Release Notes for Cisco Cyber Vision Knowledge DB

Release 202309

Compatible device list

Center	Description
All version 4 centers	All Cisco Cyber Vision center version 4 are compatible with this Knowledge DB file.

Links

Software Download

The files listed below can be found using the following link:

https://software.cisco.com/download/home/286325414/type

Center	Description
CiscoCyberVision-center-4.2.4.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.2.4.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.2.4.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.2.4.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.2.4.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.2.4.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.2.4.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.2.4.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.4.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.2.4.dat	Knowledge DB embedded in Cisco Cyber Vision 4.2.4
Updates/KDB/KDB.202309	**Description**
CiscoCyberVision_knowledgedb_20230901.db	Knowledge DB version 20230901
CiscoCyberVision_knowledgedb_20230908.db	Knowledge DB version 20230908
CiscoCyberVision_knowledgedb_20230915.db	Knowledge DB version 20230915
CiscoCyberVision_knowledgedb_20230922.db	Knowledge DB version 20230922
CiscoCyberVision_knowledgedb_20230929.db	Knowledge DB version 20230929

Related Documentation

- Cisco Cyber Vision GUI User Guide:

  https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/GUI/b_Cisco_Cyber_Vision_GUI_User_Guide.html

Database download

Cisco Cyber Vision uses an internal database which contains the list of recognized vulnerabilities, icons, threats, etc. Cisco has published a new Knowledge DB for Cisco Cyber Vision. This Knowledge DB (or KDB) is essential for Cisco Cyber Vision. It allows, in particular, the detection of vulnerabilities.

This database can be updated using the file available from the link above. The file contains a built-in RSA signature and external checking is not required; the file will be verified by Cisco Cyber Vision Center at import time.

How to update the database

To update the Knowledge DB:

1. Download the latest DB file available.
2. From the Cisco Cyber Vision system administration page, click the Import a knowledge DB button to upload the file.

Importing the new database will rematch your existing components against any new vulnerabilities.

Release contents

20230929

This release includes additions and modifications to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2023-09-28 (https://www.snort.org/advisories/talos-rules-2023-09-28)**
- **Talos Rules 2023-09-26 (https://www.snort.org/advisories/talos-rules-2023-09-26)**

The new and updated Snort rules span the following categories:

- 2 malware-cnc rules with SIDs 300710, 62452
- 2 os-windows rules with SIDs 300711, 300712
- 5 server-webapp rules with SIDs 300715, 300716, 300714, 62104, 300713

This release also adds support and modifications for the detection of the following vulnerabilities:

- CVE-2017-12652: (Improper Input Validation Vulnerability in Rockwell Automation PanelView 800)
  - An input/output validation vulnerability exists in a third-party component that the PanelView™ 800 utilizes. Libpng, which is PNG's reference library, version 1.6.32 and earlier does not properly check the length of chunks against the user limit. Libpng versions prior to 1.6.32 are susceptible to a vulnerability which, when successfully exploited, could potentially lead to a disclosure of sensitive information, addition or modification of data, or a denial-of-service condition.
- CVE-2023-2262: (Stack-based Buffer Overflow in Rockwell Logix Communication Modules)
  - A buffer overflow vulnerability exists in select communication devices. If exploited, a threat actor could potentially leverage this vulnerability to perform a remote code execution. To exploit this vulnerability, a threat actor would have to send a maliciously crafted CIP request to device.
- CVE-2022-1737: (Denial-of-Service Vulnerability in Rockwell Distributed I/O Communication Modules)
  - Pyramid Solutions' affected products, the Developer and DLL kits for EtherNet/IP Adapter and EtherNet/IP Scanner may be vulnerable to an out-of-bounds write, which may allow an unauthorized threat actor to send a specially crafted packet that may result in a denial-of-service condition.
- CVE-2023-33239: (Command-injection Vulnerability in the Key-generation Function in Moxa TN-5900 and TN-4900 Series)
  - TN-4900 Series firmware versions v1.2.4 and prior and TN-5900 Series firmware versions v3.3 and prior are vulnerable to the command injection vulnerability. This vulnerability stems from insufficient input validation in the key-generation function, which could potentially allow malicious users to execute remote code on affected devices.
- CVE-2023-34216: (Command-injection Vulnerability in the Key-delete Function of Moxa TN-5900 and TN-4900 Series)

  - TN-4900 Series firmware versions v1.2.4 and prior and TN-5900 Series firmware versions v3.3 and prior are vulnerable to the command-injection vulnerability. This vulnerability derives from insufficient input validation in the key-delete function, which could potentially allow malicious users to delete arbitrary files.

