

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة vulnerabilities by the National Institute of Standards and Technology the National Institute of Standards and Technology (NIST) من قبل (NIST) (NIST) National Vulnerability Database (NVD) for the week from 25th 2 للأسبوع من 25 فبراير إلى National Vulnerability Database (NVD) of February to 2nd of March. Vulnerabilities are scored using the Common مارس. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Vulnerability Scoring System (CVSS) standard as per the حيث يتم تصنيف الثغرات بناء على Vulnerability Scoring System (CVSS) 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

التالى:

- عالى جدًا: النتيجة الأساسية لـCVSS 9.0-10.0
 - عالى: النتيجة الأساسية لـCVSS 7.0-8.9
 - متوسط: النتيجة الأساسية LVSS 4.0-6.9
 - منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

| CVE ID & Source | Vendor - Product | Description | Publish Date | CVSS Score | Severity |
|-----------------------|------------------|---|--------------|---------------|----------|
| | | 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. | | | |
| | | 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. | | | |
| <u>CVE-2024-20267</u> | Cisco | 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. A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an | 2024-02-29 | 8.6 | High |
| | | unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a | | | |
| <u>CVE-2024-20321</u> | Cisco | 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 |
| <u>CVE-2023-25925</u> | 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 |
| <u>CVE-2023-25921</u> | 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 |
| | | 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 | | | |
| <u>CVE-2024-24903</u> | Dell | account. The attacker could retrieve the reset password token without authorization and then perform the password change. Acrobat Reader versions 20.005.30539, 23.008.20470 and earlier | 2024-03-01 | 8 | High |
| <u>CVE-2024-20765</u> | Adobe | 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 |

| | | | | [| 1 |
|-----------------------|------------|---|------------|-----|---------|
| | | Exploitation of this issue requires user interaction in that a victim must open a malicious file. | | | |
| | | 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 | | | |
| CVE-2024-24906 | Dell | information disclosure, session theft, or client-side request forgery. | 2024-03-01 | 7.6 | High |
| <u>CVL-2024-24500</u> | Dell | Dell Secure Connect Gateway (SCG) Policy Manager, all versions, | 2024-03-01 | 7.0 | Tingin |
| | | 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 | | | |
| | D | vulnerable web application. Exploitation may lead to information | 2024 02 04 | 7.6 | |
| CVE-2024-24904 | Dell | disclosure, session theft, or client-side request forgery. | 2024-03-01 | 7.6 | High |
| | | 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 | | | |
| CVE-2024-24905 | Dell | disclosure, session theft, or client-side request forgery. | 2024-03-01 | 7.6 | High |
| | | 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 | | | |
| CVE-2024-24907 | Dell | forgery. | 2024-03-01 | 7.6 | High |
| | | Due to insufficient server-side validation, a successful exploit of | | | |
| | | this vulnerability could allow an attacker to gain access to certain | | | |
| CVE-2024-25063 | Hikvision | URLs that the attacker should not have access to. | 2024-03-02 | 7.5 | High |
| | | | | | |
| | | 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 | | | |
| CVE-2024-0819 | TeamViewer | logged-in admin account. | 2024-02-27 | 7.3 | High |
| <u> </u> | | Dell Secure Connect Gateway 5.20 contains an improper | / | /.5 | |
| | | 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 | | | |
| CVE-2024-22457 | Dell | the remote server. | 2024-03-01 | 7.1 | High |
| | | 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 | | | |
| CVE-2024-22459 | Dell | exploit this vulnerability, leading to unauthorized access to all buckets and their data within a namespace | 2024-02-28 | 6.8 | Medium |
| <u>UVL'ZUZH-ZZHJJ</u> | שכוו | Dell Platform BIOS contains an Improper Null Termination | 2024-02-20 | 0.0 | wiedium |
| | | vulnerability. A high privilege user with network access to the | | | |
| | | system could potentially send malicious data to the device in order | | | |
| CVE-2023-48674 | Dell | to cause some services to cease to function. | 2024-03-01 | 6.8 | Medium |
| | | 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 | | | |
| CVE-2023-39254 | Dell | run arbitrary code as admin. | 2024-03-01 | 6.7 | Medium |
| | | 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. | | | |
| | | | | | 1 |
| | | | | | |
| | | | | | |
| | | This vulnerability is due to improper handling of specific fields in | | | |
| | | This vulnerability is due to improper handling of specific fields in an LLDP frame. An attacker could exploit this vulnerability by | | | |
| | | This vulnerability is due to improper handling of specific fields in | | | |

| T | | | [| | 1 |
|-----------------------|-------|--|------------|-----|--------|
| | | 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. | | | |
| | | | | | |
| | | 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). | | | |
| | | 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 | | | |
| <u>CVE-2022-34357</u> | IBM | ID: 230510. | 2024-02-26 | 6.5 | Medium |
| | | 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 | | | |
| CVE-2023-38367 | IBM | create an IdP configuration. IBM X-Force ID: 261130. | 2024-02-29 | 6.5 | Medium |
| | | 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: | | - | |
| <u>CVE-2023-28949</u> | IBM | 251216. IBM CP4BA - Filenet Content Manager Component 5.5.8.0, | 2024-03-01 | 6.5 | Medium |
| | | 5.5.10.0, and 5.5.11.0 could allow a user to gain the privileges of | | | |
| CVF 2022 4771C | | another user under unusual circumstances. IBM X-Force ID: | 2024 02 01 | 6.2 | Madium |
| <u>CVE-2023-47716</u> | IBM | 271656. IBM Cognos Analytics 11.1.7, 11.2.4, and 12.0.0 is vulnerable to | 2024-03-01 | 6.3 | Medium |
| | | 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 | | | |
| <u>CVE-2023-38359</u> | IBM | trusted session. IBM X-Force ID: 260744. | 2024-02-26 | 6.1 | Medium |
| | | 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 | 2024 02 20 | 6.4 | |
| <u>CVE-2023-50303</u> | IBM | trusted session. IBM X-Force ID: 273333. An unauthorized attacker who has obtained an IBM Watson IoT | 2024-02-28 | 6.1 | Medium |
| | | Platform 1.0 security authentication token can use it to | | | |
| CVE-2023-38372 | IBM | impersonate an authorized platform user. IBM X-Force ID: 261201. | 2024-02-29 | 5.9 | Medium |
| | | IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.6.0 could | 20210225 | 5.5 | |
| | | 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 | | | |
| 01/5 2024 20000 | | information using man in the middle techniques. IBM X-Force ID: | 2024 02 20 | F 0 | |
| <u>CVE-2021-39090</u> | IBM | 216388.A vulnerability in the access control list (ACL) programming for | 2024-02-29 | 5.9 | Medium |
| | | 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. | | | |
| | | | | | |
| | | 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 | | | |
