Release Notes for Cisco Cyber Vision Knowledge DB

Release 202407

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-4.4.2.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.4.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.4.2.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.4.2.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.4.2.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.4.2.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.4.2.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.4.2.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.4.2.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.4.2.dat	Knowledge DB embedded in Cisco Cyber Vision 4.4.2
Updates/KDB/KDB.202407	**Description**
CiscoCyberVision_knowledgedb_20240705.db	Knowledge DB version 20240705
CiscoCyberVision_knowledgedb_20240712.db	Knowledge DB version 20240712

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

20240712

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

- **Talos Rules 2024-07-11 (https://www.snort.org/advisories/talos-rules-2024-07-11)**
- **Talos Rules 2024-07-09 (https://www.snort.org/advisories/talos-rules-2024-07-09)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 300257
- 1 browser-ie rul with SIDs 47102
- 2 file-office rules with SIDs 63694, 63693
- 6 malware-cnc rules with SIDs 63710, 300964, 63709, 63686, 63711, 63712
- 5 malware-other rules with SIDs 300963, 300962, 63713, 63714, 63715
- 4 os-windows rules with SIDs 300960, 300958, 300961, 300959
- 1 protocol-dns rule with SID 63701
- 1 protocol-other rule with SID 53214
- 2 server-webapp rules with SIDs 63720, 63704

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

- CVE-2024-38867: (Inadequate Encryption Strength Vulnerability in Siemens SIPROTEC 5 Devices)
  - The SIPROTEC 5 devices are supporting weak encryption. This could allow an unauthorized attacker in a man-in-the-middle position to read any data passed over the connection between legitimate clients and the affected device.
- CVE-2024-38867: (Cross-Site Scripting Vulnerability in Schneider Modicon Controllers M241/ M251, M258 / LMC058 and M262)
  - A Cross-Site Scripting vulnerability exists that could cause a vulnerability leading to a cross-site scripting condition where attackers can have a victim's browser run arbitrary JavaScript when they visit a page containing the injected payload.

20240705

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

- **Talos Rules 2024-07-03 (https://www.snort.org/advisories/talos-rules-2024-07-03)**
- **Talos Rules 2024-06-27 (https://www.snort.org/advisories/talos-rules-2024-06-27)**

The new and updated Snort rules span the following categories:

- 1 file-executable rule with SID 300950
- 3 file-other rules with SIDs 300955, 300957, 300956
- 1 malware-cnc rule with SID 63669
- 3 malware-other rules with SIDs 300952, 300954, 300953
- 2 policy-other rules with SIDs 63666, 63679
- 1 protocol-rpc rule with SID 63678
- 2 server-other rules with SIDs 33654, 63659
- 22 server-webapp rules with SIDs 63652, 63645, 63676, 63637, 63639, 63649, 63644, 63643, 63641, 63677, 63640, 63651, 300949, 63642, 63638, 300948, 38511, 300951, 63635, 63636, 63646, 63650