- CVE-2023-34215: (Command-injection Vulnerability in the Certificate-generation Function of Moxa TN-5900 and TN-4900 Series)
  - TN-5900 Series firmware versions v3.3 and prior are vulnerable to the command-injection vulnerability. This vulnerability stems from insufficient input validation and improper authentication in the certification-generation function, which could potentially allow malicious users to execute remote code on affected devices.
- CVE-2023-33238: (Command-injection Vulnerability in Certificate Management in Moxa TN-5900 and TN-4900 Series)
  - TN-4900 Series firmware versions v1.2.4 and prior and TN-5900 Series firmware versions v3.3 and prior are vulnerable to the command injection vulnerability. This vulnerability stems from inadequate input validation in the certificate management function, which could potentially allow malicious users to execute remote code on affected devices.
- CVE-2023-33237: (Authentication Bypass Without Administrator Privilege in Moxa TN-5900 and TN-4900 Series)
  - TN-5900 Series firmware version v3.3 and prior is vulnerable to improper-authentication vulnerability. This vulnerability arises from inadequate authentication measures implemented in the web API handler, allowing low-privileged APIs to execute restricted actions that only high-privileged APIs are allowed This presents a potential risk of unauthorized exploitation by malicious actors.
- CVE-2023-34214: (Command-injection Vulnerability in the Key-generation Function of Moxa TN-5900 and TN-4900 Series)
  - TN-4900 Series firmware versions v1.2.4 and prior and TN-5900 Series firmware versions v3.3 and prior are vulnerable to the command-injection vulnerability. This vulnerability stems from insufficient input validation in the certificate-generation function, which could potentially allow malicious users to execute remote code on affected devices.
- CVE-2023-34217: (Command-injection Vulnerability in the Certificate-delete Function of Moxa TN-5900 and TN-4900 Series)
  - TN-4900 Series firmware versions v1.2.4 and prior and TN-5900 Series firmware versions v3.3 and prior are vulnerable to the command-injection vulnerability. This vulnerability stems from insufficient input validation in the certificate-delete function, which could potentially allow malicious users to delete arbitrary files.
- CVE-2023-34213: (Command-injection Vulnerability in the Key-generation Function of Moxa TN-5900 and TN-4900 Series)
  - TN-5900 Series firmware versions v3.3 and prior are vulnerable to command-injection vulnerability. This vulnerability stems from insufficient input validation and improper authentication in the key-

generation function, which could potentially allow malicious users to execute remote code on affected devices.

20230922

This release includes additions and modifications to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2023-09-21 (https://www.snort.org/advisories/talos-rules-2023-09-21)**
- **Talos Rules 2023-09-19 (https://www.snort.org/advisories/talos-rules-2023-09-19)**

The new and updated Snort rules span the following categories:

- 1 file-pdf rules with SIDs 300692
- 1 malware-cnc rules with SIDs 62414
- 18 malware-other rules with SIDs 300703, 300694, 300701, 300700, 300698, 300702, 300709, 300697, 300706, 300704, 300708, 300707, 300695, 300467, 300696, 300705, 300693, 300699
- 1 policy-other rules with SIDs 62451

20230915

This release includes additions and modifications to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2023-09-14 (https://www.snort.org/advisories/talos-rules-2023-09-14)**
- **Talos Rules 2023-09-12 (https://www.snort.org/advisories/talos-rules-2023-09-12)**

The new and updated Snort rules span the following categories:

- 1 file-pdf rules with SIDs 300692
- 2 malware-backdoor rules with SIDs 300690, 300689
- 1 malware-cnc rules with SIDs 62393
- 6 os-windows rules with SIDs 300691, 62396, 57193, 300687, 300688, 62401
- 2 server-webapp rules with SIDs 62383, 62384

20230908

This release includes additions and modifications to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2023-09-07 (https://www.snort.org/advisories/talos-rules-2023-09-07)**
- **Talos Rules 2023-09-05 (https://www.snort.org/advisories/talos-rules-2023-09-05)**

The new and updated Snort rules span the following categories:

- 1 malware-other rule with SID 300681
- 5 malware-tools rules with SIDs 300686, 300684, 300683, 300685, 300682

20230901

This release includes additions and modifications to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2023-08-29 (https://www.snort.org/advisories/talos-rules-2023-08-29)**
- **Talos Rules 2023-08-31 (https://www.snort.org/advisories/talos-rules-2023-08-31)**

The new and updated Snort rules span the following categories:

- 4 exploit-kit rules with SIDs 44738, 62349, 62348, 62349
- 3 file-other rules with SIDs 300678, 300679, 300680
- 3 malware-cnc rules with SIDs 62325, 47178, 62362
- 3 malware-other rules with SIDs 300672, 300671, 300673
- 1 os-windows rules with SID 62347
- 12 server-webapp rules with SIDs 300675, 300677, 300674, 300676, 62342, 62344, 62345, 62343, 62346, 62326, 62331, 300677