



Release Notes for Cisco Cyber Vision Knowledge DB

Release 202410

<i>Compatible device list</i>	2
<i>Links</i>	2
Software Download	2
Related Documentation	2
<i>Database download</i>	3
<i>How to update the database</i>	3
<i>Release contents</i>	4
20241004.....	4

Compatible device list

Center	Description
All version 4 and 5 centers	All Cisco Cyber Vision center version 4 and 5 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-5.0.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.0.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.0.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.0.1.ext	Sensor Management extension installation file
Sensor	Description
CiscoCyberVision-IOx-aarch64-5.0.1.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.0.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.0.1.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.0.1.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.0.1.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	Description
CiscoCyberVision-Embedded-KDB-5.0.1.dat	Knowledge DB embedded in Cisco Cyber Vision 5.0.1
Updates/KDB/KDB.202410	Description
CiscoCyberVision_knowledgedb_20241004.db	Knowledge DB version 20241004

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

20241004

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

- **Talos Rules 2024-10-03** (<https://www.snort.org/advisories/talos-rules-2024-10-03>)
- **Talos Rules 2024-10-01** (<https://www.snort.org/advisories/talos-rules-2024-10-01>)

The new and updated Snort rules span the following categories:

- 6 file-pdf rules with SIDs 64067, 64068, 64066, 64063, 64064, 64065
- 3 malware-cnc rules with SIDs 64056, 64054, 64072
- 8 malware-other rules with SIDs 301030, 64074, 301029, 301031, 64073, 64075, 64076, 301032
- 1 os-windows rules with SIDs 301033
- 5 server-webapp rules with SIDs 64071, 64078, 64055, 64079, 64077