الهيئة الوطنية للأمن السيبراني
National 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.

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

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 3rd of March to 10th 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**

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 3 مارس إلى 10 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 لCVSS 9.0-10.0**
- **عالي: النتيجة الأساسية لCVSS 7.0-8.9**
- **متوسط: النتيجة الأساسية لCVSS 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-2024-21899	qnap - multiple products	An improper authentication vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to compromise the security of the system via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QTS 4.5.4.2627 build 20231225 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTS hero h4.5.4.2626 build 20231225 and later QuTScloud c5.1.5.2651 and later	2024-03-08	9.8	Critical
CVE-2023-43318	tp-link - tl-sg2210p_firmware	TP-Link JetStream Smart Switch TL-SG2210P 5.0 Build 20211201 allows attackers to escalate privileges via modification of the 'tid' and 'usrlvl' values in GET requests.	2024-03-06	8.8	High
CVE-2024-20337	Cisco	A vulnerability in the SAML authentication process of Cisco Secure Client could allow an unauthenticated, remote attacker to conduct a carriage return line feed (CRLF) injection attack against a user. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link while establishing a VPN session. A successful exploit could allow the attacker to execute arbitrary script code in the browser or access sensitive, browser-based information, including a valid SAML token. The attacker could then use the token to establish a remote access VPN session with the privileges of the affected user. Individual hosts and services behind the VPN headend would still need additional credentials for successful access.	2024-03-06	8.2	High
CVE-2024-25951	Dell	A command injection vulnerability exists in local RACADM. A malicious authenticated user could gain control of the underlying operating system.	2024-03-09	8	High
CVE-2024-23225	Apple	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited.	2024-03-05	7.8	High
CVE-2024-23296	Apple	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 17.4 and iPadOS 17.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited.	2024-03-05	7.8	High
CVE-2024-23268	Apple	An injection issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges.	2024-03-08	7.8	High
CVE-2024-23270	Apple	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.7.4, macOS Ventura 13.6.5,	2024-03-08	7.8	High

		macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4, tvOS 17.4. An app may be able to execute arbitrary code with kernel privileges.			
CVE-2024-23274	Apple	An injection issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges.	2024-03-08	7.8	High
CVE-2024-23276	Apple	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to elevate privileges.	2024-03-08	7.8	High
CVE-2024-25016	IBM	IBM MQ and IBM MQ Appliance 9.0, 9.1, 9.2, 9.3 LTS and 9.3 CD could allow a remote unauthenticated attacker to cause a denial of service due to incorrect buffering logic. IBM X-Force ID: 281279.	2024-03-03	7.5	High
CVE-2023-32331	IBM	IBM Connect:Express for UNIX 1.5.0 is vulnerable to a buffer overflow that could allow a remote attacker to cause a denial of service through its browser UI. IBM X-Force ID: 254979.	2024-03-04	7.5	High
CVE-2024-22463	Dell	Dell PowerScale OneFS 8.2.x through 9.6.0.x contains a use of a broken or risky cryptographic algorithm vulnerability. A remote unprivileged attacker could potentially exploit this vulnerability, leading to compromise of confidentiality and integrity of sensitive information	2024-03-04	7.4	High
CVE-2024-22452	Dell	Dell Display and Peripheral Manager for macOS prior to 1.3 contains an improper access control vulnerability. A low privilege user could potentially exploit this vulnerability by modifying files in the installation folder to execute arbitrary code, leading to privilege escalation.	2024-03-04	7.3	High
CVE-2024-20338	Cisco	A vulnerability in the ISE Posture (System Scan) module of Cisco Secure Client for Linux could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to the use of an uncontrolled search path element. An attacker could exploit this vulnerability by copying a malicious library file to a specific directory in the filesystem and persuading an administrator to restart a specific process. A successful exploit could allow the attacker to execute arbitrary code on an affected device with root privileges.	2024-03-06	7.3	High
CVE-2023-48725	Netgear	A stack-based buffer overflow vulnerability exists in the JSON Parsing getblockschedule() functionality of Netgear RAX30 1.0.11.96 and 1.0.7.78. A specially crafted HTTP request can lead to code execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2024-03-07	7.2	High
CVE-2024-0155	Dell	Dell Digital Delivery, versions prior to 5.0.86.0, contain a Use After Free Vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to an application crash or execution of arbitrary code.	2024-03-04	7	High
CVE-2024-0156	Dell	Dell Digital Delivery, versions prior to 5.0.86.0, contain a Buffer Overflow vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to arbitrary code execution and/or privilege escalation.	2024-03-04	7	High
CVE-2024-21900	qnap - multiple products	An injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.1.3.2578 build 20231110 and later QuTS hero h5.1.3.2578 build 20231110 and later QuTScloud c5.1.5.2651 and later	2024-03-08	6.5	Medium
CVE-2024-20335	Cisco	A vulnerability in the web-based management interface of Cisco Small Business 100, 300, and 500 Series Wireless APs could allow an authenticated, remote attacker to perform command injection attacks against an affected device. In order to exploit this vulnerability, the attacker must have valid administrative credentials for the device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system.	2024-03-06	6.5	Medium
CVE-2024-20336	Cisco	A vulnerability in the web-based user interface of Cisco Small Business 100, 300, and 500 Series Wireless APs could allow an authenticated, remote attacker to perform buffer overflow attacks against an affected device. In order to exploit this vulnerability, the attacker must have valid administrative credentials for the device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to	2024-03-06	6.5	Medium

