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 ٢١ يوليو إلى ٢٧ يوليو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

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 21st July to 27th of July. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2024-38437	D-Link	D-Link - CWE-288:Authentication Bypass Using an Alternate Path or Channel	2024-07-21	9.8	Critical
CVE-2024-38438	D-Link	D-Link - CWE-294: Authentication Bypass by Capture-replay	2024-07-21	9.8	Critical
CVE-2024-38164	Microsoft	An improper access control vulnerability in GroupMe allows an a unauthenticated attacker to elevate privileges over a network by convincing a user to click on a malicious link.	2024-07-23	9.6	Critical
CVE-2024-37998	Siemens	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V5.40), SICORE Base system (All versions < V1.4.0). The password of administrative accounts of the affected applications can be reset without requiring the knowledge of the current password, given the auto login is enabled. This could allow an unauthorized attacker to obtain administrative access of the affected applications.	2024-07-22	9.3	Critical
CVE-2024-38871	ManageEngine	Zohocorp ManageEngine Exchange Reporter Plus versions 5717 and below are vulnerable to the authenticated SQL injection in the reports module.	2024-07-26	8.3	High
CVE-2024-38872	ManageEngine	Zohocorp ManageEngine Exchange Reporter Plus versions 5717 and below are vulnerable to the authenticated SQL injection in the monitoring module.	2024-07-26	8.3	High
CVE-2024-38176	Microsoft	An improper restriction of excessive authentication attempts in GroupMe allows a unauthenticated attacker to elevate privileges over a network.	2024-07-23	8.1	High
CVE-2022-32759	IBM	IBM Security Directory Integrator 7.2.0 and IBM Security Verify Directory Integrator 10.0.0 uses insufficient session expiration which could allow an unauthorized user to obtain sensitive information. IBM X-Force ID: 228565.	2024-07-25	7.5	High
CVE-2024-38508	Lenovo	A privilege escalation vulnerability was discovered in the web interface or SSH captive command shell interface of XCC that could allow an authenticated XCC user with elevated privileges to perform command injection via a specially crafted request.	2024-07-26	7.2	High
CVE-2024-38509	Lenovo	A privilege escalation vulnerability was discovered in XCC that could allow an authenticated XCC user with elevated privileges to execute arbitrary code via a specially crafted IPMI command.	2024-07-26	7.2	High
CVE-2024-38510	Lenovo	A privilege escalation vulnerability was discovered in the SSH captive command shell interface that could allow an authenticated XCC user with elevated privileges to perform command injection via specially crafted file uploads.	2024-07-26	7.2	High
CVE-2024-38511	Lenovo	A privilege escalation vulnerability was discovered in an upload processing functionality of XCC that could allow an authenticated XCC user with elevated privileges to perform command injection via specially crafted file uploads.	2024-07-26	7.2	High
CVE-2024-38512	Lenovo	A privilege escalation vulnerability was discovered in XCC that could allow an authenticated XCC user with elevated privileges to perform command injection via specially crafted IPMI commands.	2024-07-26	7.2	High
CVE-2024-39601	Siemens	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V5.40), SICORE Base	2024-07-22	7.1	High

		system (All versions < V1.4.0). Affected devices allow a remote authenticated user or an unauthenticated user with physical access to downgrade the firmware of the device. This could allow an attacker to downgrade the device to older versions with known vulnerabilities.			
CVE-2024-39672	Huawei	Memory request logic vulnerability in the memory module. Impact: Successful exploitation of this vulnerability will affect integrity and availability.	2024-07-25	7.1	High
CVE-2024-39673	Huawei	Vulnerability of serialisation/deserialisation mismatch in the iAware module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-07-25	7.1	High
CVE-2024-7153	Netgear	A vulnerability classified as problematic has been found in Netgear WN604 up to 20240719. Affected is an unknown function of the file siteSurvey.php. The manipulation leads to direct request. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-272556. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-07-27	6.9	Medium
CVE-2024-1575	Zyxel	The improper privilege management vulnerability in the Zyxel WBE660S firmware version 6.70(ACGG.3) and earlier versions could allow an authenticated user to escalate privileges and download the configuration files on a vulnerable device.	2024-07-23	6.5	Medium
CVE-2023-32471	Dell	Dell Edge Gateway BIOS, versions 3200 and 5200, contains an out-of-bounds read vulnerability. A local authenticated malicious user with high privileges could potentially exploit this vulnerability to read contents of stack memory and use this information for further exploits.	2024-07-24	6	Medium
CVE-2024-40689	IBM	IBM InfoSphere Information Server 11.7 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify, or delete information in the back-end database. IBM X-Force ID: 297719.	2024-07-26	6	Medium
CVE-2024-38103	Microsoft	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2024-07-25	5.9	Medium
CVE-2023-32466	Dell	Dell Edge Gateway BIOS, versions 3200 and 5200, contains an out-of-bounds write vulnerability. A local authenticated malicious user with high privileges could potentially exploit this vulnerability leading to exposure of some UEFI code, leading to arbitrary code execution or escalation of privilege.	2024-07-24	5.7	Medium
CVE-2024-41836	Adobe	InDesign Desktop versions ID18.5.2, ID19.3 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-07-23	5.5	Medium
CVE-2023-7271	Huawei	Privilege escalation vulnerability in the NMS module Impact: Successful exploitation of this vulnerability will affect availability.	2024-07-25	5.5	Medium
CVE-2024-39670	Huawei	Privilege escalation vulnerability in the account synchronisation module. Impact: Successful exploitation of this vulnerability will affect availability.	2024-07-25	5.5	Medium
CVE-2024-39671	Huawei	Access control vulnerability in the security verification module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-07-25	5.5	Medium
CVE-2024-39674	Huawei	Plaintext vulnerability in the Gallery search module. Impact: Successful exploitation of this vulnerability will affect availability.	2024-07-25	5.5	Medium
CVE-2024-34128	Adobe	Adobe Experience Manager versions 6.5.20 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.	2024-07-23	5.4	Medium
CVE-2024-28772	IBM	IBM Security Directory Integrator 7.2.0 and IBM Security Verify Directory Integrator 10.0.0 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: 285645.	2024-07-25	5.4	Medium
CVE-2024-41839	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could lead to a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect the integrity of the page. Exploitation of this issue requires user interaction.	2024-07-23	4.1	Medium
CVE-2024-21684	Atlassian	There is a low severity open redirect vulnerability within affected versions of Bitbucket Data Center. Versions of Bitbucket DC from 8.0.0 to 8.9.12 and 8.19.0 to 8.19.1 are affected by this	2024-07-24	3.1	Low

		vulnerability. It is patched in 8.9.13 and 8.19.2. This open redirect vulnerability, with a CVSS Score of 3.1 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N, allows an unauthenticated attacker to redirect a victim user upon login to Bitbucket Data Center to any arbitrary site which can be utilized for further exploitation which has low impact to confidentiality, no impact to integrity, no impact to availability, and requires user interaction. Atlassian recommends that Bitbucket Data Center customers upgrade to the version. If you are unable to do so, upgrade your instance to one of the supported fixed versions.			
CVE-2024-4786	Lenovo	An improper validation vulnerability was reported in the Lenovo Tab K10 that could allow a specially crafted application to keep the device on.	2024-07-26	2.8	Low
CVE-2024-37533	IBM	IBM InfoSphere Information Server 11.7 could disclose sensitive user information to another user with physical access to the machine. IBM X-Force ID: 294727.	2024-07-24	2.4	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.