الهيئــة الوطنيــة
للأمــن 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 10th of March to 17th 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**

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 10 مارس إلى 17 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**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-36554	Fortinet	A improper access control in Fortinet FortiManager version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.10, version 6.4.0 through 6.4.13, 6.2 all versions allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.	2024-03-12	9.8	Critical
CVE-2023-42789	Fortinet	A out-of-bounds write in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.	2024-03-12	9.8	Critical
CVE-2023-48788	Fortinet	A improper neutralization of special elements used in an sql command ('sql injection') in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, FortiClientEMS 7.0.1 through 7.0.10 allows attacker to execute unauthorized code or commands via specially crafted packets.	2024-03-12	9.8	Critical
CVE-2024-21334	Microsoft	Open Management Infrastructure (OMI) Remote Code Execution Vulnerability	2024-03-12	9.8	Critical
CVE-2024-21400	Microsoft	Microsoft Azure Kubernetes Service Confidential Container Elevation of Privilege Vulnerability	2024-03-12	9	Critical
CVE-2023-46717	Fortinet	An improper authentication vulnerability [CWE-287] in FortiOS versions 7.4.1 and below, versions 7.2.6 and below, and versions 7.0.12 and below when configured with FortiAuthenticator in HA may allow a readonly user to gain read-write access via successive login attempts.	2024-03-12	8.8	High
CVE-2023-47534	Fortinet	A improper neutralization of formula elements in a csv file in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.10, 6.4.0 through 6.4.9, 6.2.0 through 6.2.9, 6.0.0 through 6.0.8 allows attacker to execute unauthorized code or commands via specially crafted packets.	2024-03-12	8.8	High
CVE-2024-21411	Microsoft	Skype for Consumer Remote Code Execution Vulnerability	2024-03-12	8.8	High
CVE-2024-21435	Microsoft	Windows OLE Remote Code Execution Vulnerability	2024-03-12	8.8	High
CVE-2024-21440	Microsoft	Microsoft ODBC Driver Remote Code Execution Vulnerability	2024-03-12	8.8	High
CVE-2024-21441	Microsoft	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-03-12	8.8	High
CVE-2024-21444	Microsoft	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-03-12	8.8	High
CVE-2024-21450	Microsoft	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-03-12	8.8	High
CVE-2024-21451	Microsoft	Microsoft ODBC Driver Remote Code Execution Vulnerability	2024-03-12	8.8	High
CVE-2024-26159	Microsoft	Microsoft ODBC Driver Remote Code Execution Vulnerability	2024-03-12	8.8	High
CVE-2024-26161	Microsoft	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-03-12	8.8	High
CVE-2024-26162	Microsoft	Microsoft ODBC Driver Remote Code Execution Vulnerability	2024-03-12	8.8	High
CVE-2024-26164	Microsoft	Microsoft Django Backend for SQL Server Remote Code Execution Vulnerability	2024-03-12	8.8	High
CVE-2024-26165	Microsoft	Visual Studio Code Elevation of Privilege Vulnerability	2024-03-12	8.8	High

CVE-2024-26166	Microsoft	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2024-03-12	8.8	High
CVE-2024-26198	Microsoft	Microsoft Exchange Server Remote Code Execution Vulnerability	2024-03-12	8.8	High
CVE-2024-27266	IBM	IBM Maximo Application Suite 7.6.1.3 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 284566.	2024-03-14	8.2	High
CVE-2023-42790	Fortinet	A stack-based buffer overflow in Fortinet FortiOS 7.4.0 through 7.4.1, 7.2.0 through 7.2.5, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, FortiProxy 7.4.0, 7.2.0 through 7.2.6, 7.0.0 through 7.0.12, 2.0.0 through 2.0.13 allows attacker to execute unauthorized code or commands via specially crafted HTTP requests.	2024-03-12	8.1	High
CVE-2024-21407	Microsoft	Windows Hyper-V Remote Code Execution Vulnerability	2024-03-12	8.1	High
CVE-2024-27907	Siemens	A vulnerability has been identified in Simcenter Femap (All versions < V2306.0000). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted Catia MODEL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-22051)	2024-03-12	7.8	High
