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 21st of April to 28th of April. 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 ٢١ أبريل إلى ٢٨ أبريل. 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-2023-47731	IBM	IBM QRadar Suite Software 1.10.12.0 through 1.10.19.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 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: 272203.	2024-04-23	5.4	Medium
CVE-2024-28977	Dell	Dell Repository Manager, versions 3.4.2 through 3.4.4,contains a Path Traversal vulnerability in logger module. A local attacker with low privileges could potentially exploit this vulnerability to gain unauthorized read access to the files stored on the server filesystem with the privileges of the running web application.	2024-04-24	3.3	Low
CVE-2023-20249	Cisco	A vulnerability in the web-based management interface of Cisco TelePresence Management Suite (TMS) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data in a specific data field in the interface. 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.	2024-04-24	5.4	Medium
CVE-2024-20359	Cisco	A vulnerability in a legacy capability that allowed for the preloading of VPN clients and plug-ins and that has been available in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a file when it is read from system flash memory. An attacker could exploit this vulnerability by copying a crafted file to the disk0: file system of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.	2024-04-24	6	Medium
CVE-2024-28963	Dell	Telemetry Dashboard v1.0.0.7 for Dell ThinOS 2402 contains a sensitive information disclosure vulnerability. An unauthenticated user with local access to the device could exploit this vulnerability to read sensitive proxy settings information.	2024-04-24	6.2	Medium
CVE-2024-20358	Cisco	A vulnerability in the Cisco Adaptive Security Appliance (ASA) restore functionality that is available in Cisco ASA Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges.	2024-04-24	6.7	Medium

		Administrator-level privileges are required to exploit this vulnerability. This vulnerability exists because the contents of a backup file are improperly sanitized at restore time. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as root.			
CVE-2024-20313	Cisco	A vulnerability in the OSPF version 2 (OSPFv2) feature of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of OSPF updates that are processed by a device. An attacker could exploit this vulnerability by sending a malformed OSPF update to the device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2024-04-24	7.4	High
CVE-2024-20353	Cisco	A vulnerability in the management and VPN web servers for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to incomplete error checking when parsing an HTTP header. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted web server on a device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.	2024-04-24	8.6	High
CVE-2024-20356	Cisco	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker with Administrator-level privileges to perform command injection attacks on an affected system and elevate their privileges to root. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by sending crafted commands to the web-based management interface of the affected software. A successful exploit could allow the attacker to elevate their privileges to root.	2024-04-24	8.7	High
CVE-2024-20295	Cisco	A vulnerability in the CLI of the Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have read-only or higher privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	2024-04-24	8.8	High
CVE-2024-28976	Dell	Dell Repository Manager, versions prior to 3.4.5, contains a Path Traversal vulnerability in API module. A local attacker with low privileges could potentially exploit this vulnerability to gain unauthorized write access to the files stored on the server filesystem with the privileges of the running web application.	2024-04-24	8.8	High
CVE-2024-23527	Ivanti	An out-of-bounds read vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3, in certain conditions can allow an unauthenticated remote attacker to read sensitive information in memory.	2024-04-25	5.3	Medium
CVE-2024-25026	IBM	IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.4 are vulnerable to a denial of service, caused by sending a specially crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. IBM X-Force ID: 281516.	2024-04-25	5.9	Medium
CVE-2024-29205	Ivanti	An Improper Check for Unusual or Exceptional Conditions vulnerability in the web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a remote unauthenticated attacker to send specially crafted requests in-order-to cause service disruptions.	2024-04-25	7.5	High
CVE-2024-4235	Netgear	A vulnerability classified as problematic was found in Netgear DG834Gv5 1.6.01.34. This vulnerability affects unknown code of the component Web Management Interface. The manipulation leads to cleartext storage of sensitive information. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-262126 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-04-26	2.7	Low

CVE-2024-25048	IBM	IBM MQ Appliance 9.3 CD and LTS are vulnerable to a heap-based buffer overflow, caused by improper bounds checking. A remote authenticated attacker could overflow a buffer and execute arbitrary code on the system or cause the server to crash. IBM X-Force ID: 283137.	2024-04-27	7.5	High

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.