| CVE-2024-20291 | Cisco | should be protected by an ACL that was applied on port channel subinterfaces. | 2024-02-29 | 5.8 | Medium |
| | | 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. | | | |
| | D-11 | Exploitation may lead to information disclosure and unauthorized | 2024 02 01 | F 0 | Madia |
| <u>CVE-2024-24900</u> | Dell | access to the system. IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, | 2024-03-01 | 5.8 | Medium |
| | | 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 | | | |
| <u>CVE-2023-25926</u> | IBM | memory resources. IBM X-Force ID: 247599. | 2024-02-29 | 5.5 | Medium |
| CVE_2022 44241 | 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 | 55 | Medium |
| <u>CVE-2023-44341</u> | AUDDE | earner are anected by a NOLL Pointer Dereierence vulnerability. | 2024-02-29 | 5.5 | weulum |

| a delice an application desirie/service in the context of the content user. Splicitation of this issue requires user interaction in that a victim must open a mailous file. Image: Content of the context of the content of the content of the context of the context of the content of the content of the context of the context of the content of the content of the context of the context of the content of the content of the context of the context of the content of the context of the context of the context of the content of the context of the context of the context of the content of the context of the context of the context of the content of the context of the context of the context of the content of the context of the context of the context of the context of the context of the context of the context of the context of the context of the context of the context of the context of t | | | | | | I |
|--|-----------------------|--------|---|------------|------------|----------|
| current user. Exploitation of this loss requires user interaction in value | | | An unauthenticated attacker could leverage this vulnerability to | | | |
| Out Part a decim must open a mailous file. | | | | | | |
| cvit 2023-46342 Adobe Adobe 224-02-20 5.5 Medium cvit 2023-46342 Adobe 2024-02-20 5.5 Medium cvit 2023-46343 Adobe Statistics and stati | | | | | | |
| CVE 2023-4032 Adobe Adobe infocience of services user interaction in that a victim interaction with the super regimes user interaction in that a victim interaction and the super regimes user interaction in that a victim interaction and the super regimes user interaction in that a victim interaction and interaction and observations and interaction in that a victim interaction and interaction and observations and interaction in that a victim interaction and interaction and observation and interaction in that a victim interaction and interaction and observations and interaction in that a victim interaction and interaction and observation and interaction in that a victim interaction and interaction in the interaction in that a victim interaction and interaction in the interaction in that a victim interaction and interaction in the interaction in that a victim interaction and interaction in the interaction in the interaction in the interaction in the interaction interaction and interaction interaction in the i | | | Adobe InDesign versions ID18.5 (and earlier) and ID17.4.2 (and | | | |
| UP: 2023-4432 Adobe Everage this vulnerability to bypass mitigations such as ASU. Exploitation of this scale requires user interaction in that a victim must open a milicions file. 2024-02-28 5.5 Medium CVE 2023-4432 Adobe Medium Scale (Scale and Scale and Sc | | | | | | |
| CVT-2023-4642 Explosition of this issue requires user interaction in that a victim must open an anilocos file. 2024-02-29 5.5 Medium CVT-2023-4642 Adobe Mode integraps versions 1D38.3 (ind earlier) and 1D27.4 2 (and caule) lead to indicious file. 2024-02-29 5.5 Medium CVT-2023-46431 Adobe Mode integraps versions 1D38.3 (ind earlier) and 1D27.4 2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to factors or to smith emmory. An attacker could leverage this vulnerability to bypass mitigations such as X4R. 2024-02-29 5.5 Medium CVT-2023-46434 Adobe must open anilocos file. 2024-02-29 5.5 Medium CVT-2023-46444 Adobe must open anilocos file. 2024-02-29 5.5 Medium CVT-2023-46444 Adobe must open anilocos file. 2024-02-29 5.5 Medium CVT-2023-46444 Adobe must open anilocos file. 2024-02-29 5.5 Medium CVT-2023-46444 Adobe must open anilocos file. 2024-02-29 5.5 Medium CVT-2023-46444 Adobe must open anilocos file. 2024-02-29 5.5 Medium | | | | | | |
| CVI-2023-4842 Adobe must open a malicious file. 2024-02-29 5.5 Medium CVI-2023-4843 Adobe Medium resins 103.5 (and earlier) and 107.4.2 (and earlier) and 107.4.2 (and earlier) are affected by an out-of-bounds read vulnerability to the could lead to inclosure of earlier and mean runeraction in this value. 2024-02.29 5.5 Medium CVI-2023-4843 Adobe Earlier are affected by an out-of-bounds read vulnerability to the could lead to inclosure of earlier are affected by an out-of-bounds read vulnerability to the could lead to inclosure of earlier are affected by an out-of-bounds read vulnerability to the could lead to inclosure of earlier are affected by an out-of-bounds read vulnerability to the could lead to inclosure of earlier and 1027.4.2 (and earlier) | | | | | | |
| CVE 2023-44345 Adobe Description of sinking energy in the set within memory. An attacker could lever age this vulnerability to bypass mitigations such as ASIR. 2024-02.29 5.5 Medium CVE 2023-44345 Adobe Mode in Desgription such as ASIR. 2024-02.29 5.5 Medium CVE 2023-44345 Adobe Mode in Desgription such as ASIR. 2024-02.29 5.5 Medium CVE 2023-44345 Adobe Mode in Desgription such as a fifted by an out-of-bounds read vulnerability that and the advectore of the instruction in that a victim memory. An attacker could be advectore of the instruction in that a victim velocity of a set of the instruction in that a victim velocity of a set of the instruction in that a victim velocity of a set of the instruction in that a victim velocity of the instruction in that a victim velocity of a set of the instruction in that a victim velocity of a set of the instruction in that a victim velocity of a set of the instruction in that a victim velocity of a set of the instruction in that a victim velocity of a set of the instruction in that a victim velocity of a set of the instruction in that a victim velocity of a set of the instruction in that a victim velocity of a set of the instruction in the instructin instruction in the i | CVE-2023-44342 | Adobe | | 2024-02-29 | 5.5 | Medium |
| CVE-2023-44342 Adobe Medium CVE-2023-44342 Adobe Paiploitation of this (Ssue requires user interaction in that a victim earlier) are affected by an out-obcounds real dynamethity that could lead to disclosure of sensitive memory. An attacker could learning in a material para material that a victim mort open a material para material that a victim earlier) are affected by an out-obcound real dynamethity that could learning this material that a victim mort open amaterial structure (uncertain that a victim earlier) are affected by an out-obcound real dynamethity that could learning this material structure (uncertain that a victim earlier) are affected by a mort-open input Violation unlear ability. 2024-02-29 5.5 Medium CVF-2023-44345 Adobe material attacker could learning that material distacker could learning that wick open analicious file. 2024-02-29 5.5 Medium CVF-2023-44345 Adobe Hot a victim must open analicious file. 2024-02-29 5.5 Medium earlier (an affected by a nut-of-bounds real vinteraction in a dhieve end application devices results with and that a victim must open a malicious file. 2024-02-29 5.5 Medium CVF-2023-44345 Adobe must open a malicious file. 2024-02-29 5.5 Medium CVF-2023-44345 Adobe must open a malicious file. 2024-02-29 5.5 Medium CVF-2023-44345 | | | | | | |