CVE-2024-21330	Microsoft	Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-21418	Microsoft	Software for Open Networking in the Cloud (SONiC) Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-21426	Microsoft	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-03-12	7.8	High
CVE-2024-21431	Microsoft	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability	2024-03-12	7.8	High
CVE-2024-21434	Microsoft	Microsoft Windows SCSI Class System File Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-21436	Microsoft	Windows Installer Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-21437	Microsoft	Windows Graphics Component Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-21442	Microsoft	Windows USB Print Driver Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-21446	Microsoft	NTFS Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-26169	Microsoft	Windows Error Reporting Service Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-26170	Microsoft	Windows Composite Image File System (CimFS) Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-26173	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-26176	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-26178	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-26182	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-26199	Microsoft	Microsoft Office Elevation of Privilege Vulnerability	2024-03-12	7.8	High
CVE-2024-20320	Cisco	A vulnerability in the SSH client feature of Cisco IOS XR Software for Cisco 8000 Series Routers and Cisco Network Convergence System (NCS) 540 Series and 5700 Series Routers could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient validation of arguments that are included with the SSH client CLI command. An attacker with low-privileged access to an affected device could exploit this vulnerability by issuing a crafted SSH client command to the CLI. A successful exploit could allow the attacker to elevate privileges to root on the affected device.	2024-03-13	7.8	High
CVE-2024-22346	IBM	Db2 for IBM i 7.2, 7.3, 7.4, and 7.5 infrastructure could allow a local user to gain elevated privileges due to an unqualified library call. A malicious actor could cause user-controlled code to run with administrator privilege. IBM X-Force ID: 280203.	2024-03-14	7.8	High
CVE-2024-21419	Microsoft	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	2024-03-12	7.6	High
CVE-2024-22040	Siemens	A vulnerability has been identified in Cerberus PRO EN Engineering Tool (All versions), Cerberus PRO EN Fire Panel FC72x (All versions < IP8 SR4), Cerberus PRO EN X200 Cloud Distribution (All versions < V4.3.5618), Cerberus PRO EN X300 Cloud Distribution (All versions < V4.3.5617), Sinteso FS20 EN Engineering Tool (All versions), Sinteso FS20 EN Fire Panel FC20 (All versions < MP8 SR4), Sinteso FS20 EN X200 Cloud Distribution (All versions < V4.3.5618), Sinteso FS20 EN X300 Cloud Distribution (All versions < V4.3.5617), Sinteso Mobile (All versions). The network communication library in affected systems insufficiently validates HMAC values which might result in a buffer overread. This could allow an unauthenticated remote attacker to crash the network service.	2024-03-12	7.5	High
CVE-2024-22041	Siemens	A vulnerability has been identified in Cerberus PRO EN Engineering Tool (All versions), Cerberus PRO EN Fire Panel FC72x (All versions < IP8 SR4), Cerberus PRO EN X200 Cloud Distribution (All versions < V4.3.5618), Cerberus PRO EN X300 Cloud Distribution (All versions	2024-03-12	7.5	High

		< V4.3.5617), Sinteso FS20 EN Engineering Tool (All versions), Sinteso FS20 EN Fire Panel FC20 (All versions < MP8 SR4), Sinteso FS20 EN X200 Cloud Distribution (All versions < V4.3.5618), Sinteso FS20 EN X300 Cloud Distribution (All versions < V4.3.5617), Sinteso Mobile (All versions). The network communication library in affected systems improperly handles memory buffers when parsing X.509 certificates. This could allow an unauthenticated remote attacker to crash the network service.			
