
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 25 فبراير إلى 2 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 لـ CVSS 9.0-10.0
- عالي: النتيجة الأساسية لـ CVSS 7.0-8.9
- متوسط: النتيجة الأساسية لـ CVSS 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 25th of February to 2nd 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-2024-20267 | Cisco | A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload.<br><br>This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS-enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.<br><br>Note: The IPv6 packet can be generated multiple hops away from the targeted device and then encapsulated within MPLS. The DoS condition may occur when the NX-OS device processes the packet. | 2024-02-29 | 8.6 | High |
| CVE-2024-20321 | Cisco | A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.<br><br>This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network. | 2024-02-29 | 8.6 | High |
| CVE-2023-25925 | IBM | IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 247632. | 2024-02-28 | 8.5 | High |
| CVE-2023-25921 | IBM | IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. IBM X-Force ID: 247620. | 2024-02-29 | 8.5 | High |
| CVE-2024-24903 | Dell | Dell Secure Connect Gateway (SCG) Policy Manager, version 5.10+, contain a weak password recovery mechanism for forgotten passwords. An adjacent network low privileged attacker could potentially exploit this vulnerability, leading to unauthorized access to the application with privileges of the compromised account. The attacker could retrieve the reset password token without authorization and then perform the password change. | 2024-03-01 | 8 | High |
| CVE-2024-20765 | Adobe | Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. | 2024-02-29 | 7.8 | High |

| | | | | | |
|---|---|---|---|---|---|
| | | Exploitation of this issue requires user interaction in that a victim must open a malicious file. | | | |
| CVE-2024-24906 | Dell | Dell Secure Connect Gateway (SCG) Policy Manager, all versions, contain(s) a Stored Cross-Site Scripting Vulnerability in Policy page. An adjacent network high privileged attacker could potentially exploit this vulnerability, leading to the storage of malicious HTML or JavaScript codes in a trusted application data store. When a victim user accesses the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery. | 2024-03-01 | 7.6 | High |
| CVE-2024-24904 | Dell | Dell Secure Connect Gateway (SCG) Policy Manager, all versions, contain(s) a Stored Cross-Site Scripting Vulnerability. An adjacent network high privileged attacker could potentially exploit this vulnerability, leading to the storage of malicious HTML or JavaScript codes in a trusted application data store. When a victim user accesses the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery. | 2024-03-01 | 7.6 | High |
| CVE-2024-24905 | Dell | Dell Secure Connect Gateway (SCG) Policy Manager, all versions, contain(s) a Stored Cross-Site Scripting Vulnerability. An adjacent network high privileged attacker could potentially exploit this vulnerability, leading to the storage of malicious HTML or JavaScript codes in a trusted application data store. When a victim user accesses the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery. | 2024-03-01 | 7.6 | High |
| CVE-2024-24907 | Dell | Dell Secure Connect Gateway (SCG) Policy Manager, all versions, contain(s) a Stored Cross-Site Scripting Vulnerability in the Filters page. An adjacent network high privileged attacker could potentially exploit this vulnerability, leading to the storage of malicious HTML or JavaScript codes in a trusted application data store. When a victim user accesses the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery. | 2024-03-01 | 7.6 | High |
| CVE-2024-25063 | Hikvision | Due to insufficient server-side validation, a successful exploit of this vulnerability could allow an attacker to gain access to certain URLs that the attacker should not have access to. | 2024-03-02 | 7.5 | High |
| CVE-2024-0819 | TeamViewer | Improper initialization of default settings in TeamViewer Remote Client prior version 15.51.5 for Windows, Linux and macOS, allow a low privileged user to elevate privileges by changing the personal password setting and establishing a remote connection to a logged-in admin account. | 2024-02-27 | 7.3 | High |
| CVE-2024-22457 | Dell | Dell Secure Connect Gateway 5.20 contains an improper authentication vulnerability during the SRS to SCG update path. A remote low privileged attacker could potentially exploit this vulnerability, leading to impersonation of the server through presenting a fake self-signed certificate and communicating with the remote server. | 2024-03-01 | 7.1 | High |
| CVE-2024-22459 | Dell | Dell ECS, versions 3.6 through 3.6.2.5, and 3.7 through 3.7.0.6, and 3.8 through 3.8.0.4 versions, contain an improper access control vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to unauthorized access to all buckets and their data within a namespace | 2024-02-28 | 6.8 | Medium |
