Release Notes for Cisco Cyber Vision Knowledge DB

Release 202307

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-4.2.2.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.2.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.2.2.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.2.2.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.2.2.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.2.2.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.2.2.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.2.2.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.2.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.2.2.dat	Knowledge DB embedded in Cisco Cyber Vision 4.2.1
Updates/KDB/KDB.202307	**Description**
CiscoCyberVision_knowledgedb_20230707.db	Knowledge DB version 20230707
CiscoCyberVision_knowledgedb_20230724.db	Knowledge DB version 20230724
CiscoCyberVision_knowledgedb_20230728.db	Knowledge DB version 20230728

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

20230728

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

- **Talos Rules 2023-07-27 (https://www.snort.org/advisories/talos-rules-2023-07-27)**
- **Talos Rules 2023-07-25 (https://www.snort.org/advisories/talos-rules-2023-07-25)**

The new and updated Snort rules span the following categories:

- 1 file-pdf rules with SID 300629
- 2 malware-backdoor rules with SIDs 300631, 300632
- 1 malware-cnc rules with SID 300589
- 1 server-other rules with SID 62107
- 22 server-webapp rules with SIDs 300630, 62102, 62103, 62104, 62108, 62109, 62110, 62111, 62112, 62113, 62114, 62115, 62116, 62121, 62122, 62123, 62124, 62125, 62127, 62128, 62129, 62130

20230724

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

- **Talos Rules 2023-07-20 (https://www.snort.org/advisories/talos-rules-2023-07-20)**
- **Talos Rules 2023-07-18 (https://www.snort.org/advisories/talos-rules-2023-07-18)**
- **Talos Rules 2023-07-12 (https://www.snort.org/advisories/talos-rules-2023-07-12-7-12-2023)**
- **Talos Rules 2023-07-12 (https://www.snort.org/advisories/talos-rules-2023-07-12)**
- **Talos Rules 2023-07-11 (https://www.snort.org/advisories/talos-rules-2023-07-11)**

The new and updated Snort rules span the following categories:

- 11 protocol-scada rules with SIDs 62028, 62029, 61927, 61928, 62030, 62031, 61929, 61930, 62032, 62033, 61931
- 1 file-office rules with SID 300615
- 1 malware-backdoor rules with SID 300616
- 6 malware-cnc rules with SIDs 62057, 62060, 62061, 62084, 62085, 62086
- 14 malware-other rules with SIDs 300617, 300618, 300619, 300620, 300621, 300622, 300623, 300624, 300625, 300626, 300608, 300609, 300610, 300611
- 3 os-windows rules with SIDs 300612, 300613, 300614
- 1 server-other rules with SID 62047

- 33 server-webapp rules with SIDs 47458, 47459, 47460, 62036, 62037, 62038, 62039, 62040, 62041, 62042, 62043, 62044, 62045, 62046, 62049, 62050, 62051, 62052, 62095, 62096, 62097, 62098, 62099, 62100, 62101, 300627, 300628, 62009, 62012, 62013, 62026, 62027, 300607

In particular, the protocol-scada rules detect remote code execution and denial-of-service vulnerabilities affecting select Rockwell ControlLogix communication modules. Exploitation of these vulnerabilities could allow malicious actors to gain remote access of the running memory of the module and perform malicious activity, such as manipulating the module's firmware, inserting new functionality into the module, wiping the module's memory, falsifying traffic to/from the module, establishing persistence on the module, and potentially affect the underlying industrial process. Please consult the associated Rockwell advisory for more information and for mitigations:

https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140010

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

- CVE-2023-3595: (Out-of-bounds Write Vulnerability in Rockwell ControlLogix Communication Modules)
    - Where this vulnerability exists in the 1756 EN2* and 1756 EN3* products, it could allow a malicious user to perform remote code execution with persistence on the target system through maliciously crafted CIP messages. This includes the ability to modify, deny, and exfiltrate data passing through the device.
- CVE-2023-3596: (Out-of-bounds Write Vulnerability in Rockwell ControlLogix Communication Modules)
    - Where this vulnerability exists in the 1756-EN4* products, it could allow a malicious user to cause a denial of service by asserting the target system through maliciously crafted CIP messages.

20230707

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

- **Talos Rules 2023-07-06 (https://www.snort.org/advisories/talos-rules-2023-07-06)**

The new and updated Snort rules span the following categories:

- 1 file-identify rules with SID 62002
- 5 server-webapp rules with SIDs 300596, 300597, 61997, 300605, 300606