CVE-2024-22044	Siemens	A vulnerability has been identified in SENTRON 3KC ATC6 Expansion Module Ethernet (3KC9000-8TL75) (All versions). Affected devices expose an unused, unstable http service at port 80/tcp on the Modbus-TCP Ethernet. This could allow an attacker on the same Modbus network to create a denial of service condition that forces the device to reboot.	2024-03-12	7.5	High
CVE-2024-21392	Microsoft	.NET and Visual Studio Denial of Service Vulnerability	2024-03-12	7.5	High
CVE-2024-21421	Microsoft	Azure SDK Spoofing Vulnerability	2024-03-12	7.5	High
CVE-2024-21427	Microsoft	Windows Kerberos Security Feature Bypass Vulnerability	2024-03-12	7.5	High
CVE-2024-21438	Microsoft	Microsoft AllJoyn API Denial of Service Vulnerability	2024-03-12	7.5	High
CVE-2024-26190	Microsoft	Microsoft QUIC Denial of Service Vulnerability	2024-03-12	7.5	High
CVE-2024-26204	Microsoft	Outlook for Android Information Disclosure Vulnerability	2024-03-12	7.5	High
CVE-2024-20318	Cisco	A vulnerability in the Layer 2 Ethernet services of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause the line card network processor to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of specific Ethernet frames that are received on line cards that have the Layer 2 services feature enabled. An attacker could exploit this vulnerability by sending specific Ethernet frames through an affected device. A successful exploit could allow the attacker to cause the ingress interface network processor to reset, resulting in a loss of traffic over the interfaces that are supported by the network processor. Multiple resets of the network processor would cause the line card to reset, resulting in a DoS condition.	2024-03-13	7.4	High
CVE-2024-20327	Cisco	A vulnerability in the PPP over Ethernet (PPPoE) termination feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers could allow an unauthenticated, adjacent attacker to crash the ppp_ma process, resulting in a denial of service (DoS) condition. This vulnerability is due to the improper handling of malformed PPPoE packets that are received on a router that is running Broadband Network Gateway (BNG) functionality with PPPoE termination on a Lightspeed-based or Lightspeed-Plus-based line card. An attacker could exploit this vulnerability by sending a crafted PPPoE packet to an affected line card interface that does not terminate PPPoE. A successful exploit could allow the attacker to crash the ppp_ma process, resulting in a DoS condition for PPPoE traffic across the router.	2024-03-13	7.4	High
CVE-2024-21443	Microsoft	Windows Kernel Elevation of Privilege Vulnerability	2024-03-12	7.3	High
CVE-2024-26203	Microsoft	Azure Data Studio Elevation of Privilege Vulnerability	2024-03-12	7.3	High
CVE-2024-0161	Dell	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain an Improper SMM communication buffer verification vulnerability. A local low privileged attacker could potentially exploit this vulnerability leading to arbitrary writes to SMRAM.	2024-03-13	7.2	High
CVE-2024-21390	Microsoft	Microsoft Authenticator Elevation of Privilege Vulnerability	2024-03-12	7.1	High
CVE-2024-21432	Microsoft	Windows Update Stack Elevation of Privilege Vulnerability	2024-03-12	7	High
CVE-2024-21433	Microsoft	Windows Print Spooler Elevation of Privilege Vulnerability	2024-03-12	7	High
CVE-2024-21439	Microsoft	Windows Telephony Server Elevation of Privilege Vulnerability	2024-03-12	7	High
CVE-2024-21445	Microsoft	Windows USB Print Driver Elevation of Privilege Vulnerability	2024-03-12	7	High
CVE-2024-21429	Microsoft	Windows USB Hub Driver Remote Code Execution Vulnerability	2024-03-12	6.8	Medium
CVE-2023-41842	Fortinet	A use of externally-controlled format string vulnerability [CWE-134] in Fortinet FortiManager version 7.4.0 through 7.4.1, version 7.2.0 through 7.2.3 and before 7.0.10, Fortinet FortiAnalyzer version 7.4.0 through 7.4.1, version 7.2.0 through 7.2.3 and before 7.0.10, Fortinet FortiAnalyzer-BigData before 7.2.5 and Fortinet FortiPortal version 6.0 all versions and version 5.3 all versions allows a privileged attacker to execute unauthorized code or commands via specially crafted command arguments.	2024-03-12	6.7	Medium
CVE-2024-26201	Microsoft	Microsoft Intune Linux Agent Elevation of Privilege Vulnerability	2024-03-12	6.6	Medium
