Release Notes for Cisco Cyber Vision Knowledge DB

Release 202611

Compatible device list ***2***

Links ***2***

Software Download **2**

Related Documentation **3**

Database download ***3***

How to update the database ***3***

Release contents ***4***

20261106 ..... **4**

Snort rules 4

Vulnerabilities 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-5.6.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.6.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.6.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.6.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.6.1.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.6.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.6.1.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.6.1.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.6.1.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.6.1.dat	Knowledge DB embedded in Cisco Cyber Vision 5.6.1
Updates/KDB/KDB.202611	**Description**
CiscoCyberVision_knowledgedb_20261106.db	Knowledge DB version 20261106

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

20261106

Snort rules

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

- **Talos Rules 2026-11-05 (https://www.snort.org/advisories/talos-rules-2026-11-05)**
- **Talos Rules 2026-11-03 (https://www.snort.org/advisories/talos-rules-2026-11-03)**

The new and updated Snort rules span the following categories:

- 4 server-other rules with SIDs 67434, 67152, 67435, 67433
- 13 server-webapp rules with SIDs 301728, 67420, 67421, 67438, 301727, 67427, 67436, 67428, 67424, 67425, 67423, 67437, 67426

Vulnerabilities

This release adds support for the detection of the following vulnerabilities:

Schweitzer Engineering Laboratories

- PVT-2026-00010: Improper Input Validation Vulnerability in Precision Time Protocol (PTP) Handling on Schweitzer Engineering Laboratories SEL-2488 Satellite-Synchronized Network Clock
  - In SEL-2488 Satellite-Synchronized Network Clock firmware revision R112-V0, specifically formatted Ethernet packets from an unauthenticated external device could cause the Precision Time Protocol (PTP) functionality of the receiving port to momentarily reset. SEL resolved the issue in firmware revision R112-V1.