Release Notes for Cisco Cyber Vision Knowledge DB

Release 202404

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-4.3.3.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.3.3.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.3.3.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.3.3.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.3.3.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.3.3.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.3.3.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.3.3.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.3.3.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.3.3.dat	Knowledge DB embedded in Cisco Cyber Vision 4.3.3
Updates/KDB/KDB.202404	**Description**
CiscoCyberVision_knowledgedb_20240405.db	Knowledge DB version 20240405
CiscoCyberVision_knowledgedb_20240412.db	Knowledge DB version 20240412
CiscoCyberVision_knowledgedb_20240419.db	Knowledge DB version 20240419
CiscoCyberVision_knowledgedb_20240426.db	Knowledge DB version 20240426

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

20240426

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

- **Talos Rules 2024-04-24 (https://www.snort.org/advisories/talos-rules-2024-04-24)**
- **Talos Rules 2024-04-23 (https://www.snort.org/advisories/talos-rules-2024-04-23)**

The new and updated Snort rules span the following categories:

- 2 browser-chrome rules with SIDs 300892, 63327
- 4 os-windows rules with SIDs 63324, 63330, 63329, 63328
- 1 protocol-ftp rules with SID 63326
- 1 server-samba rules with SID 43053
- 6 server-webapp rules with SIDs 63320, 63323, 63319, 63321, 63325, 63322

20240419

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

- **Talos Rules 2024-04-18 (https://www.snort.org/advisories/talos-rules-2024-04-18)**
- **Talos Rules 2024-04-16 (https(://www.snort.org/advisories/talos-rules-2024-04-16-4-17-2024)**
- **Talos Rules 2024-04-16 (https://www.snort.org/advisories/talos-rules-2024-04-16)**
- **Talos Rules 2024-04-12 (https://www.snort.org/advisories/talos-rules-2024-04-12)**

The new and updated Snort rules span the following categories:

- 7 malware-other rules with SIDs 300882, 300884, 300885, 300886, 300875, 300876, 300883
- 8 os-windows rules with SIDs 300880, 300878, 300881, 300874, 300873, 63265, 300879, 300877
- 4 pua-other rules with SIDs 57633, 57634, 57632, 57631
- 3 server-oracle rules with SIDs 13618, 13617, 13719
- 4 server-webapp rules with SIDs 63253, 63262, 300887, 63289

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

- CVE-2024-3493: (Improper Input Validation Vulnerability in Rockwell ControlLogix and GuardLogix)
  - A specific malformed fragmented packet type (fragmented packets may be generated automatically by devices that send large amounts of data) can cause a major nonrecoverable fault (MNRF). If exploited, the affected product will become unavailable and require a manual restart to recover it. Additionally, an MNRF could result in a loss of view and/or control of connected devices.

20240412

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

- **Talos Rules 2024-04-11 (https://www.snort.org/advisories/talos-rules-2024-04-11)**
- **Talos Rules 2024-04-09 (https://www.snort.org/advisories/talos-rules-2024-04-09)**

The new and updated Snort rules span the following categories:

- 7 malware-other rules with SIDs 300882, 300884, 300885, 300886, 300875, 300876, 300883
- 8 os-windows rules with SIDs 300880, 300878, 300881, 300874, 300873, 63265, 300879, 300877
- 4 pua-other rules with SIDs 57633, 57634, 57632, 57631
- 3 server-oracle rules with SIDs 13618, 13617, 13719
- 4 server-webapp rules with SIDs 63253, 63262, 300887, 63289

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

- CVE-2024-2427: (Uncontrolled Resource Consumption Vulnerability in Rockwell PowerFlex 527)
  - A denial-of-service vulnerability exists in the PowerFlex® 527 due to improper traffic throttling in the device. If multiple data packets are sent to the device repeatedly the device will crash and require a manual restart to recover.
- CVE-2024-2426: (Improper Input Validation Vulnerability in Rockwell PowerFlex 527)
  - A denial-of-service vulnerability exists in the PowerFlex® 527 due to improper input validation in the device. If exploited, a disruption in the CIP communication will occur and a manual restart will be required by the user to recover it.
- CVE-2024-2425: (Improper Input Validation Vulnerability in Rockwell PowerFlex 527)
  - A denial-of-service vulnerability exists in the PowerFlex 527 due to improper input validation in the device. If exploited, the web server will crash and need a manual restart to recover it.

20240405

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

- **Talos Rules 2024-04-04 (https://www.snort.org/advisories/talos-rules-2024-04-04)**
- **Talos Rules 2024-04-02 (https://www.snort.org/advisories/talos-rules-2024-04-02)**

The new and updated Snort rules span the following categories:

- 3 malware-cnc rules with SIDs 63242, 63241, 63240
- 3 server-webapp rules with SIDs 300871, 62342, 300872