CVE-2024-2049	Citrix	Server-Side Request Forgery (SSRF) in Citrix SD-WAN Standard/Premium Editions on or after 11.4.0 and before 11.4.4.46 allows an attacker to disclose limited information from the appliance via Access to management IP.	2024-03-12	6.5	Medium
CVE-2024-26185	Microsoft	Windows Compressed Folder Tampering Vulnerability	2024-03-12	6.5	Medium
CVE-2024-26197	Microsoft	Windows Standards-Based Storage Management Service Denial of Service Vulnerability	2024-03-12	6.5	Medium

CVE-2024-20262	Cisco	A vulnerability in the Secure Copy Protocol (SCP) and SFTP feature of Cisco IOS XR Software could allow an authenticated, local attacker to create or overwrite files in a system directory, which could lead to a denial of service (DoS) condition. The attacker would require valid user credentials to perform this attack. This vulnerability is due to a lack of proper validation of SCP and SFTP CLI input parameters. An attacker could exploit this vulnerability by authenticating to the device and issuing SCP or SFTP CLI commands with specific parameters. A successful exploit could allow the attacker to impact the functionality of the device, which could lead to a DoS condition. The device may need to be manually rebooted to recover. Note: This vulnerability is exploitable only when a local user invokes SCP or SFTP commands at the Cisco IOS XR CLI. A local user with administrative privileges could exploit this vulnerability remotely.	2024-03-13	6.5	Medium
CVE-2024-27265	IBM	IBM Integration Bus for z/OS 10.1 through 10.1.0.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 284564.	2024-03-14	6.5	Medium
CVE-2023-38723	IBM	IBM Maximo Application Suite 7.6.1.3 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: 262192.	2024-03-13	6.4	Medium
CVE-2023-47162	IBM	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 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: 270973.	2024-03-15	6.1	Medium
CVE-2023-47699	IBM	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 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: 270974.	2024-03-15	6.1	Medium
CVE-2024-20315	Cisco	A vulnerability in the access control list (ACL) processing on MPLS interfaces in the ingress direction of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to improper assignment of lookup keys to internal interface contexts. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to access resources behind the affected device that were supposed to be protected by a configured ACL.	2024-03-13	5.8	Medium
CVE-2024-20322	Cisco	A vulnerability in the access control list (ACL) processing on Pseudowire interfaces in the ingress direction of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to improper assignment of lookup keys to internal interface contexts. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to access resources behind the affected device that were supposed to be protected by a configured ACL.	2024-03-13	5.8	Medium
CVE-2024-21430	Microsoft	Windows USB Attached SCSI (UAS) Protocol Remote Code Execution Vulnerability	2024-03-12	5.7	Medium
CVE-2023-45793	Siemens	A vulnerability has been identified in Siveillance Control (All versions >= V2.8 < V3.1.1). The affected product does not properly check the list of access groups that are assigned to an individual user. This could enable a locally logged on user to gain write privileges for objects where they only have read privileges.	2024-03-12	5.5	Medium
CVE-2024-20671	Microsoft	Microsoft Defender Security Feature Bypass Vulnerability	2024-03-12	5.5	Medium
CVE-2024-21408	Microsoft	Windows Hyper-V Denial of Service Vulnerability	2024-03-12	5.5	Medium
CVE-2024-26160	Microsoft	Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability	2024-03-12	5.5	Medium
CVE-2024-26174	Microsoft	Windows Kernel Information Disclosure Vulnerability	2024-03-12	5.5	Medium
CVE-2024-26177	Microsoft	Windows Kernel Information Disclosure Vulnerability	2024-03-12	5.5	Medium
CVE-2024-26181	Microsoft	Windows Kernel Denial of Service Vulnerability	2024-03-12	5.5	Medium
CVE-2021-38938	IBM	IBM Host Access Transformation Services (HATS) 9.6 through 9.6.1.4 and 9.7 through 9.7.0.3 stores user credentials in plain	2024-03-15	5.5	Medium

		clear text which can be read by a local user. IBM X-Force ID: 210989.			