| CVE-2023-48674 | Dell | Dell Platform BIOS contains an Improper Null Termination vulnerability. A high privilege user with network access to the system could potentially send malicious data to the device in order to cause some services to cease to function. | 2024-03-01 | 6.8 | Medium |
| CVE-2023-39254 | Dell | Dell Update Package (DUP), Versions prior to 4.9.10 contain an Uncontrolled Search Path vulnerability. A malicious user with local access to the system could potentially exploit this vulnerability to run arbitrary code as admin. | 2024-03-01 | 6.7 | Medium |
| CVE-2024-20294 | Cisco | A vulnerability in the Link Layer Discovery Protocol (LLDP) feature of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device.<br><br>This vulnerability is due to improper handling of specific fields in an LLDP frame. An attacker could exploit this vulnerability by sending a crafted LLDP packet to an interface of an affected device and having an authenticated user retrieve LLDP statistics from the affected device through CLI show commands or Simple Network | 2024-02-29 | 6.6 | Medium |

| | | | | | |
|---|---|---|---|---|---|
| | | Management Protocol (SNMP) requests. A successful exploit could allow the attacker to cause the LLDP service to crash and stop running on the affected device. In certain situations, the LLDP crash may result in a reload of the affected device.<br><br>Note: LLDP is a Layer 2 link protocol. To exploit this vulnerability, an attacker would need to be directly connected to an interface of an affected device, either physically or logically (for example, through a Layer 2 Tunnel configured to transport the LLDP protocol). | | | |
| CVE-2022-34357 | IBM | IBM Cognos Analytics Mobile Server 11.1.7, 11.2.4, and 12.0.0 is vulnerable to Denial of Service due to due to weak or absence of rate limiting. By making unlimited http requests, it is possible for a single user to exhaust server resources over a period of time making service unavailable for other legitimate users. IBM X-Force ID: 230510. | 2024-02-26 | 6.5 | Medium |
| CVE-2023-38367 | IBM | IBM Cloud Pak Foundational Services Identity Provider (idP) API (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) allows CRUD Operations with an invalid token. This could allow an unauthenticated attacker to view, update, delete or create an IdP configuration. IBM X-Force ID: 261130. | 2024-02-29 | 6.5 | Medium |
| CVE-2023-28949 | IBM | IBM Engineering Requirements Management DOORS 9.7.2.7 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: 251216. | 2024-03-01 | 6.5 | Medium |
| CVE-2023-47716 | IBM | IBM CP4BA - Filenet Content Manager Component 5.5.8.0, 5.5.10.0, and 5.5.11.0 could allow a user to gain the privileges of another user under unusual circumstances. IBM X-Force ID: 271656. | 2024-03-01 | 6.3 | Medium |
| CVE-2023-38359 | IBM | IBM Cognos Analytics 11.1.7, 11.2.4, and 12.0.0 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: 260744. | 2024-02-26 | 6.1 | Medium |
| CVE-2023-50303 | IBM | IBM InfoSphere Information Server 11.7 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: 273333. | 2024-02-28 | 6.1 | Medium |
| CVE-2023-38372 | IBM | An unauthorized attacker who has obtained an IBM Watson IoT Platform 1.0 security authentication token can use it to impersonate an authorized platform user. IBM X-Force ID: 261201. | 2024-02-29 | 5.9 | Medium |
| CVE-2021-39090 | IBM | IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.6.0 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: 216388. | 2024-02-29 | 5.9 | Medium |
| CVE-2024-20291 | Cisco | A vulnerability in the access control list (ACL) programming for port channel subinterfaces of Cisco Nexus 3000 and 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, remote attacker to send traffic that should be blocked through an affected device.<br><br>This vulnerability is due to incorrect hardware programming that occurs when configuration changes are made to port channel member ports. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to access network resources that should be protected by an ACL that was applied on port channel subinterfaces. | 2024-02-29 | 5.8 | Medium |
| CVE-2024-24900 | Dell | Dell Secure Connect Gateway (SCG) Policy Manager, all versions, contain an improper authorization vulnerability. An adjacent network low privileged attacker could potentially exploit this vulnerability, leading to unauthorized devices added to policies. Exploitation may lead to information disclosure and unauthorized access to the system. | 2024-03-01 | 5.8 | Medium |
| CVE-2023-25926 | IBM | IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 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: 247599. | 2024-02-29 | 5.5 | Medium |
| CVE-2023-44341 | Adobe | Adobe InDesign versions ID18.5 (and earlier) and ID17.4.2 (and earlier) are affected by a NULL Pointer Dereference vulnerability. | 2024-02-29 | 5.5 | Medium |

| | | | | | |
|---|---|---|---|---|---|
| | | An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | | | |
| CVE-2023-44342 | Adobe | Adobe InDesign versions ID18.5 (and earlier) and ID17.4.2 (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. | 2024-02-29 | 5.5 | Medium |