		execute arbitrary code as the root user on the underlying operating system.			
CVE-2024-20345	Cisco	A vulnerability in the file upload functionality of Cisco AppDynamics Controller could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to an affected device. A successful exploit could allow the attacker to access sensitive data on an affected device.	2024-03-06	6.5	Medium
CVE-2023-46169	IBM	IBM DS8900F HMC 89.21.19.0, 89.21.31.0, 89.30.68.0, 89.32.40.0, and 89.33.48.0 could allow an authenticated user to arbitrarily delete a file. IBM X-Force ID: 269406.	2024-03-07	6.5	Medium
CVE-2023-46170	IBM	IBM DS8900F HMC 89.21.19.0, 89.21.31.0, 89.30.68.0, 89.32.40.0, and 89.33.48.0 could allow an authenticated user to arbitrarily read files after enumerating file names. IBM X-Force ID: 269407.	2024-03-07	6.5	Medium
CVE-2023-43054	IBM	IBM Engineering Test Management 7.0.2 and 7.0.3 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: 267459.	2024-03-03	6.4	Medium
CVE-2023-47745	IBM	IBM MQ Operator 2.0.0 LTS, 2.0.18 LTS, 3.0.0 CD, 3.0.1 CD, 2.4.0 through 2.4.7, 2.3.0 through 2.3.3, 2.2.0 through 2.2.2, and 2.3.0 through 2.3.3 stores or transmits user credentials in plain clear text which can be read by a local user using a trace command. IBM X-Force ID: 272638.	2024-03-03	6.2	Medium
CVE-2024-20301	Cisco	A vulnerability in Cisco Duo Authentication for Windows Logon and RDP could allow an authenticated, physical attacker to bypass secondary authentication and access an affected Windows device. This vulnerability is due to a failure to invalidate locally created trusted sessions after a reboot of the affected device. An attacker with primary user credentials could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the affected device without valid permissions.	2024-03-06	6.2	Medium
CVE-2022-43855	IBM	IBM SPSS Statistics 26.0, 27.0.1, and 28.0 could allow a local user to create multiple files that could exhaust the file handles capacity and cause a denial of service. IBM X-Force ID: 230235.	2024-03-08	6.2	Medium
CVE-2023-38360	IBM	IBM CICS TX Advanced 10.1 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: 260769.	2024-03-04	6.1	Medium
CVE-2024-2188	TP-Link	Cross-Site Scripting (XSS) vulnerability stored in TP-Link Archer AX50 affecting firmware version 1.0.11 build 2022052. This vulnerability could allow an unauthenticated attacker to create a port mapping rule via a SOAP request and store a malicious JavaScript payload within that rule, which could result in an execution of the JavaScript payload when the rule is loaded.	2024-03-05	6.1	Medium
CVE-2024-1442	Grafana	A user with the permissions to create a data source can use Grafana API to create a data source with UID set to *. Doing this will grant the user access to read, query, edit and delete all data sources within the organization.	2024-03-07	6	Medium
CVE-2024-27255	IBM	IBM MQ Operator 2.0.0 LTS, 2.0.18 LTS, 3.0.0 CD, 3.0.1 CD, 2.4.0 through 2.4.7, 2.3.0 through 2.3.3, 2.2.0 through 2.2.2, and 2.3.0 through 2.3.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 283905.	2024-03-03	5.9	Medium
CVE-2023-47742	IBM	IBM QRadar Suite Products 1.10.12.0 through 1.10.18.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 could disclose sensitive information using man in the middle techniques due to not correctly enforcing all aspects of certificate validation in some circumstances. IBM X-Force ID: 272533.	2024-03-03	5.9	Medium
CVE-2024-22355	IBM	IBM QRadar Suite Products 1.10.12.0 through 1.10.18.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 280781.	2024-03-03	5.9	Medium
CVE-2023-28512	IBM	IBM Watson CP4D Data Stores 4.6.0, 4.6.1, and 4.6.2 could allow an attacker with specific knowledge about the system to manipulate data due to improper input validation. IBM X-Force ID: 250396.	2024-03-03	5.9	Medium