CVE-2024-24693	zoom - rooms	Improper access control in the installer for Zoom Rooms Client for Windows before version 5.17.5 may allow an authenticated user to conduct a denial of service via local access.	2024-03-13	5.5	Medium
CVE-2023-28517	IBM	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 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: 250421.	2024-03-13	5.4	Medium
CVE-2023-46182	IBM	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 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: 269692.	2024-03-15	5.4	Medium
CVE-2024-0162	Dell	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain an Improper SMM communication buffer verification vulnerability. A local low privileged attacker could potentially exploit this vulnerability leading to out-of-bound read/writes to SMRAM.	2024-03-13	5.3	Medium
CVE-2024-0163	Dell	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain a TOCTOU race condition vulnerability. A local low privileged attacker could potentially exploit this vulnerability to gain access to otherwise unauthorized resources.	2024-03-13	5.3	Medium
CVE-2024-20266	Cisco	A vulnerability in the DHCP version 4 (DHCPv4) server feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to trigger a crash of the dhcpd process, resulting in a denial of service (DoS) condition. This vulnerability exists because certain DHCPv4 messages are improperly validated when they are processed by an affected device. An attacker could exploit this vulnerability by sending a malformed DHCPv4 message to an affected device. A successful exploit could allow the attacker to cause a crash of the dhcpd process. While the dhcpd process is restarting, which may take approximately two minutes, DHCPv4 server services are unavailable on the affected device. This could temporarily prevent network access to clients that join the network during that time period and rely on the DHCPv4 server of the affected device. Notes: Only the dhcpd process crashes and eventually restarts automatically. The router does not reload. This vulnerability only applies to DHCPv4. DHCP version 6 (DHCPv6) is not affected.	2024-03-13	5.3	Medium
CVE-2023-47147	IBM	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 could allow an attacker to overwrite a log message under specific conditions. IBM X-Force ID: 270598.	2024-03-15	5.3	Medium
CVE-2023-43043	IBM	IBM Maximo Application Suite - Maximo Mobile for EAM 8.10 and 8.11 could disclose sensitive information to a local user. IBM X-Force ID: 266875.	2024-03-13	5.1	Medium
CVE-2024-21448	Microsoft	Microsoft Teams for Android Information Disclosure Vulnerability	2024-03-12	5	Medium
CVE-2024-26163	Microsoft	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2024-03-14	4.7	Medium
CVE-2024-24692	zoom - rooms	Race condition in the installer for Zoom Rooms Client for Windows before version 5.17.5 may allow an authenticated user to conduct a denial of service via local access.	2024-03-13	4.7	Medium
CVE-2024-21483	Siemens	A vulnerability has been identified in SENTRON 7KM PAC3120 AC/DC (7KM3120-0BA01-1DA0) (All versions >= V3.2.3 < V3.3.0 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...)), SENTRON 7KM PAC3120 DC (7KM3120-1BA01-1EA0) (All versions >= V3.2.3 < V3.3.0 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...)), SENTRON 7KM PAC3220 AC/DC (7KM3220-0BA01-1DA0) (All versions >= V3.2.3 < V3.3.0 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...)), SENTRON 7KM PAC3220 DC (7KM3220-1BA01-1EA0) (All versions >= V3.2.3 < V3.3.0 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...)). The read out protection of the internal flash of affected devices was not properly set at the end of the manufacturing process. An attacker with physical access to the device could read out the data.	2024-03-12	4.6	Medium
CVE-2024-21761	Fortinet	An improper authorization vulnerability [CWE-285] in FortiPortal version 7.2.0, and versions 7.0.6 and below reports may allow a user to download other organizations reports via modification in the request payload.	2024-03-12	4.3	Medium

