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 ٢٦ مايو إلى ١ يونيو. 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 26th of May to 1st of June. 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-2024-29822	Ivanti	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	2024-05-31	9.6	Critical
CVE-2024-29823	Ivanti	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	2024-05-31	9.6	Critical
CVE-2024-29824	Ivanti	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	2024-05-31	9.6	Critical
CVE-2024-29825	Ivanti	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	2024-05-31	9.6	Critical
CVE-2024-29826	Ivanti	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	2024-05-31	9.6	Critical
CVE-2024-29827	Ivanti	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an unauthenticated attacker within the same network to execute arbitrary code.	2024-05-31	9.6	Critical
CVE-2024-5274	Google	Type Confusion in V8 in Google Chrome prior to 125.0.6422.112 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2024-05-28	8.8	High
CVE-2024-22059	Ivanti	A SQL injection vulnerability in web component of Ivanti Neurons for ITSM allows a remote authenticated user to read/modify/delete information in the underlying database. This may also lead to DoS.	2024-05-31	8.8	High
CVE-2024-35142	IBM	IBM Security Verify Access Docker 10.0.0 through 10.0.6 could allow a local user to escalate their privileges due to execution of unnecessary privileges. IBM X-Force ID: 292418.	2024-05-31	8.4	High
CVE-2024-29828	Ivanti	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an authenticated attacker within the same network to execute arbitrary code.	2024-05-31	8.4	High
CVE-2024-29829	Ivanti	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an authenticated attacker within the same network to execute arbitrary code.	2024-05-31	8.4	High
CVE-2024-29830	Ivanti	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an authenticated attacker within the same network to execute arbitrary code.	2024-05-31	8.4	High
CVE-2024-29846	Ivanti	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2022 SU5 and prior allows an authenticated attacker within the same network to execute arbitrary code.	2024-05-31	8.4	High
CVE-2023-38551	Ivanti	A CRLF Injection vulnerability in Ivanti Connect Secure (9.x, 22.x) allows an authenticated high-privileged user to inject malicious code on a victim's browser, thereby leading to cross-site scripting attack.	2024-05-31	8.2	High
CVE-2023-52547	Huawei	Huawei Matebook D16(Model: CREM-WXX9, BIOS: v2.26. Memory Corruption in SMI Handler of HddPassword SMM Module. This can be leveraged by a malicious OS attacker to corrupt data structures	2024-05-28	7.8	High

		stored at the beginning of SMRAM and can potentially lead to code execution in SMM.			
CVE-2023-52548	Huawei	Huawei Matebook D16(Model: CREM-WXX9, BIOS: v2.26) Arbitrary Memory Corruption in SMI Handler of ThisiServicesSmm SMM module. This can be leveraged by a malicious OS attacker to corrupt arbitrary SMRAM memory and, in turn, lead to code execution in SMM	2024-05-28	7.8	High
CVE-2023-52710	Huawei	Huawei Matebook D16(Model: CREM-WXX9, BIOS: v2.26), As the communication buffer size hasn't been properly validated to be of the expected size, it can partially overlap with the beginning SMRAM.This can be leveraged by a malicious OS attacker to corrupt data structures stored at the beginning of SMRAM and can potentially lead to code execution in SMM.	2024-05-28	7.8	High
CVE-2023-52711	Huawei	Various Issues Due To Exposed SMI Handler in AmdPspP2CmboxV2. The first issue can be leveraged to bypass the protections that have been put in place by previous UEFI phases to prevent direct access to the SPI flash. The second issue can be used to both leak and corrupt SMM memory thus potentially leading code execution in SMM	2024-05-28	7.8	High
CVE-2023-52712	Huawei	Various Issues Due To Exposed SMI Handler in AmdPspP2CmboxV2. The first issue can be leveraged to bypass the protections that have been put in place by previous UEFI phases to prevent direct access to the SPI flash. The second issue can be used to both leak and corrupt SMM memory, thus potentially leading code execution in SMM	2024-05-28	7.8	High
CVE-2023-38042	Ivanti	A local privilege escalation vulnerability in Ivanti Secure Access Client for Windows allows a low privileged user to execute code as SYSTEM.	2024-05-31	7.8	High
CVE-2024-22058	Ivanti	A buffer overflow allows a low privilege user on the local machine that has the EPM Agent installed to execute arbitrary code with elevated permissions in Ivanti EPM 2021.1 and older.	2024-05-31	7.8	High
CVE-2024-35140	IBM	IBM Security Verify Access Docker 10.0.0 through 10.0.6 could allow a local user to escalate their privileges due to improper certificate validation. IBM X-Force ID: 292416.	2024-05-31	7.7	High
CVE-2024-28974	Dell	Dell Data Protection Advisor, version(s) 19.9, contain(s) an Inadequate Encryption Strength vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Denial of service.	2024-05-29	7.6	High
