Release Notes for Cisco Cyber Vision Knowledge DB

Release 202504

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-5.1.3.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.1.3.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.1.3.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.1.3.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.1.3.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.1.3.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.1.3.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.1.3.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.1.3.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.1.3.dat	Knowledge DB embedded in Cisco Cyber Vision 5.1.3
Updates/KDB/KDB.202504	**Description**
CiscoCyberVision_knowledgedb_20250404.db	Knowledge DB version 20250404
CiscoCyberVision_knowledgedb_20250411.db	Knowledge DB version 20250411
CiscoCyberVision_knowledgedb_20250418.db	Knowledge DB version 20250418
CiscoCyberVision_knowledgedb_20250425.db	Knowledge DB version 20250425

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

20250425

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

- **Talos Rules 2025-04-24 (https://www.snort.org/advisories/talos-rules-2025-04-24)**
- **Talos Rules 2025-04-22 (https://www.snort.org/advisories/talos-rules-2025-04-22)**

The new and updated Snort rules span the following categories:

- 1 app-detect rule with SID 64789
- 2 file-multimedia rules with SIDs 64805, 64804
- 2 file-other rules with SIDs 64807, 64806
- 2 file-pdf rules with SIDs 64803, 64802
- 1 indicator-compromise rule with SID 301186
- 6 malware-cnc rules with SIDs 64797, 64800, 64799, 64801, 64798, 301185
- 3 malware-other rules with SIDs 301187, 64812, 64796
- 1 policy-other rule with SID 64790
- 2 server-other rules with SIDs 64788, 64795
- 6 server-webapp rules with SIDs 58450, 58449, 64792, 300362, 64791, 61069

20250418

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

- **Talos Rules 2025-04-17 (https://www.snort.org/advisories/talos-rules-2025-04-17)**
- **Talos Rules 2025-04-15 (https://www.snort.org/advisories/talos-rules-2025-04-15)**
- **Talos Rules 2025-04-10 (https://www.snort.org/advisories/talos-rules-2025-04-10)**

The new and updated Snort rules span the following categories:

- 2 browser-chrome rules with SIDs 52401, 52400
- 1 exploit-kit rule with SID 26292
- 2 file-other rules with SIDs 64771, 64772
- 2 file-pdf rules with SIDs 64785, 64784
- 3 malware-other rules with SIDs 301182, 301181, 301184
- 2 os-windows rules with SIDs 301183, 301180
- 1 policy-other rule with SID 64778

- 3 server-other rules with SIDs 64766, 64768, 64767
- 1 server-samba rule with SID 64779
- 9 server-webapp rules with SIDs 64773, 64774, 64503, 300628, 64765, 300627, 64786, 64787, 64777

20250411

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

- **Talos Rules 2025-04-08 (https://www.snort.org/advisories/talos-rules-2025-04-08)**

The new and updated Snort rules span the following categories:

- 9 os-windows rules with SIDs 64747, 64748, 64762, 301178, 64432, 301179, 64746, 301176, 301177
- 9 server-webapp rules with SIDs 58317, 64760, 58316, 64757, 51453, 64241, 64758, 64761, 64488

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

- CVE-2024-23814: (Uncontrolled Resource Consumption Vulnerability in multiple Siemens Industrial Devices)
  - The integrated ICMP service of the network stack of affected devices can be forced to exhaust its available memory resources when receiving specially crafted messages targeting IP fragment re-assembly. This could allow an unauthenticated remote attacker to cause a temporary denial of service condition of the ICMP service, other communication services are not affected. Affected devices will resume normal operation after the attack terminates.

20250404

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

- **Talos Rules 2025-04-03 (https://www.snort.org/advisories/talos-rules-2025-04-03)**
- **Talos Rules 2025-04-01 (https://www.snort.org/advisories/talos-rules-2025-04-01)**

The new and updated Snort rules span the following categories:

- 8 malware-cnc rules with SIDs 48153, 48151, 48157, 48154, 48152, 64741, 48155, 48156
- 4 malware-other rules with SIDs 301175, 64725, 301173, 301174
- 2 os-other rules with SIDs 64737, 64738
- 1 policy-other rule with SID 64733
- 3 protocol-other rules with SIDs 64728, 64729, 64727
- 1 server-apache rule with SID 64730
- 1 server-other rule with SID 50908

- 10 server-webapp rules with SIDs 64722, 64726, 64724, 64736, 64723, 64735, 64721, 64732, 64734, 64731