| Electropic this submeridative to bypass mitigations such as ASIR. Vision | | | | | | |
| CVF-2023-4343 Papel notations of this issue requires user interaction in that a victim must open a mail circuit file. 2024-02-29 5.5 Medium CVF-2023-4343 Adobe InDesign versions D18.5 (and earlier) and ID17.4.2 (and earlier) are affected by an out-of-booms free dumenshifty that could lead to disclosure of sensitive memory, an attacker could leverage this vulnerability to thypess mitigations such as ASLR. 2024-02-29 5.5 Medium CVF-2023-44344 Adobe InDesign versions D18.5 (and earlier) and ID17.4.2 (and earlier) are affected by a improver input Validation veloces of this corrent user. Publishing the correct of this corrent user. Publishing the correct of this earlier) are affected by a mouter-thoous of this earlier) are affected by an out-of-boomds read vulnerability. An three on application densities of services in the correct of the could lead to disclosure of annitive the memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. 2024-02-29 5.5 Medium CVF-2023-44346 Adobe that a victim must open a mailcous file. 2024-02-29 5.5 Medium leverage this vulnerability to bypass mitigations such as ASLR. CVF-2023-44346 Adobe this as require user requires user interaction in the as ASLR. 2024-02-29 5.5 Medium CVF-2023-44346 Adobe this as requires user requires user interaction in the as ASLR. 2024-02-29 5.5 Medium | | | | | | |
| CVE 2023-44343 Adobe must open a malicious file. 2024-02-29 5.5 Medium Adobe Indegrave previous D123 S (and earlier) and D127.4.2 (and carlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of ansitive memory. An attacker could leaverage this vulnerability to bypass mitigations such as ASR. 2024-02-29 5.5 Medium CVE 2023-44344 Adobe Made Indegrave resins D125 (and earlier) and D127.4.2 (and earlier) are affected by a lumpoper input Vuldation vulnerability. An unsufficient da tacket could leaverage this vulnerability. An unsufficient da tacket could leaverage this vulnerability. An unsufficient and tacket attacket could leaverage this vulnerability to achieve an application deniel-of-service in the context of the correct user. Exploitation of this sour requires user interaction in that a victim must open amalicious file. 2024-02-29 5.5 Medium CVE 2023-44345 Adobe Made Indegravery on 20.3-context of the correct user. Exploitation of this sour requires user interaction in that a victim must open amalicious file. 2024-02-29 5.5 Medium CVE 2023-44347 Adobe Adobe Indegraverison 103.5 (and earlier) and 1077.4.2 (and earlier) are affected by a VULE Protein the context of the correct user. Exploitation of this issue requires user interaction in that a victim must open amalicous file. 2024-02-26 5.5 Medium CVE 2023-44347 Adobe indegraverisons 103.5 (and earlier) and 102.1 (and indegravi | | | | | | |
| cvif 2023-4434 Adobe Cvif 2023-44344 Adobe Cvif 2023-44345 Adobe Cvif 2023-44347 Cvif 2023-44347 Adobe Cvif 2023-44347 Cvif 2023-44347 Adobe Cvif 2023-44347 Adobe Cvif 2023-4347 Adobe Cvif | CVE-2023-44343 | Adobe | | 2024-02-29 | 5.5 | Medium |
| CVE-2023-44344 Adobe exploration of this issue requires user interaction in that avictim must open analicous file. 2024-02-29 5.5 Medium CVE-2023-44344 Adobe Adobe inDesign versions ID18.5 (and sarling) and ID17.4.2 (and carlied) are affected by a improve input Validation vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an aplication denial-orservice in the councer ator the Current user. Explosition of this issue requires user interaction in that a victim must open analicous file. 2024-02-29 5.5 Medium CVE-2023-44345 Adobe Adobe inDesign versions ID18.5 (and earlier) and ID17.4.2 (and carlier) are affected by an out-of-bounds red vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to those to be freence vulnerability. A dobe inDesign versions ID18.5 (and earlier) and ID17.4.2 (and carlier) are afficted by a number to be freence vulnerability. A dobe inDesign versions ID18.5 (and earlier) and ID17.4.2 (and carlier) are afficted by a number to be freence vulnerability. A dobe inDesign versions ID18.5 (and earlier) and ID17.4.2 (and carlier) are afficted by a number to be forease vulnerability. A dobe inDesign versions ID18.5 (and earlier) and ID17.4.2 (and carlier) are afficted by a number to be forease vulnerability and arbitrary avical and basis requires user interaction in the version and the interaction in the avictim must open analyticas II.1.2, 1.2.4, and I2.0.0 is vulnerability and arbitrary avical and basis requires and the interaction in the version. INTEX version in the interaction in the version. INTEX version | | | | | | |
| UVE-2023-44344 Adobe Exploitation of this issue equires user interaction in that a victim must open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44344 Adobe Adobe interaction in that a victim must open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44345 Adobe Exploitation of this issue requires universability. An unauthenticate attacker could leverget this vulnerability that could lead to disclasure of sname interaction in that a victim round lead to disclasure of sname interaction in that a victim could lead to disclasure of sname issue requires user interaction in that a victim must open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44345 Adobe Adobe interactive subs requires user interaction in that a victim must open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44345 Adobe Adobe interactive subs requires user interaction in must open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44347 Adobe Interactive subs reputation wulnerability at the subscription of this issue requires using that subscription in that a victim must open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44347 Adobe Interactive subscription of this subscription of the subscrip | | | | | | |
| Exploitation of this issue requires user inferaction in that avidim 2024-02-29 5.5 Medium Adobe Adobe inDesign versions IDIR 5 (and earlier) and IDI7.4-2 (and earlier) and aplication denia-berge this vulnerability to achieve an application denia-berge this vulnerability to achieve an application denia-berge this vulnerability to achieve an application denia-berge this vulnerability to that a victim must gene ameliations file. 2024-02-29 5.5 Medium CVE-2023-44345 Adobe Adobe inDesign versions IDIR 5 (and earlier) and IDI7.4-2 (and earlier) are affected by an out-of-bounds rad vulnerability to cold lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to those sensitive memory. An attacker could leverage this vulnerability to those those program disclosur file. 2024-02-29 5.5 Medium CVE-2023-44346 Adobe Adobe inDesign versions IDIR 5.1 (and earlier) and IDI7.4-2 (and earlier) are afficted by a NULL Dinter Dereference vulnerability. A nunauthenticated attacker could leverage this vulnerability to achieve an application dinti bissue requires user interaction in that a victim must open a malticus file. 2024-02-29 5.5 Medium CVE-2023-44347 Adobe IBM Cognox Analytics 11.1.7, 11.2.4, and 12.0.0 is vulnerable to cross site scripting. This vulnerability and user interaction in that a victim must open amalticus file. 2024-02-26 5.5 Medium CVE-2023-49051 IBM Vulnerability in system resource m | | | | | | |