CVE-2024-23112	Fortinet	An authorization bypass through user-controlled key vulnerability [CWE-639] in FortiOS version 7.4.0 through 7.4.1, 7.2.0 through 7.2.6, 7.0.1 through 7.0.13, 6.4.7 through 6.4.14, and FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14 SSL-VPN may allow an authenticated attacker to gain access to another user's bookmark via URL manipulation.	2024-03-12	4.3	Medium
CVE-2024-20319	Cisco	A vulnerability in the UDP forwarding code of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to bypass configured management plane protection policies and access the Simple Network Management Plane (SNMP) server of an affected device. This vulnerability is due to incorrect UDP forwarding programming when using SNMP with management plane protection. An attacker could exploit this vulnerability by attempting to perform an SNMP operation using broadcast as the destination address that could be processed by an affected device that is configured with an SNMP server. A successful exploit could allow the attacker to communicate to the device on the configured SNMP ports. Although an unauthenticated attacker could send UDP datagrams to the configured SNMP port, only an authenticated user can retrieve or modify data using SNMP requests.	2024-03-13	4.3	Medium
CVE-2023-46179	IBM	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 269683.	2024-03-15	4.3	Medium
CVE-2024-26246	Microsoft	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2024-03-14	3.9	Low
CVE-2024-0154	Dell	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain an improper parameter initialization vulnerability. A local low privileged attacker could potentially exploit this vulnerability to read the contents of non-SMM stack memory.	2024-03-13	3.8	Low
CVE-2024-0173	Dell	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain an improper parameter initialization vulnerability. A local low privileged attacker could potentially exploit this vulnerability to read the contents of non-SMM stack memory.	2024-03-13	3.8	Low
CVE-2023-32335	IBM	IBM Maximo Application Suite 8.10, 8.11 and IBM Maximo Asset Management 7.6.1.3 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 255075.	2024-03-13	3.7	Low
CVE-2023-46181	IBM	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 269686.	2024-03-15	3.3	Low
CVE-2022-32257	siemens - sinema_remote_connect_server	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V3.2). The affected application consists of a web service that lacks proper access control for some of the endpoints. This could lead to unauthorized access to resources and potentially lead to code execution.	2024-03-12	0	Low
CVE-2024-22039	siemens - multiple products	A vulnerability has been identified in Cerberus PRO EN Engineering Tool (All versions < IP8), Cerberus PRO EN Fire Panel FC72x (All versions < IP8), Cerberus PRO EN X200 Cloud Distribution (All versions < V4.0.5016), Cerberus PRO EN X300 Cloud Distribution (All versions < V4.2.5015), Sinteso FS20 EN Engineering Tool (All versions < MP8), Sinteso FS20 EN Fire Panel FC20 (All versions < MP8), Sinteso FS20 EN X200 Cloud Distribution (All versions < V4.0.5016), Sinteso FS20 EN X300 Cloud Distribution (All versions < V4.2.5015), Sinteso Mobile (All versions < V3.0.0). The network communication library in affected systems does not validate the length of certain X.509 certificate attributes which might result in a stack-based buffer overflow. This could allow an unauthenticated remote attacker to execute code on the underlying operating system with root privileges.	2024-03-12	0	Low
CVE-2024-22045	siemens - multiple products	A vulnerability has been identified in SINEMA Remote Connect Client (All versions < V3.1 SP1). The product places sensitive information into files or directories that are accessible to actors who are allowed to have access to the files, but not to the sensitive information. This information is also available via the web interface of the product.	2024-03-12	0	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.**