Release Notes for Cisco Cyber Vision Knowledge DB

Release 202405

Compatible device list *2*

Links *2*

Software Download 2

Related Documentation 2

Database download *3*

How to update the database *3*

Release contents *4*

20240517 4

20240503 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-4.3.3.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.202405	**Description**
CiscoCyberVision_knowledgedb_20240503.db	Knowledge DB version 20240503
CiscoCyberVision_knowledgedb_20240517.db	Knowledge DB version 20240517

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

20240517

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

- **Talos Rules 2024-05-16 (https://www.snort.org/advisories/talos-rules-2024-05-16)**
- **Talos Rules 2024-05-14 (https://www.snort.org/advisories/talos-rules-2024-05-14)**
- **Talos Rules 2024-05-09 (https://www.snort.org/advisories/talos-rules-2024-05-09)**
- **Talos Rules 2024-05-07 (https://www.snort.org/advisories/talos-rules-2024-05-07)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 63398
- 1 file-executable rule with SID 300910
- 1 file-image rule with SID 300914
- 3 file-other rules with SIDs 32904, 300902, 32903
- 1 malware-cnc rule with SID 300901
- 1 netbios rule with SID 63396
- 16 os-windows rules with SIDs 63393, 300911, 300912, 300906, 43175, 63394, 63329, 300907, 63265, 43176, 63392, 63391, 300909, 63328, 300908, 63340
- 2 policy-other rules with SIDs 300903, 63433
- 1 protocol-dns rule with SID 59579
- 1 protocol-other rule with SID 63397
- 2 protocol-voip rules with SIDs 51086, 51087
- 4 server-other rules with SIDs 63407, 63447, 63388, 63389
- 4 server-samba rules with SIDs 33826, 63395, 63440, 63421
- 46 server-webapp rules with SIDs 63436, 63456, 63457, 63402, 63399, 300905, 63387, 300904, 63439, 63409, 63424, 63374, 63438, 63446, 63379, 63410, 63382, 63343, 62285, 63418, 63437, 63380, 63381, 63449, 63344, 63373, 63386, 63416, 63376, 63452, 63454, 63453, 63448, 63400, 63375, 63383, 63455, 63384, 63415, 63445, 62649, 63417, 63401, 63385, 63408, 58339

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

- CVE-2024-3576: (Cross-site Scripting Vulnerability in Moxa NPort 5100A Series)
  - The NPort 5100A Series firmware version v1.6 and prior versions are affected by web server vulnerability. The vulnerability is caused by not correctly neutralizing user-controllable input before

placing it in output. Malicious users may use the vulnerability to get sensitive information and escalate privileges.

- CVE-2024-28133: (Untrusted Search Path Vulnerability in Phoenix Contact CHARX-SEC3xxx Charge controllers)
    - A local low privileged attacker can use an untrusted search path in a CHARX system utility to gain root privileges.
- CVE-2024-28134: (Cleartext Transmission of Sensitive Information Vulnerability in Phoenix Contact CHARX-SEC3xxx Charge controllers)
    - An unauthenticated remote attacker can extract a session token with a MitM attack and gain web-based management access with the privileges of the currently logged in user due to cleartext transmission of sensitive information. No additional user interaction is required. The access is limited as only non-sensitive information can be obtained but the availability can be seriously affected.
- CVE-2024-28135: (Improper Input Validation Vulnerability in Phoenix Contact CHARX-SEC3xxx Charge controllers)
    - The exploit allows a user of the web-based management to perform remote code execution on the device as a user with low privileges.
- CVE-2024-28136: (Improper Input Validation Vulnerability in Phoenix Contact CHARX-SEC3xxx Charge controllers)
    - When the OCPP management port is opened, the exploit allows an attacker without local account to gain root privileges and perform remote code execution.
- CVE-2024-28137: (Race Condition Vulnerability in Phoenix Contact CHARX-SEC3xxx Charge controllers)
    - The exploit allows a local user to gain root privileges, which allows them to take over the device.

20240503

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

- **Talos Rules 2024-05-02 (https://www.snort.org/advisories/talos-rules-2024-05-02)**
- **Talos Rules 2024-04-30 (https://www.snort.org/advisories/talos-rules-2024-04-30)**

The new and updated Snort rules span the following categories:

- 1 browser-ie rule with SID 35053
- 1 file-office rule with SID 300894
- 2 malware-cnc rules with SIDs 63368, 63345
- 4 malware-other rules with SIDs 300898, 300900, 300899, 300897
- 3 os-windows rules with SIDs 63351, 63340, 63346
- 3 policy-other rules with SIDs 63355, 59657, 63354

- 2 server-other rules with SIDs 63331, 300896
- 1 server-samba rule with SID 63349
- 14 server-webapp rules with SIDs 63343, 63334, 62851, 63359, 63337, 63344, 63335, 300895, 35668, 63338, 63339, 63336, 63333, 63332