| CVE_2023.44344 Adobe must open a malicious file. 2024.02.29 5.5 Medium Adobe infossing versions DID.8.3 (and earlier) and DID.7.4.2 (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 sure requires user interaction in the adobe infossing versions DID.8.5 (and earlier) and DID.7.4.2 (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 issure requires user interaction in that a victim must open a malicious file. 2024.02.29 5.5 Medium CVE-2023.44346 Adobe must open a malicious file. 2024.02.29 5.5 Medium CVE-2023.44346 Adobe must open a malicious file. 2024.02.29 5.5 Medium CVE-2023.44347 Adobe Instance and an advertime and advertime and advertime advev | | | | | | |
| cvf: 2023-44345 Adobe Advance could leverage this issue requires user interaction in that a victim must open a malicious file. 2024-02-29 5.5 Medium Cvf: 2023-44345 Adobe Adobe modern wershilt is sue requires user interaction in that a victim must open a malicious file. 2024-02-29 5.5 Medium Cvf: 2023-44345 Adobe Adobe modern wershilt balks (and carlier) and ID17-42 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leaverage this vulnerability to bypass mitigations such as ASLR. 2024-02-29 5.5 Medium Cvf: 2023-44345 Adobe must open a malicious file. 2024-02-29 5.5 Medium Cvf: 2023-44347 Adobe must open a malicious file. 2024-02-29 5.5 Medium Cvf: 2023-44347 Adobe IBM Cognos shnghists 11.17, 11.2.4, and 12.0.0 is vulnerability of achieve an application denial-of-service in the context of the current user, Exploitation of this issue requires user interaction in achieve an application denial-of-service in the context of the current user, Exploitation of this issue requires user interaction in achieve an application denial-of-service in the context of the current user, Exploitation of the were the were the mabed arbitrary harser to information leakage due to unverified sources in messages sen between Windows objects of different origins. IBM Avaliance abitrary tharesting the interac | CVE-2023-44344 | Adobe | | 2024-02-29 | 5.5 | Medium |
| An unauthenticated attacker could leverage this vulnerability to achieve an application of this issue requires user interaction in that a victim must open a malicious file. 2024-02-29 5.5 Medium CVF-2023-44345 Adobe Madbe inDesign versions IDIR 5 (and earlier) and IDIT A2 (and carlier) are affected by an out-of-boundr seal vulnerability. Utat could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability is submers bility to hypers mitigibility is such as ASIR. Exploration of this issue requires user interaction in that a victim must open a malicious file. 2024-02-29 5.5 Medium CVF-2023-44345 Adobe must open a malicious file. 2024-02-29 5.5 Medium CVF-2023-44346 Adobe must open a malicious file. 2024-02-29 5.5 Medium Adobe adhieve an application denial-of-service in the context of the current user. Exploitation denial-of-service in the context of the current user. Exploitation denial-of-service in the woll of this suber requires user interaction in that a victim must open a malicious file. 2024-02-29 5.5 Medium CVF-2023-44347 Adobe IBM Cognos Analytiss 11.7, 11.2.4, and 12.0.0 is vulnerability to eucherability in system resource management in Cisco UCS 5400 and 5505 Series fabric interconnetts that are in intersight 2024-02-26 5.4 Medium CVF-2023-43056 IBM Cognos Singliss 11.7, 11. | | | | | | |
| achieve an application demial-of-service in the context of the current user. Exploitation of this issue reginary sure interaction in 2024-02-29 5.5 Medium CVE-2023-44345 Adobe that a victim must open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44345 Adobe the software affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to thypass mitigations such as ASIA. 2024-02-29 5.5 Medium CVE-2023-44345 Adobe must open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44345 Adobe must open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44347 Adobe this issue reguines user interaction in achieve an application denial-of-service in the context of the current user. Exploitation of this issue reguines user interaction in achieve an application denial-of-service in the context of the current user. Exploitation of this issue reguines user interaction in achieve an application must open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44347 Adobe that a victim must open a malicious file. 2024-02-26 5.4 Medium CVE-2023-49551 IBM trus of essinite memory. 2024-02-26 <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td></td<> | | | | | | |
| cvre.tuser. Exploration of this issue requires user interaction in that a victim must open a malicious file. 2024-02-29 5.5 Medium cvre.2022-44345 Adobe Mode inDesign versions IDL8 5 (and earlier) and IDL7 42 (and carlier) are affected by an out-of-bound resolver vulnerability that could lead to disclosure of sensitive memory. An attacker could leavage this vulnerability to hypers mitigations such as ASIR. 2024-02-29 5.5 Medium cvre.2022-44345 Adobe must open a malicious file. 2024-02-29 5.5 Medium cvre.2022-44346 Adobe amility open simptions such as ASIR. 2024-02-29 5.5 Medium must open a malicious file. adobe inDesign versions IDL8.5 (and earlier) and IDL7.42 (and earlier) are affected by a VULL Pohice vulnerability. 2024-02-29 5.5 Medium cvre.2022-44342 Adobe Current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. 2024-02-29 5.5 Medium cvre.2022-44347 Adobe IBM Cognos Analytics 11.1.7, 11.2.4, and 12.0.0 is vulnerability to ensiste scripting. This vulnerability allows users to embed antitrary baseCription file. 2024-02-26 5.4 Medium cvre.2023-43051 IBM Cognos Analytics 11.1.7, 11.2.4, and 12.0.0 could be vulnerability in system resou | | | | | | |
| CVF-2023-44345 Adobe that a victim must open a malicious file. 2024-02-29 5.5 Medium CVF-2023-44345 Adobe Disegin versions ID3.5 (and carlier) and ID17.4 (and carlier) and tothounds 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 CVF-2023-44345 Adobe Adobe inDesign versions ID18.5 (and earlier) and ID17.4.2 (and earlier) and ID17.4.2 (and earlier) are filtered by an unathenticated attacker could leverage this vulnerability to achieve an application deniar-los-service in the context of the courter of the memory and the courter of the memory and the courter of the courter o | | | | | | |