| CVE-2023-44343 | Adobe | Adobe InDesign versions ID18.5 (and earlier) and ID17.4.2 (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. | 2024-02-29 | 5.5 | Medium |
| CVE-2023-44344 | Adobe | Adobe InDesign versions ID18.5 (and earlier) and ID17.4.2 (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. | 2024-02-29 | 5.5 | Medium |
| CVE-2023-44345 | Adobe | Adobe InDesign versions ID18.5 (and earlier) and ID17.4.2 (and earlier) are affected by a Improper Input Validation vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 2024-02-29 | 5.5 | Medium |
| CVE-2023-44346 | Adobe | Adobe InDesign versions ID18.5 (and earlier) and ID17.4.2 (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. | 2024-02-29 | 5.5 | Medium |
| CVE-2023-44347 | Adobe | Adobe InDesign versions ID18.5 (and earlier) and ID17.4.2 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 2024-02-29 | 5.5 | Medium |
| CVE-2023-43051 | IBM | IBM Cognos Analytics 11.1.7, 11.2.4, and 12.0.0 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: 267451. | 2024-02-26 | 5.4 | Medium |
| CVE-2023-30996 | IBM | IBM Cognos Analytics 11.1.7, 11.2.4, and 12.0.0 could be vulnerable to information leakage due to unverified sources in messages sent between Windows objects of different origins. IBM X-Force ID: 254290. | 2024-02-26 | 5.3 | Medium |
| CVE-2024-20344 | Cisco | A vulnerability in system resource management in Cisco UCS 6400 and 6500 Series Fabric Interconnects that are in Intersight Managed Mode (IMM) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the Device Console UI of an affected device.<br><br>This vulnerability is due to insufficient rate-limiting of TCP connections to an affected device. An attacker could exploit this vulnerability by sending a high number of TCP packets to the Device Console UI. A successful exploit could allow an attacker to cause the Device Console UI process to crash, resulting in a DoS condition. A manual reload of the fabric interconnect is needed to restore complete functionality. | 2024-02-29 | 5.3 | Medium |
| CVE-2023-50324 | IBM | IBM Cognos Command Center 10.2.4.1 and 10.2.5 exposes details the X-AspNet-Version Response Header that could allow an attacker to obtain information of the application environment to conduct further attacks. IBM X-Force ID: 275038. | 2024-03-01 | 5.3 | Medium |
| CVE-2023-38366 | IBM | IBM Filenet Content Manager Component 5.5.8.0, 5.5.10.0, and 5.5.11.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 261115. | 2024-03-01 | 5.3 | Medium |
| CVE-2023-50312 | IBM | IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.2 could provide weaker than expected security for outbound TLS connections caused by a failure to honor user configuration. IBM X-Force ID: 274711. | 2024-03-01 | 5.3 | Medium |
| CVE-2024-20328 | Cisco | A vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of the application service account.The vulnerability is due to unsafe | 2024-03-01 | 5.3 | Medium |

| | | | | | |
|---|---|---|---|---|---|
| | | handling of file names. A local attacker could exploit this vulnerability by supplying a file name containing command-line sequences. When processed on a system using configuration options for the VirusEvent feature, the attacker could cause the application to execute arbitrary commands.<br>ClamAV has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. | | | |
| CVE-2023-50305 | IBM | IBM Engineering Requirements Management DOORS 9.7.2.7 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: 273336. | 2024-03-01 | 5.1 | Medium |
| CVE-2023-7207 | Debian | Debian's cpio contains a path traversal vulnerability. This issue was introduced by reverting CVE-2015-1197 patches which had caused a regression in --no-absolute-filenames. Upstream has since provided a proper fix to --no-absolute-filenames. | 2024-02-29 | 4.9 | Medium |
| CVE-2023-28525 | IBM | IBM Engineering Requirements Management 9.7.2.7 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: 251052. | 2024-03-01 | 4.8 | Medium |
| CVE-2023-32344 | IBM | IBM Cognos Analytics 11.1.7, 11.2.4, and 12.0.0 is vulnerable to form action hijacking where it is possible to modify the form action to reference an arbitrary path. IBM X-Force ID: 255898. | 2024-02-26 | 4.3 | Medium |
| CVE-2023-25922 | IBM | IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. IBM X-Force ID: 247621. | 2024-02-28 | 4.3 | Medium |
| CVE-2024-25064 | Hikvision | Due to insufficient server-side validation, an attacker with login privileges could access certain resources that the attacker should not have access to by changing parameter values. | 2024-03-02 | 4.3 | Medium |
| CVE-2023-27545 | IBM | IBM Watson CloudPak for Data Data Stores information disclosure 4.6.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 248947. | 2024-02-29 | 4 | Medium |
| CVE-2024-22458 | Dell | Dell Secure Connect Gateway, 5.18, contains an Inadequate Encryption Strength Vulnerability. An unauthenticated network attacker could potentially exploit this vulnerability, allowing an attacker to recover plaintext from a block of ciphertext. | 2024-03-01 | 3.7 | 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.