CVE-2024-23277	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, iOS 17.4 and iPadOS 17.4. An attacker in a privileged network position may be able to inject keystrokes by spoofing a keyboard.	2024-03-08	5.9	Medium
CVE-2023-46172	IBM	IBM DS8900F HMC 89.21.19.0, 89.21.31.0, 89.30.68.0, 89.32.40.0, and 89.33.48.0 could allow a remote attacker to bypass authentication restrictions for authorized user. IBM X-Force ID: 269409.	2024-03-07	5.6	Medium
CVE-2024-23266	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to modify protected parts of the file system.	2024-03-08	5.5	Medium
CVE-2024-23267	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to bypass certain Privacy preferences.	2024-03-08	5.5	Medium
CVE-2024-23272	Apple	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. A user may gain access to protected parts of the file system.	2024-03-08	5.5	Medium
CVE-2022-22399	IBM	IBM Aspera Faspex 5.0.0 and 5.0.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 222562.	2024-03-05	5.4	Medium
CVE-2024-20346	Cisco	A vulnerability in the web-based management interface of Cisco AppDynamics Controller could allow an authenticated, remote attacker to perform a reflected cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2024-03-06	5.4	Medium
CVE-2022-43890	IBM	IBM Security Verify Privilege On-Premises 11.5 could disclose sensitive information through an HTTP request that could aid an attacker in further attacks against the system. IBM X-Force ID: 240453.	2024-03-04	5.3	Medium
CVE-2023-38362	IBM	IBM CICS TX Advanced 10.1 could disclose sensitive information to a remote attacker due to observable discrepancy in HTTP responses. IBM X-Force ID: 260814.	2024-03-04	5.3	Medium
CVE-2023-25681	IBM	LDAP users on IBM Spectrum Virtualize 8.5 which are configured to require multifactor authentication can still authenticate to the CIM interface using only username and password. This does not affect local users with MFA configured or remote users authenticating via single sign-on. IBM X-Force ID: 247033.	2024-03-05	5.3	Medium
CVE-2024-21901	qnap - multiple products	A SQL injection vulnerability has been reported to affect myQNAPcloud. If exploited, the vulnerability could allow authenticated administrators to inject malicious code via a network. We have already fixed the vulnerability in the following versions: myQNAPcloud 1.0.52 (2023/11/24) and later QTS 4.5.4.2627 build 20231225 and later	2024-03-08	4.7	Medium
CVE-2024-23275	Apple	A race condition was addressed with additional validation. This issue is fixed in macOS Sonoma 14.4, macOS Monterey 12.7.4, macOS Ventura 13.6.5. An app may be able to access protected user data.	2024-03-08	4.7	Medium
CVE-2023-27291	IBM	IBM Watson CP4D Data Stores 4.6.0, 4.6.1, 4.6.2, and 4.6.3 does not encrypt sensitive or critical information before storage or transmission which could allow an attacker to obtain sensitive information. IBM X-Force ID: 248740.	2024-03-03	4.5	Medium
CVE-2022-43880	IBM	IBM QRadar WinCollect Agent 10.0 through 10.1.2 could allow a privileged user to cause a denial of service. IBM X-Force ID: 240151.	2024-03-03	4.4	Medium
CVE-2024-20292	Cisco	A vulnerability in the logging component of Cisco Duo Authentication for Windows Logon and RDP could allow an authenticated, local attacker to view sensitive information in clear text on an affected system. This vulnerability is due to improper storage of an unencrypted registry key in certain logs. An attacker could exploit this vulnerability by accessing the logs on an affected system. A successful exploit could allow the attacker to view sensitive information in clear text.	2024-03-06	4.4	Medium

CVE-2023-46171	IBM	IBM DS8900F HMC 89.21.19.0, 89.21.31.0, 89.30.68.0, 89.32.40.0, and 89.33.48.0 could allow an authenticated user to view sensitive log information after enumerating filenames. IBM X-Force ID: 269408.	2024-03-07	4.3	Medium
CVE-2024-26167	Microsoft	Microsoft Edge for Android Spoofing Vulnerability	2024-03-07	4.3	Medium
CVE-2024-22256	vmware - cloud_director	VMware Cloud Director contains a partial information disclosure vulnerability. A malicious actor can potentially gather information about organization names based on the behavior of the instance.	2024-03-07	4.3	Medium
CVE-2024-23273	Apple	This issue was addressed through improved state management. This issue is fixed in Safari 17.4, iOS 17.4 and iPadOS 17.4, macOS Sonoma 14.4. Private Browsing tabs may be accessed without authentication.	2024-03-08	4.3	Medium
CVE-2023-26282	IBM	IBM Watson CP4D Data Stores 4.6.0 through 4.6.3 could allow a user with physical access and specific knowledge of the system to modify files or data on the system. IBM X-Force ID: 248415.	2024-03-05	4.2	Medium
CVE-2024-24901	Dell	Dell PowerScale OneFS 8.2.x through 9.6.0.x contain an insufficient logging vulnerability. A local malicious user with high privileges could potentially exploit this vulnerability, causing audit messages lost and not recorded for a specific time period.	2024-03-04	3	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.