Release Notes for Cisco Cyber Vision Knowledge DB

Release 202305

Compatible device list *2*

Links *2*

Software Download 2

Related Documentation 3

Database download *3*

How to update the database *3*

Release contents *4*

20230526 4

20230512 4

20230505 5

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-4.2.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.2.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.2.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.2.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.2.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.2.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.2.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.2.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.2.0.dat	Knowledge DB embedded in Cisco Cyber Vision 4.2.0
Updates/KDB/KDB.202305	**Description**
CiscoCyberVision_knowledgedb_20230505.db	Knowledge DB version 20230505
CiscoCyberVision_knowledgedb_20230512.db	Knowledge DB version 20230512
CiscoCyberVision_knowledgedb_20230526.db	Knowledge DB version 20230526

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

20230526

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

- **Talos Rules 2023-05-25 (https://www.snort.org/advisories/talos-rules-2023-05-25)**
- **Talos Rules 2023-05-23 (https://www.snort.org/advisories/talos-rules-2023-05-23)**
- **Talos Rules 2023-05-18 (https://www.snort.org/advisories/talos-rules-2023-05-18)**
- **Talos Rules 2023-05-16 (https://www.snort.org/advisories/talos-rules-2023-05-16)**
- **Talos Rules 2023-05-12 (https://www.snort.org/advisories/talos-rules-2023-05-12**)

The new and updated Snort rules span the following categories:

- 1 file-other rule with SID 300554
- 1 malware-cnc rule with SID 300543
- 1 malware-other rule with SID 300544
- 2 os-linux rules with SID 300552, 300553
- 9 os-windows rules with SID 300551, 300550, 300549, 300548, 300547, 300546, 300545, 59521, 59522
- 1 policy-other rule with SID 61800
- 1 server-other rule with SID 36826
- 10 server-webapp rules with SID 39908, 61765, 61766, 61783, 61784, 61794, 61795, 61798, 61799, 61801

20230512

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

- **Talos Rules 2023-05-11 (https://www.snort.org/advisories/talos-rules-2023-05-11)**
- **Talos Rules 2023-05-09 (https://www.snort.org/advisories/talos-rules-2023-05-09)**

The new and updated Snort rules span the following categories:

- 2 file-image rules with SIDs 300528, 300530
- 1 file-office rule with SID 300525
- 14 malware-other rules with SIDs 61708, 300529, 300531, 300532, 300533, 300534, 300535, 300536, 300537, 300538, 300539, 300540, 300541, 300542
- 5 os-windows rules with SIDs 300522, 61707, 300524, 300526, 300527
- 7 policy-other rules with SIDs 61724, 61725, 61726, 61727, 61728, 61729, 61736
- 5 server-webapp rules with SIDs 61709, 300523, 61713, 61720, 61721

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

- CVE-2022-46680: (Cleartext Transmission of Sensitive Information in Schneider PowerLogic ION7400 / PM8000 / ION9000 Power Meters)
  - Schneider Electric is aware of the use of an unsecure protocol in its PowerLogic ION9000, PowerLogic ION7400, PowerLogic PM8000, PowerLogic ION8650, PowerLogic ION8800 and all legacy ION products. A CWE-319: Cleartext transmission of sensitive information vulnerability exists that could cause disclosure of sensitive information, denial of service, or modification of data if an attacker is able to intercept network traffic.
- CVE-2023-27410: (Heap-based Buffer Overflow Vulnerability in Siemens SCALANCE LPE9403)
  - A heap-based buffer overflow vulnerability was found in the edgebox_web_app binary. The binary will crash if supplied with a backup password longer than 255 characters. This could allow an authenticated privileged attacker to cause a denial of service.
- CVE-2023-27409: (Path Traversal Vulnerability in Siemens SCALANCE LPE9403)
  - A path traversal vulnerability was found in the deviceinfo binary via the mac parameter. This could allow an authenticated attacker with access to the SSH interface on the affected device to read the contents of any file named address.
- CVE-2023-27408: (Insecure Temporary File Vulnerability in Siemens SCALANCE LPE9403)
  - The i2c mutex file is created with the permissions bits of -rw-rw-rw-. This file is used as a mutex for multiple applications interacting with i2c. This could allow an authenticated attacker with access to the SSH interface on the affected device to interfere with the integrity of the mutex and the data it protects.
- CVE-2023-27407: (Command Injection Vulnerability in Siemens SCALANCE LPE9403)
  - The web based management of affected device does not properly validate user input, making it susceptible to command injection. This could allow an authenticated remote attacker to access the underlying operating system as the root user.
- CVE-2022-47522: (Improper Input Validation in Siemens SCALANCE W1750D)
  - The IEEE 802.11 specifications through 802.11ax allow physically proximate attackers to intercept (possibly cleartext) target-destined frames by spoofing a target's MAC address, sending Power Save frames to the access point, and then sending other frames to the access point (such as authentication frames or re-association frames) to remove the target's original security context. This behavior occurs because the specifications do not require an access point to purge its transmit queue before removing a client's pairwise encryption key.

20230505

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

- **Talos Rules 2023-05-04 (https://www.snort.org/advisories/talos-rules-2023-05-04)**

- **Talos Rules 2023-05-02 (https://www.snort.org/advisories/talos-rules-2023-05-02)**

The new and updated Snort rules span the following categories:

- 1 malware-cnc rules with SID 61689
- 3 policy-other rules with SIDs 61692, 61702, 61703
- 5 server-webapp rules with SIDs 61690, 61691, 61697, 61698, 300521