| Adobe InDesign versions ID18.5 (and earlier) and ID17.4.2 (and earlier) are affected by an out-of-bound read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASL. CVE-2023-44346 Adobe must open a malicious file. 2024-02-29 5.5 Medium Adobe Indesign versions ID18.5 (and earlier) and ID17.4.2 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unsutthenticated 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-2023-44347 Adobe that a victim must open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44347 Adobe that a victim must open a malicious file. 2024-02-26 5.4 Medium CVE-2023-44347 Adobe that a victim must open a malicious file. 2024-02-26 5.4 Medium CVE-2023-44347 Adobe that a victim must open a malicious file. 2024-02-26 5.4 Medium CVE-2023-43051 IBM trust open sharkits 11.7, 11.2.4, and 12.0.0 could be vulnerability in system resource management in Cisco UCS 6400 and 6500 Serics Fabric Interconnects that are in Interright Managed | CVE-2023-44345 | Adobe | | 2024-02-29 | 5.5 | Medium |
| CVE-2023-44346 Adobe mest open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44346 Adobe mest open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44346 Adobe mest open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44347 Adobe The comparison IDA 55 (and carlier) and ID17 A.2 (and table in the context of the conte | | | | | | |
| Leverage this vulnerability to bypass mitigations such as ASLR. 2024-02-29 5.5 Medium CVE-2023-44345 Adobe Madobe inDesign versions ID18.5 (and earlier) and ID17.4.2 (and earlier) are affected by ANUL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application of this issue requires user interaction in that a victim must open a malicious file. 2024-02-29 5.5 Medium (VE-2023-44347) Adobe IBM Cognos Analytics 11.17, 11.24, and 12.0.0 is vulnerable to 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-2023-44347 Adobe IBM Cognos Analytics 11.17, 11.24, and 12.0.0 is vulnerable to current vuser. Exploitation leakage due to unverified sources in messages sent between Windows objects of different origins. 2024-02-26 5.4 Medium CVE-2023-43051 IBM trusted session. IBM X-Force ID: 267431. 2024-02-26 5.3 Medium CVE-2023-30996 IBM Vulnerability in system resource management in Cisco UCS 4000 and 6500 Series Fabric Interconnect Is that are in Intersight Managed Mode (IMM) could allow an unauthenticated, remote attacker to cause a device. An attacker to a dual addity an attacker to cause the Device Console UL system it for councel is needed to condition. A manaul reliad of series fabric interconnect Is needed to condition. A manaul reliad of th | | | - · · · · · | | | |
| CVF-2023-44346 Adobe Exploitation of this issue requires user interaction in that a victim must open a malicous file. 2024-02-29 5.5 Medium CVF-2023-44346 Adobe inDesign versions ID18.5 (and earlier) an ID17.4.2 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability. An unauthenticated attacker could leverage this vulnerability. 2024-02-29 5.5 Medium CVF-2023-44347 Adobe IBM Cognos Analytics 11.7. 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. 2024-02-25 5.4 Medium CVF-2023-43051 IBM trusted session. IBM X-Force ID: 267451. 2024-02-25 5.4 Medium CVF-2023-43051 IBM trusted session. IBM X-force ID: 267451. 2024-02-25 5.4 Medium CVF-2023-43051 IBM trusted session. IBM X-force ID: 267451. 2024-02-25 5.4 Medium CVF-2023-43096 IBM X-Force ID: 254290. 2024-02-26 5.3 Medium CVF-2023-30896 IBM X-force ID: 254290. 2024-02-29 | | | | | | |
| CVE-2023-44346 Adobe must open a malicious file. 2024-02-29 5.5 Medium Adobe Adobe inbesign versions 1018.5 (and earlier) and 1017.4.2 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application of this issue requires user interaction in the context of the current vuent. Exploitation of this issue requires user interaction in the transmitter variable to increase the context of the current variable to increase the scripting. This vulnerability to vulnerability to users interaction in the transmitter variable var | | | | | | |
| Adobe inDesign versions 1018.5 (and earlier) and 107-4.2 (and earlier) are affected by A WLL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application of this succendence interaction in the correct of the current user. Exploitation of this issue requires user interaction in this current user. Exploitation of this issue requires user interaction in the correct of the current user. Exploitation of this issue requires user interaction in consistence in the correct of the current user. Exploitation of this issue requires user interaction in consistence of the this way that way that way that the intended arbitrary lavaScript code in the Web UI thus aftering the intended arbitrary lavaScript code in the Web UI thus aftering 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 trusted session. IBM X-force ID: 267451. 2024-02-26 5.3 Medium CVE-2023-30996 IBM X-force ID: 254290. 2024-02-26 5.3 Medium Avoinerability 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 at leadia of the rice (DoS) condition on the Device Console UI or an affected device. 2024-02-29 5.3 Medium CVE-2023-20344 Cisco This vulnerability is due to insufficient rate-limiting of TCP connections to an affected device. 2024-02-29 5.3 Medium | CVF-2023-44346 | Adobe | | 2024-02-29 | 55 | Medium |
| cvE-2023-44347 Adobe 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 the context of the current user. Exploitation of this issue requires user interaction in the cross-site scripting. This vulnerability allows users to embed arbitrary lavaScript 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 Trusted session. IBM X-force ID: 267451. 2024-02-26 5.3 Medium cvE-2023-30996 IBM RV Cognos Analytics 11.17, 11.2.4, and 12.0.0 could be vulnerability in system resource management in Cisco UCS 6400 and 5500 Series Fabric Interconnects that are in intersight 2024-02-26 5.3 Medium CVE-2023-30996 IBM A vulnerability in system resource management in Cisco UCS 6400 and 5500 Series Fabric Interconnects that are in intersight 2024-02-26 5.3 Medium CVE-2023-30996 IBM A vulnerability is due to insufficient rate-limiting of TCP connects to the available to information of the packets to the Device Console UI on an affected device. 2024-02-29 5.3 Medium CVE-2024-2034 Cisco restore complete functionality. 2024-02-29 5.3 Medium CVE-2024-2034 Cisco | | 7,0050 | | 20210225 | 5.5 | Wiediam |
| cVE-2023-44347 Adobe achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction and that a victim must open a malicious file. 2024-02-29 5.5 Medium CVE-2023-44347 Adobe IBM Cognos Analytis: 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 tor credentials diclosure within a current within a trusted session. IBM X-force ID: 267451. 2024-02-26 5.4 Medium CVE-2023-30996 IBM trusted session. IBM X-force ID: 267451. 2024-02-26 5.3 Medium CVE-2023-30996 IBM X-force ID: 25420. 2024-02-26 5.3 Medium CVE-2023-30996 IBM X-force ID: 25420. 2024-02-26 5.3 Medium 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 or an affected device. An attacker could glow an attacker to cause the Device Console UI or an affected device. An attacker could allow an attacher to cause the Device Console UI or and field point in the current in resight the Vulnerability by sending a high number of TCP packets to the Device Console UI or an affected device. An attacker could glow an attacker to cause the Device Console UI process to | | | | | | |
