Release Notes for Cisco Cyber Vision Knowledge DB

Release 202401

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-4.3.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.3.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.3.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.3.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.3.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.3.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.3.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.3.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.3.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.3.0.dat	Knowledge DB embedded in Cisco Cyber Vision 4.3.0
Updates/KDB/KDB.202401	**Description**
CiscoCyberVision_knowledgedb_20240112.db	Knowledge DB version 20240112
CiscoCyberVision_knowledgedb_20240119.db	Knowledge DB version 20240119
CiscoCyberVision_knowledgedb_20240126.db	Knowledge DB version 20240126

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

20240126

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

- **Talos Rules 2024-01-25 (https://www.snort.org/advisories/talos-rules-2024-01-25)**
- **Talos Rules 2024-01-23 (https://www.snort.org/advisories/talos-rules-2024-01-23)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SIDs 300809
- 3 malware-other rules with SIDs 300811, 300813, 300810
- 7 server-webapp rules with SIDs 300812, 62930, 62924, 62920, 62921, 62919, 62918

20240119

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

- **Talos Rules 2024-01-18 (https://www.snort.org/advisories/talos-rules-2024-01-18)**
- **Talos Rules 2024-01-16 (https://www.snort.org/advisories/talos-rules-2024-01-16)**

The new and updated Snort rules span the following categories:

- 2 file-office rules with SIDs 300807, 300808
- 3 malware-cnc rules with SIDs 62911, 62905, 62906
- 10 os-windows rules with SIDs 62904, 62897, 62900, 62899, 300806, 61707, 62903, 62898, 62901, 62902
- 12 server-webapp rules with SIDs 62113, 62114, 62886, 62895, 62896, 300805, 300804, 62894, 62893, 62888, 62892, 62889

20240112

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

- **Talos Rules 2024-01-11 (https://www.snort.org/advisories/talos-rules-2024-01-11)**
- **Talos Rules 2024-01-09 (https://www.snort.org/advisories/talos-rules-2024-01-09)**
- **Talos Rules 2024-01-04 (https://www.snort.org/advisories/talos-rules-2024-01-04)**
- **Talos Rules 2023-12-28 (https://www.snort.org/advisories/talos-rules-2023-12-28)**

The new and updated Snort rules span the following categories:

- 2 malware-cnc rules with SIDs 62817, 47235
- 2 malware-other rules with SIDs 300790, 300791
- 6 os-windows rules with SIDs 300802, 300797, 300799, 300798, 300800, 300801

- 2 policy-other rules with SIDs 300796, 300795
- 20 server-webapp rules with SIDs 62872, 300794, 62836, 62834, 300803, 62835, 62869, 62844, 62845, 300792, 62811, 300789, 62829, 62846, 62822, 62823, 62828, 62812, 300793, 62851

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

- CVE-2023-49621: (Use of Default Credentials Vulnerability in Siemens SIMATIC CN 4100)
  - The "intermediate installation" system state of the affected application uses default credential with admin privileges. An attacker could use the credentials to gain complete control of the affected device.
- CVE-2023-49252: (Improper Input Validation Vulnerability in Siemens SIMATIC CN 4100)
  - The affected application allows IP configuration change without authentication to the device. This could allow an attacker to cause denial of service condition.
- CVE-2023-49251: (Authorization Bypass Through User-Controlled Key Vulnerability in Siemens SIMATIC CN 4100)
  - The "intermediate installation" system state of the affected application allows an attacker to add their own login credentials to the device. This allows an attacker to remotely login as root and take control of the device even after the affected device is fully set up.
- CVE-2023-42797: (Command Injection Vulnerability in the CPCI85 Firmware of Siemens SICAM A8000 Devices)
  - The network configuration service of affected devices contains a flaw in the conversion of ipv4 addresses that could lead to an uninitialized variable being used in succeeding validation steps. By uploading specially crafted network configuration, an authenticated remote attacker could be able to inject commands that are executed on the device with root privileges during device startup.