CVE-2023-42005	IBM	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data 3.5, 4.0, 4.5, 4.6, 4.7, and 4.8 could allow a user with access to the Kubernetes pod, to make system calls compromising the security of containers. IBM X-Force ID: 265264.	2024-05-29	7.4	High
CVE-2023-46810	Ivanti	A local privilege escalation vulnerability in Ivanti Secure Access Client for Linux before 22.7R1, allows a low privileged user to execute code as root.	2024-05-31	7.3	High
CVE-2022-48681	Huawei	Some Huawei smart speakers have a memory overflow vulnerability. Successful exploitation of this vulnerability may cause certain functions to fail.	2024-05-28	7.2	High
CVE-2024-29848	Ivanti	An unrestricted file upload vulnerability in web component of Ivanti Avalanche before 6.4.x allows an authenticated, privileged user to execute arbitrary commands as SYSTEM.	2024-05-31	7.2	High
CVE-2024-32760	F5	When NGINX Plus or NGINX OSS are configured to use the HTTP/3 QUIC module, undisclosed HTTP/3 encoder instructions can cause NGINX worker processes to terminate or cause or other potential impact.	2024-05-29	6.5	Medium
CVE-2024-2451	TeamViewer	Improper fingerprint validation in the TeamViewer Client (Full & Host) prior Version 15.54 for Windows and macOS allows an attacker with administrative user rights to further elevate privileges via executable sideloading.	2024-05-28	6.4	Medium
CVE-2024-31908	IBM	IBM Planning Analytics Local 2.0 and 2.1 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: 289890.	2024-05-31	6.4	Medium
CVE-2024-27313	ManageEngine	Zoho ManageEngine PAM360 is vulnerable to Stored XSS vulnerability. This vulnerability is applicable only in the version 6610.	2024-05-29	6.3	Medium
CVE-2024-36037	ManageEngine	Zoho ManageEngine ADAudit Plus versions 7260 and below allows unauthorized local agent machine users to view the session recordings.	2024-05-27	5.5	Medium
CVE-2022-43575	IBM	IBM Aspera Console 3.4.0 through 3.4.2 PL5 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: 238645.	2024-05-30	5.4	Medium
CVE-2024-31889	IBM	IBM Planning Analytics Local 2.0 and 2.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended	2024-05-31	5.4	Medium

		functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 288136.			
CVE-2024-31907	IBM	IBM Planning Analytics Local 2.0 and 2.1 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: 289889.	2024-05-31	5.4	Medium
CVE-2024-27310	ManageEngine	Zoho ManageEngine ADSelfService Plus versions below 6401 are vulnerable to the DOS attack due to the malicious LDAP query.	2024-05-27	5.3	Medium
CVE-2024-34161	F5	When NGINX Plus or NGINX OSS are configured to use the HTTP/3 QUIC module and the network infrastructure supports a Maximum Transmission Unit (MTU) of 4096 or greater without fragmentation, undisclosed QUIC packets can cause NGINX worker processes to leak previously freed memory.	2024-05-29	5.3	Medium
CVE-2024-35200	F5	When NGINX Plus or NGINX OSS are configured to use the HTTP/3 QUIC module, undisclosed HTTP/3 requests can cause NGINX worker processes to terminate.	2024-05-29	5.3	Medium
CVE-2024-28793	IBM	IBM Engineering Workflow Management 7.0.2 and 7.0.3 is vulnerable to stored cross-site scripting. Under certain configurations, 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: 286830.	2024-05-28	4.9	Medium
CVE-2023-37411	IBM	IBM Aspera Faspex 5.0.0 through 5.0.6 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: 260139.	2024-05-28	4.8	Medium
CVE-2024-31079	F5	When NGINX Plus or NGINX OSS are configured to use the HTTP/3 QUIC module, undisclosed HTTP/3 requests can cause NGINX worker processes to terminate or cause other potential impact. This attack requires that a request be specifically timed during the connection draining process, which the attacker has no visibility and limited influence over.	2024-05-29	4.8	Medium
CVE-2022-43384	IBM	IBM Aspera Console 3.4.0 through 3.4.2 PL5 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: 238645.	2024-05-30	4.6	Medium
CVE-2024-36036	ManageEngine	Zoho ManageEngine ADAudit Plus versions 7260 and below allows unauthorized local agent machine users to access sensitive information and modifying the agent configuration.	2024-05-27	4.2	Medium
CVE-2022-43841	IBM	IBM Aspera Console 3.4.0 through 3.4.2 PL9 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 239078.	2024-05-30	4	Medium
CVE-2024-22338	IBM	IBM Security Verify Access OIDC Provider 22.09 through 23.03 could disclose sensitive information to a local user due to hazardous input validation. IBM X-Force ID: 279978.	2024-05-31	4	Medium
CVE-2024-27314	ManageEngine	Zoho ManageEngine ServiceDesk Plus versions below 14730, ServiceDesk Plus MSP below 14720 and SupportCenter Plus below 14720 are vulnerable to stored XSS in the Custom Actions menu on the request details. This vulnerability can be exploited only by the SDAdmin role users.	2024-05-27	2.4	Low