| cvremt user, Exploitation of this issue requires user interaction in that a victim must open a mailcious file. 2024-02-29 5.5 Medium CVE-2023-44347 Adobe IBM Cognos Analytics 11.17, 11.24, and 12.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary lavaScriptic ode in the Web U thus altering the intended functionality potentially leading to credentials disclosure within a 2024-02-26 5.4 Medium CVE-2023-43051 IBM trusted session. IBM X-Force ID: 267451. 2024-02-26 5.4 Medium CVE-2023-30996 IBM X-Force ID: 254290. 2024-02-26 5.3 Medium CVE-2023-30996 IBM X-Force ID: 254290. 2024-02-26 5.3 Medium 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. 2024-02-29 5.3 Medium CVE-2024-20344 Cisco 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 process to crash, resulting in a DoS condition. A manual reload of the fabric interconnect is needed to conduct further attacks. IBM X-Force ID: 275038. </td <td></td> <td></td> <td>- · ·</td> <td></td> <td></td> <td></td> | | | - · · | | | |
| CVE-2023-44347 Adobe that a victim must open a malicious file. 2024-02-29 5.5 Medium 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 2024-02-26 5.4 Medium CVE-2023-43051 IBM trusted session. IBM X-Force ID: 267451. 2024-02-26 5.4 Medium CVE-2023-30996 IBM X-Force ID: 254290. 2024-02-26 5.3 Medium CVE-2023-30996 IBM X-Force ID: 254290. 2024-02-26 5.3 Medium 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. 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 of an affected device. 2024-02-29 5.3 Medium CVE-2024-20344 Cisco restore complete functionality. 2024-02-29 5.3 Medium IBM Cognos Command Center 10.2.4.1 and 1 | | | | | | |
| UBM 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 × Force ID: 257451. 2024-02-26 5.4 Medium CVE-2023-30996 IBM IBM Store ID: 257451. 2024-02-26 5.3 Medium CVE-2023-30996 IBM Vinerable 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 Avidnerability in system resource management in Clsco 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. 2024-02-29 5.3 Medium CVE-2024-20344 Cisco restore compilete functionality. 2024-02-29 5.3 Medium UPE-2023-50324 Cisco restore compilete functionality. 2024-02-29 5.3 Medium UPE-2023-50324 Cisco restore compilete functionality. 2024-02-29 5.3 Medium IBM Filenet Content Manager Component 5.5.8.0.5.5.10.0, and 5.5.11.0 could allow a remote attacker to culd allow an attacker to obtain | CVF-2023-44347 | Adobe | | 2024-02-29 | 55 | Medium |
| cvf=2023-30951 iBM 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 2024-02-26 5.4 Medium cvf=2023-30951 IBM trusted session. IBM X-Force ID: 267451. 2024-02-26 5.4 Medium cvf=2023-30996 IBM X-force ID: 254290. 2024-02-26 5.3 Medium cvf=2023-30996 IBM X-force ID: 254290. 2024-02-26 5.3 Medium cvf=2023-30996 IBM X-force ID: 254290. 2024-02-26 5.3 Medium 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. 2024-02-29 5.3 Medium This vulnerability is due to insufficient rate-limiting of TCP connections to an affected device. This vulnerability bending a high number of TCP packets to the Device Console UI of an affected device. 2024-02-29 5.3 Medium cvf=2024-20344 Gisco restore complete functionality. Force ID: 275038. 2024-02-29 5.3 Medium cvf=2024-20344 Gisco restore complete functionality. Force ID: 276738. 2024-02-29 5.3 Medium < | <u>CVL-2023-44347</u> | Adobe | | 2024-02-29 | 5.5 | weulum |
| CVE-2023-30301 IBM functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 267451. 2024-02-26 5.4 Medium IBM Cognos Analytics 11.1.7.1.2.4, 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-2023-30996 IBM X-Force ID: 254290. 2024-02-26 5.3 Medium 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. S.3 Medium CVE-2024-20344 Cisco This vulnerability is due to insufficient rate-limiting of TCP connections to an affected device. An attacker could exploit this vulnerability by sendig a high number of TCP packets to the Device Console UI of an affected device. An attacker could exploit this vulnerability by sendig a high number of TCP packets to the Device Console UI and an attacker 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 the SAspNet-Version Response Header that could allow an attacker to obtain information of the application environment to conduct further attacks. BMX -Force ID: 275038. 2024-03-01 5.3 Medium CVE-2023-50324 IBM IBM Filenet Content Manager Component 5.5.8.0, 5.5.10.0, | | | | | | |
| CVE-2023-43051 IBM trusted session. IBM X-Force ID: 267451. 2024-02-26 5.4 Medium IBM Cognos Analytics 11.17, 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 2024-02-26 5.3 Medium CVE-2023-30996 IBM X-Force ID: 254290. 2024-02-26 5.3 Medium 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. 5.3 Medium 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 create the Device Console UI process to crash, resulting in a DoS 2024-02-29 5.3 Medium CVE-2024-20344 Cisco restore complete functionality. 2024-02-10 5.3 Medium CVE-2023-50324 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 env | | | | | | |
| CVE-2023-30996 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 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. 2024-02-26 5.3 Medium CVE-2024-20344 Cisco 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 UVE-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 UVE-2023-50324 IBM IBM Filenet Content Manager Component 5.5.8.0, 5.5.10.0, and 5.5.1.1.0 could allow a remote attacker to traverse directories on the system. An attacker could sequences (//) to view arbitrary files on the system. IBM X-Force ID: 261115. <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td></t<> | | | | | | |
| CVE-2023-30996 IBM X-Force ID: 254290. 2024-02-26 5.3 Medium 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. X-V X-V This vulnerability is gue to insufficient rate-limiting of TCP connections to an affected device. X-V X-V X-V CVE-2024-20344 Cisco restore console UI of 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 2024-02-29 5.3 Medium CVE-2023-20324 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-2023-50324 IBM IBM Force ID: 2511.5 2024-03-01 5.3 Medium S.5.11.0. could allow are attacker to traverse directories on the system. IBM X-Force ID: 275038. 2024-03-01 5.3 Medium UFE-2023-38366 IBM System. Responser Listory T20.0. | <u>CVE-2023-43051</u> | IBIVI | | 2024-02-26 | 5.4 | Iviedium |
| CVE-2023-30996 IBM messages sent between Windows objects of different origins. IBM X-Force ID: 254290. 2024-02-26 5.3 Medium 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. Image: Court of the cause and enal of service (DoS) condition on the Device Console UI of 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-2023-20342 Cisco IBM Cognos Command Center 10.2.4.1 and 10.2.5 exposes details the X-spyte-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-2023-50324 IBM conduct further attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (<i>I</i> ./) to view arbitrary files on the system. IBM X-Force ID: 274711. 2024-03-01 5.3 Medium CVE-2023-50312 IBM IBM Keopsphere Application Server Liberty 17.0.0.3 through 24.0.0.2 could provide weaker than expected | | | - · · · · · · · · · · · · · · · · · · · | | | |
