-2024-20740	adobe - substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	High
CVE-2024-20741	adobe - substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by a Write-what-where Condition vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	High
CVE-2024-20742	adobe - substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	High
CVE-2024-20743	adobe - substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	High
CVE-2024-20744	adobe - substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	7.8	High
CVE-2024-21327	microsoft - dynamics_365	Microsoft Dynamics 365 Customer Engagement Cross-Site Scripting Vulnerability	2024-02-13	7.6	High

CVE-2024-21328	microsoft - dynamics_365	Dynamics 365 Sales Spoofing Vulnerability	2024-02-13	7.6	High
CVE-2024-21389	microsoft - dynamics_365	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2024-02-13	7.6	High
CVE-2024-21393	microsoft - dynamics_365	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2024-02-13	7.6	High
CVE-2024-21394	microsoft - dynamics_365	Dynamics 365 Field Service Spoofing Vulnerability	2024-02-13	7.6	High
CVE-2024-21396	microsoft - dynamics_365	Dynamics 365 Sales Spoofing Vulnerability	2024-02-13	7.6	High
CVE-2024-20667	microsoft - multiple products	Azure DevOps Server Remote Code Execution Vulnerability	2024-02-13	7.5	High
CVE-2024-21342	microsoft - multiple products	Windows DNS Client Denial of Service Vulnerability	2024-02-13	7.5	High
CVE-2024-21386	microsoft - multiple products	.NET Denial of Service Vulnerability	2024-02-13	7.5	High
CVE-2024-21404	microsoft - multiple products	.NET Denial of Service Vulnerability	2024-02-13	7.5	High
CVE-2023-50387	redhat - multiple products	Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.	2024-02-14	7.5	High
CVE-2024-21329	microsoft - azure_connected_machine_agent	Azure Connected Machine Agent Elevation of Privilege Vulnerability	2024-02-13	7.3	High
CVE-2023-45581	fortinet - multiple products	An improper privilege management vulnerability [CWE-269] in Fortinet FortiClientEMS version 7.2.0 through 7.2.2 and before 7.0.10 allows an Site administrator with Super Admin privileges to perform global administrative operations affecting other sites via crafted HTTP or HTTPS requests.	2024-02-15	7.2	High
CVE-2024-21402	microsoft - 365_apps	Microsoft Outlook Elevation of Privilege Vulnerability	2024-02-13	7.1	High
CVE-2024-21371	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2024-02-13	7	High
CVE-2024-21405	microsoft - multiple products	Microsoft Message Queuing (MSMQ) Elevation of Privilege Vulnerability	2024-02-13	7	High
CVE-2024-21341	microsoft - multiple products	Windows Kernel Remote Code Execution Vulnerability	2024-02-13	6.8	Medium
CVE-2024-21381	microsoft - azure_active_directory	Microsoft Azure Active Directory B2C Spoofing Vulnerability	2024-02-13	6.8	Medium
CVE-2024-1430	netgear - r7000_firmware	A vulnerability has been found in Netgear R7000 1.0.11.136_10.2.120 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /currentsetting.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. The identifier VDB-253381 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-11	6.5	Medium
CVE-2024-1431	netgear - r7000_firmware	A vulnerability was found in Netgear R7000 1.0.11.136_10.2.120 and classified as problematic. Affected by this issue is some unknown functionality of the file /debuginfo.htm of the component Web Management Interface. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. VDB-253382 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-02-11	6.5	Medium
CVE-2024-22221	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains SQL Injection vulnerability. An authenticated attacker could potentially exploit this vulnerability, leading to exposure of sensitive information.	2024-02-12	6.5	Medium
CVE-2024-22226	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contain a path traversal vulnerability in its svc_supportassist utility. An authenticated attacker could potentially exploit this vulnerability, to gain unauthorized write access to the files stored on the server filesystem, with elevated privileges.	2024-02-12	6.5	Medium
CVE-2024-20718	adobe - multiple products	Adobe Commerce versions 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to trick a victim into performing actions they did not intend to do, which could be used to bypass security measures and gain unauthorized access. Exploitation of this issue requires user interaction, typically in the form of the victim clicking a link or visiting a malicious website.	2024-02-15	6.5	Medium

CVE-2024-23799	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions), Tecnomatix Plant Simulation V2302 (All versions < V2302.0007). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted SPP files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-02-13	5.5	Medium
CVE-2024-23800	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions), Tecnomatix Plant Simulation V2302 (All versions < V2302.0007). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted SPP files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-02-13	5.5	Medium
CVE-2024-23801	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions), Tecnomatix Plant Simulation V2302 (All versions < V2302.0007). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted SPP files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-02-13	5.5	Medium
CVE-2024-20722	adobe - substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	5.5	Medium
CVE-2024-20724	adobe - substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	5.5	Medium
CVE-2024-20725	adobe - substance_3d_painter	Substance3D - Painter versions 9.1.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-02-15	5.5	Medium
CVE-2024-0169	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains a cross-site scripting (XSS) vulnerability. An authenticated attacker could potentially exploit this vulnerability, leading users to download and execute malicious software crafted by this product's feature to compromise their systems.	2024-02-12	5.4	Medium
CVE-2024-22230	dell - unity_operating_environment	Dell Unity, versions prior to 5.4, contains a Cross-site scripting vulnerability. An authenticated attacker could potentially exploit this vulnerability, stealing session information, masquerading as the affected user or carry out any actions that this user could perform, or to generally control the victim's browser.	2024-02-12	5.4	Medium
CVE-2024-20717	adobe - multiple products	Adobe Commerce versions 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-02-15	5.4	Medium
CVE-2024-21397	microsoft - multiple products	Microsoft Azure File Sync Elevation of Privilege Vulnerability	2024-02-13	5.3	Medium
CVE-2024-21374	microsoft - teams	Microsoft Teams for Android Information Disclosure	2024-02-13	5	Medium
CVE-2023-44253	fortinet - multiple products	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in Fortinet FortiManager version 7.4.0 through 7.4.1 and before 7.2.5, FortiAnalyzer version 7.4.0 through 7.4.1 and before 7.2.5 and FortiAnalyzer-BigData before 7.2.5 allows an adom administrator to enumerate other adoms and device names via crafted HTTP or HTTPS requests.	2024-02-15	5	Medium
CVE-2024-20716	adobe - multiple products	Adobe Commerce versions 2.4.6-p3, 2.4.5-p5, 2.4.4-p6 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to an application denial-of-service. A high-privileged attacker could leverage this vulnerability to exhaust system resources, causing the application to slow down or crash. Exploitation of this issue does not require user interaction.	2024-02-15	4.9	Medium
CVE-2023-47537	fortinet - multiple products	An improper certificate validation vulnerability in Fortinet FortiOS 7.0.0 - 7.0.13, 7.2.0 - 7.2.6 and 7.4.0 - 7.4.1 allows a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the FortiLink communication channel between the FortiOS device and FortiSwitch.	2024-02-15	4.8	Medium
CVE-2024-21340	microsoft - multiple products	Windows Kernel Information Disclosure Vulnerability	2024-02-13	4.6	Medium

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.