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 17 مارس إلى 24 مارس. 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 17th of March to 24th of March. 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-2024-28916	Microsoft	Xbox Gaming Services Elevation of Privilege Vulnerability	2024-03-21	8.8	High
CVE-2024-21677	Atlassian	This High severity Path Traversal vulnerability was introduced in version 6.13.0 of Confluence Data Center. This Path Traversal vulnerability, with a CVSS Score of 8.3, allows an unauthenticated attacker to exploit an undefinable vulnerability which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Data Center Atlassian recommends that Confluence Data Center customers upgrade to the latest version and that Confluence Server customers upgrade to the latest 8.5.x LTS version. If you are unable to do so, upgrade your instance to one of the specified supported fixed versions See the release notes https://confluence.atlassian.com/doc/confluence-release-notes-327.html You can download the latest version of Confluence Data Center and Server from the download center https://www.atlassian.com/software/confluence/download-archives. This vulnerability was reported via our Bug Bounty program.	2024-03-19	8.3	High
CVE-2024-20767	Adobe	ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Access Control vulnerability that could lead to arbitrary file system read. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized access to sensitive files and perform arbitrary file system write. Exploitation of this issue does not require user interaction.	2024-03-18	8.2	High
CVE-2024-20745	Adobe	Premiere Pro versions 24.1, 23.6.2 and earlier are affected by a Heap-based 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.	2024-03-18	7.8	High
CVE-2024-20746	Adobe	Premiere Pro versions 24.1, 23.6.2 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.	2024-03-18	7.8	High
CVE-2024-20752	Adobe	Bridge versions 13.0.5, 14.0.1 and earlier are affected by a Use After Free 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.	2024-03-18	7.8	High

CVE-2024-20755	Adobe	Bridge versions 13.0.5, 14.0.1 and earlier are affected by a Heap-based 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.	2024-03-18	7.8	High
CVE-2024-20756	Adobe	Bridge versions 13.0.5, 14.0.1 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.	2024-03-18	7.8	High
CVE-2024-20761	Adobe	Animate versions 24.0, 23.0.3 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.	2024-03-18	7.8	High
CVE-2024-20754	Adobe	Lightroom Desktop versions 7.1.2 and earlier are affected by an Untrusted Search Path vulnerability that could result in arbitrary code execution in the context of the current user. If the application uses a search path to locate critical resources such as programs, then an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-03-18	7.5	High
CVE-2024-29059	Microsoft	.NET Framework Information Disclosure Vulnerability	2024-03-23	7.5	High
CVE-2024-22453	Dell	Dell PowerEdge Server BIOS contains a heap-based buffer overflow vulnerability. A local high privileged attacker could potentially exploit this vulnerability to write to otherwise unauthorized memory.	2024-03-19	7.2	High
CVE-2023-35899	IBM	IBM Cloud Pak for Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 259354.	2024-03-21	7	High
CVE-2024-22352	IBM	IBM InfoSphere Information Server 11.7 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 280361.	2024-03-21	6.5	Medium
CVE-2024-27277	IBM	The private key for the IBM Storage Protect Plus Server 10.1.0 through 10.1.16 certificate can be disclosed, undermining the security of the certificate. IBM X-Force ID: 285205.	2024-03-21	6.2	Medium
CVE-2023-35888	IBM	IBM Security Verify Governance 10.0.2 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 258375.	2024-03-20	5.9	Medium
CVE-2024-20757	Adobe	Bridge versions 13.0.5, 14.0.1 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.	2024-03-18	5.5	Medium
CVE-2024-20762	Adobe	Animate versions 24.0, 23.0.3 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.	2024-03-18	5.5	Medium
CVE-2024-20763	Adobe	Animate versions 24.0, 23.0.3 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.	2024-03-18	5.5	Medium
CVE-2024-20764	Adobe	Animate versions 24.0, 23.0.3 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.	2024-03-18	5.5	Medium
CVE-2024-20760	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-20768	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26028	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that	2024-03-18	5.4	Medium

		could be abused by an 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.			
CVE-2024-26030	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26031	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26032	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable web pages. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable script. This could result in arbitrary code execution in the context of the victim's browser. Exploitation of this issue requires user interaction.	2024-03-18	5.4	Medium
CVE-2024-26033	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26034	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26035	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26038	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26040	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26041	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26042	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable web pages. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable script. This could result in arbitrary code execution in the context of the victim's browser.	2024-03-18	5.4	Medium
CVE-2024-26043	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26044	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into a webpage. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable	2024-03-18	5.4	Medium

		script. This could result in arbitrary code execution in the context of the victim's browser.			
CVE-2024-26045	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26052	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26056	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26059	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26061	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26062	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26064	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into a webpage. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable script. This could result in arbitrary code execution in the context of the victim's browser. Exploitation of this issue requires user interaction.	2024-03-18	5.4	Medium
CVE-2024-26065	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26067	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26069	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26073	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26080	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable web pages. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable script.	2024-03-18	5.4	Medium
CVE-2024-26094	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into	2024-03-18	5.4	Medium

		vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.			
CVE-2024-26096	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26101	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	Medium
CVE-2024-26102	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	Medium
CVE-2024-26103	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	Medium
CVE-2024-26104	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	Medium
CVE-2024-26105	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	Medium
CVE-2024-26106	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	Medium
CVE-2024-26107	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	Medium
CVE-2024-26118	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-03-18	5.4	Medium
CVE-2024-26120	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26124	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26125	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	5.4	Medium
CVE-2024-26063	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by an Information Exposure vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to gain unauthorized access to sensitive information, potentially bypassing security measures. Exploitation of this issue does not require user interaction.	2024-03-18	5.3	Medium
CVE-2024-26119	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized access. Exploitation of this issue does not require user interaction.	2024-03-18	5.3	Medium

CVE-2023-45177	IBM	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS and 9.3 CD is vulnerable to a denial-of-service attack due to an error within the MQ clustering logic. IBM X-Force ID: 268066.	2024-03-20	5.3	Medium
CVE-2022-32751	IBM	IBM Security Verify Directory 10.0.0 could disclose sensitive server information that could be used in further attacks against the system. IBM X-Force ID: 228437.	2024-03-22	5.3	Medium
CVE-2024-26050	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	4.8	Medium
CVE-2022-32754	IBM	IBM Security Verify Directory 10.0.0 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: 228445.	2024-03-22	4.8	Medium
CVE-2024-26247	Microsoft	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2024-03-22	4.7	Medium
CVE-2022-32753	IBM	IBM Security Verify Directory 10.0.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 228444.	2024-03-22	4.5	Medium
CVE-2024-25942	Dell	Dell PowerEdge Server BIOS contains an Improper SMM communication buffer verification vulnerability. A physical high privileged attacker could potentially exploit this vulnerability leading to arbitrary writes to SMRAM.	2024-03-19	4.4	Medium
CVE-2024-26196	Microsoft	Microsoft Edge for Android (Chromium-based) Information Disclosure Vulnerability	2024-03-21	4.3	Medium
CVE-2023-47715	IBM	IBM Storage Protect Plus Server 10.1.0 through 10.1.16 could allow an authenticated user with read-only permissions to add or delete entries from an existing HyperVisor configuration. IBM X-Force ID: 271538.	2024-03-21	4.3	Medium
CVE-2024-29057	Microsoft	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-03-22	4.3	Medium
CVE-2024-26051	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an 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.	2024-03-18	3.4	Low
CVE-2022-32756	IBM	IBM Security Verify Directory 10.0.0 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. IBM X-Force ID: 228507.	2024-03-22	2.7	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.