| 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. 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-2023-20344 Cisco restore complete functionality. 2024-03-01 5.3 Medium UE-2023-50324 IBM Conduct further attacks. IBM X-Force ID: 275038. 2024-03-01 5.3 Medium UE-2023-38366 IBM system. IBM X-Force ID: 27038. 2024-03-01 5.3 Medium CVE-2023-38366 IBM system. IBM X-Force ID: 2711. 2024-03-01 5.3 Medium CVE-2023-50312 IBM IBM Flence 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. IBM X-Force ID: 27411. 2024-03-01 5.3 Medium CVE-2023-38366 IBM system. IBM X-Force ID: 274711. 2024-03-01 | | | - | | | |
| 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. An attacker could exploit 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 as successful exploit could allow an attacker to cause the Device Console UI as successful exploit could allow an attacker to cause the Device Console UI as successful exploit could allow an attacker to cause the Device Console UI as successful exploit could allow an attacker to cause the Device Console UI as successful exploit could allow an attacker to cause the Device Console UI as successful exploit could allow an attacker to cause the Device Console UI as successful exploit could allow an attacker to cause the Device Console UI as successful exploit could allow an attacker to cause the Device Console UI as successful exploit could allow an attacker to attacker to obtain information of the application environment to conduct further attacks. IBM X-Force ID: 275038. 2024-02-29 5.3 Medium CVE-2023-50324 IBM IBM Silenet 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. BM X-Force ID: 254115. 2024-03-01 5.3 Medium CVE-2023-50312 IBM configuration. IBM X-Force ID: 274711. 2024-03-01 5.3 Medium Avulnerability in the VirusEvent | CVE-2023-30996 | IBM | X-Force ID: 254290. | 2024-02-26 | 5.3 | Medium |
| 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.Image: Console UI of an affected device.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 nocess ful 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.2024-02-295.3MediumCVE-2024-20344Ciscorestore complete functionality.2024-02-295.3MediumCVE-2023-50324IBMconduct further attacks. IBM X-Force ID: 275038.2024-03-015.3MediumCVE-2023-50324IBMinformation of the application environment to conduct further attacker could send a specially crafted URL request containing "dot dot" sequences (/./) to view arbitrary files on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/./) to view arbitrary files on the 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: 274711.2024-03-015.3MediumCVE-2023-50312IBMconductions caused by a failure to honor user configuration. IBM X-Force ID: 274711.2024-03-015.3MediumCVE-2023-50312IBMconductions caused by a failure to honor user configuration. IBM X-Force ID: 274711.2024-03-015.3Medium | | | | | | |
| attacker to cause a denial of service (DoS) condition on the Device Console UI of an affected device.attacker Console UI of an affected device.attacker console UI of an affected device.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.2024-02-295.3MediumCVE-2024-20344Ciscorestore complete functionality.2024-02-295.3MediumCVE-2023-50324IBMConduct further attacks. IBM X-Force ID: 275038.2024-03-015.3MediumCVE-2023-50324IBMSystem. An attacker could send a specially crafted URI request containing "dot dot" sequences (//) to view arbitrary files on the system. IBM X-Force ID: 261115.2024-03-015.3MediumCVE-2023-50312IBMconduct further attacker could security for outbound TLS connections caused by a failure to honor user configuration. IBM X-Force ID: 27411.2024-03-015.3Medium | | | | | | |
| Console UI of an affected device.Image: Console UI of an affected device.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.2024-02-295.3MediumCVE-2024-20344Ciscorestore complete functionality.2024-02-295.3MediumIBM 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 CVE-2023-503242024-03-015.3MediumIBM 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: 261115.2024-03-015.3MediumIBM 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: 274711.2024-03-015.3MediumCVE-2023-50312IBMA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of5.3Medium | | | | | | |
| CVE-2024-20344CiscoIBM 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: 275038.2024-03-015.3MediumCVE-2023-50324IBMIBM 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 sequences (//) to view arbitrary files on the system. IBM X-Force ID: 261115.2024-03-015.3MediumCVE-2023-50312IBMIBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.2 could provide weaker than expected security for outbound TLS connections Cause of Cause than expected security for outbound TLS connections IBM X-Force ID: 274711.2024-03-015.3Medium | | | | | | |
| 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.2024-02-295.3MediumCVE-2024-20344Ciscorestore complete functionality.2024-02-295.3MediumCVE-2023-50324IBM 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: 275038.2024-03-015.3MediumCVE-2023-50324IBMiBM 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: 261115.2024-03-015.3MediumCVE-2023-50312IBMconfiguration. IBM X-Force ID: 274711.2024-03-015.3MediumCVE-2023-50312IBMconfiguration. IBM X-Force ID: 274711.2024-03-015.3Medium | | | | | | |
| 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.2024-02-295.3MediumCVE-2024-20344Ciscorestore complete functionality.2024-02-295.3MediumIBM 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: 275038.2024-03-015.3MediumCVE-2023-50324IBMIBM 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: 261115.2024-03-015.3MediumCVE-2023-50312IBMconfiguration. IBM X-Force ID: 274711.2024-03-015.3MediumCVE-2023-50312IBMconfiguration. IBM X-Force ID: 274711.2024-03-015.3MediumA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of5.3Medium | | | | | | |
| 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.2024-02-295.3MediumCVE-2024-20344Ciscorestore complete functionality.2024-02-295.3MediumIBM 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 COVE-2023-503242024-03-015.3MediumCVE-2023-50324IBMconduct further attacks. IBM X-Force ID: 275038.2024-03-015.3MediumCVE-2023-50324IBMconduct further attacks. IBM X-Force ID: 275038.2024-03-015.3MediumCVE-2023-38366IBMsystem. IBM X-Force ID: 261115.2024-03-015.3MediumCVE-2023-50312IBMconfiguration. IBM X-Force ID: 274711.2024-03-015.3MediumCVE-2023-50312IBMconfiguration. IBM X-Force ID: 274711.2024-03-015.3MediumA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands | | | | | | |
| 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.2024-02-295.3MediumCVE-2024-20344CiscoIBM 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: 275038.2024-03-015.3MediumCVE-2023-50324IBMIBM 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: 261115.2024-03-015.3MediumCVE-2023-50312IBMIBM Ellemet Content Ibm X-Force ID: 274711.2024-03-015.3MediumCVE-2023-50312IBMA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of5.3Medium | | | | | | |
| CVE-2024-20344Ciscocause 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.2024-02-295.3MediumIBM 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: 275038.2024-03-015.3MediumCVE-2023-50324IBMconduct further attacks. IBM X-Force ID: 275038.2024-03-015.3MediumCVE-2023-50326IBMiBM 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: 261115.2024-03-015.3MediumCVE-2023-50312IBMIBM 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 user2024-03-015.3MediumCVE-2023-50312IBMconfiguration. IBM X-Force ID: 274711.2024-03-015.3Medium | | | | | | |
| CVE-2024-20344Ciscocondition. A manual reload of the fabric interconnect is needed to restore complete functionality.2024-02-295.3MediumIBM 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: 275038.2024-03-015.3MediumCVE-2023-50324IBMconduct further attacks. IBM X-Force ID: 275038.2024-03-015.3MediumIBM 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: 261115.2024-03-015.3MediumCVE-2023-38366IBMsystem. IBM X-Force ID: 261115.2024-03-015.3MediumCVE-2023-50312IBMconfiguration. IBM X-Force ID: 274711.2024-03-015.3MediumA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of5.3Medium | | | | | | |
| 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: 275038.2024-03-015.3MediumIBMIBMIBM 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: 261115.2024-03-015.3MediumCVE-2023-38366IBMsystem. IBM X-Force ID: 261115.2024-03-015.3MediumIBM 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: 274711.2024-03-015.3MediumA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of5.3Medium | | | | | | |
| CVE-2023-50324IBMthe 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: 275038.2024-03-015.3MediumCVE-2023-50324IBMIBM 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: 261115.2024-03-015.3MediumCVE-2023-38366IBMsystem. IBM X-Force ID: 261115.2024-03-015.3MediumCVE-2023-50312IBMIBM 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: 274711.2024-03-015.3MediumCVE-2023-50312IBMA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of5.3Medium | <u>CVE-2024-20344</u> | Cisco | | 2024-02-29 | 5.3 | Medium |
| CVE-2023-50324IBMattacker to obtain information of the application environment to conduct further attacks. IBM X-Force ID: 275038.2024-03-015.3MediumIBM 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: 261115.2024-03-015.3MediumCVE-2023-38366IBMsystem. IBM X-Force ID: 261115.2024-03-015.3MediumIBM 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: 274711.2024-03-015.3MediumCVE-2023-50312IBMA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of5.3Medium | | | | | | |
| CVE-2023-50324IBMconduct further attacks. IBM X-Force ID: 275038.2024-03-015.3MediumIBM 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: 261115.2024-03-015.3MediumCVE-2023-38366IBMsystem. IBM X-Force ID: 261115.2024-03-015.3MediumIBM 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: 274711.2024-03-015.3MediumCVE-2023-50312IBMA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of5.3Medium | | | | | | |
| 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: 261115.2024-03-015.3MediumCVE-2023-38366IBMIBM 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 user2024-03-015.3MediumCVE-2023-50312IBMconfiguration. IBM X-Force ID: 274711.2024-03-015.3MediumA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of5.3Medium | CVE-2023-50324 | IBM | | 2024-03-01 | 53 | Medium |
| CVE-2023-38366IBM5.5.11.0 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: 261115.2024-03-015.3MediumCVE-2023-38366IBMIBM 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 user2024-03-015.3MediumCVE-2023-50312IBMconfiguration. IBM X-Force ID: 274711.2024-03-015.3MediumA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of5.3Medium | <u>010_002</u> | .0.11 | | | 5.5 | |
| CVE-2023-38366IBMcontaining "dot dot" sequences (//) to view arbitrary files on the system. IBM X-Force ID: 261115.2024-03-015.3MediumIBM 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: 274711.2024-03-015.3MediumCVE-2023-50312IBMconfiguration. IBM X-Force ID: 274711.2024-03-015.3MediumA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of5.3Medium | | | | | | |
| CVE-2023-38366IBMsystem. IBM X-Force ID: 261115.2024-03-015.3MediumIBM 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: 274711.2024-03-015.3MediumCVE-2023-50312IBMA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of5.3Medium | | | | | | |
| CVE-2023-50312IBMWebSphere 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: 274711.2024-03-015.3MediumA vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges ofIBMIBMIBM | | | | | - - | |
| CVE-2023-50312 IBM 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 A vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of 5.3 Medium | <u>CVE-2023-38366</u> | IBM | | 2024-03-01 | 5.3 | Medium |
| CVE-2023-50312 IBM outbound TLS connections caused by a failure to honor user configuration. IBM X-Force ID: 274711. 2024-03-01 5.3 Medium A vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of Image: Content of the privileges of | | | | | | |
| CVE-2023-50312 IBM configuration. IBM X-Force ID: 274711. 2024-03-01 5.3 Medium A vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of 5.3 Medium | | | | | | |
| A vulnerability in the VirusEvent feature of ClamAV could allow a local attacker to inject arbitrary commands with the privileges of | CVE-2023-50312 | IBM | | 2024-03-01 | 5.3 | Medium |
| | | | A vulnerability in the VirusEvent feature of ClamAV could allow a | | | |
| CVE-2024-20328 Cisco 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. 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 |
| <u>CVL-2023-30303</u> | | Debian's cpio contains a path traversal vulnerability. This issue was | 2024-03-01 | 5.1 | Weddini |
| | | introduced by reverting CVE-2015-1197 patches which had caused a regression inno-absolute-filenames. Upstream has since | | | |
| <u>CVE-2023-7207</u> | Debian | provided a proper fix tono-absolute-filenames. | 2024-02-29 | 4.9 | Medium |
| | | 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 | | | |
| CVE-2023-28525 | IBM | trusted session. IBM X-Force ID: 251052. | 2024-03-01 | 4.8 | Medium |
| | | 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 | | | |
| <u>CVE-2023-32344</u> | IBM | to reference an arbitrary path. IBM X-Force ID: 255898. | 2024-02-26 | 4.3 | Medium |
| | | 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 | | | |
| 01/5 2022 25022 | | dangerous types that can be automatically processed within the product's environment. IBM X-Force ID: 247621. | 2024-02-28 | 4.3 | Medium |
| <u>CVE-2023-25922</u> | IBM | Due to insufficient server-side validation, an attacker with login | 2024-02-28 | 4.5 | weaturn |
| | | privileges could access certain resources that the attacker should | | | |
| <u>CVE-2024-25064</u> | Hikvision | not have access to by changing parameter values. | 2024-03-02 | 4.3 | Medium |
| | | IBM Watson CloudPak for Data Data Stores information disclosure | | | |
| | | 4.6.0 allows web pages to be stored locally which can be read by | | | |
| <u>CVE-2023-27545</u> | IBM | another user on the system. IBM X-Force ID: 248947. | 2024-02-29 | 4 | Medium |
| | | Dell Secure Connect Gateway, 5.18, contains an Inadequate | | | |
| | | Encryption Strength Vulnerability. An unauthenticated network | | | |
| CVE_2024_22459 | Dell | attacker could potentially exploit this vulnerability, allowing an attacker to recover plaintext from a block of ciphertext. | 2024-03-01 | 3.7 | Low |
| <u>CVE-2024-22458</u> | Dell | | 2024-03-01 | 5.7 | LOW |

Where NCA provides the vulnerability information as published by NIST's . وإذ تبقى NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة. implementation of appropriate recommendations.

متاح