Release Notes for Cisco Cyber Vision Knowledge DB

Release 202602

Compatible device list 2

Links 2

Software Download 2

Related Documentation 3

Database download 3

How to update the database 3

Release contents 4

20260227 4

Snort rules 4

Vendor Database 4

20260220 4

Snort rules 4

Vulnerabilities 5

Vendor Database 5

20260213 5

Snort rules 5

Vulnerabilities 6

20260206 6

Snort rules 6

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-5.3.3.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.3.3.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.3.3.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.3.3.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.3.3.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.3.3.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.3.3.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.3.3.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.3.3.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.3.3.dat	Knowledge DB embedded in Cisco Cyber Vision 5.3.3
Updates/KDB/KDB.202602	**Description**
CiscoCyberVision_knowledgedb_20260206.db	Knowledge DB version 20260206
CiscoCyberVision_knowledgedb_20260213.db	Knowledge DB version 20260213
CiscoCyberVision_knowledgedb_20260220.db	Knowledge DB version 20260220
CiscoCyberVision_knowledgedb_20260227.db	Knowledge DB version 20260227

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

20260227

Snort rules

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

- **Talos Rules 2026-02-26 (https://www.snort.org/advisories/talos-rules-2026-02-26)**
- **Talos Rules 2026-02-24 (https://www.snort.org/advisories/talos-rules-2026-02-24-2-24-2026)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 301413
- 1 file-other rule with SID 301412
- 2 malware-cnc rules with SIDs 2, 1
- 1 malware-other rule with SID 301410
- 2 os-windows rules with SIDs 23837, 23838
- 7 policy-other rules with SIDs 61703, 61702, 65965, 65966, 65968, 65964, 65967
- 4 server-other rules with SIDs 65991, 65992, 65938, 65958
- 21 server-webapp rules with SIDs 65993, 65994, 65976, 301411, 65974, 65995, 24339, 65986, 65982, 65981, 65975, 65983, 65996, 65978, 65973, 65977, 65969, 65970, 65963, 65971, 65972

Vendor Database

The new UI in Cyber Vision relies on a vendor database included in this Knowledge Base to represent physical assets and give them a type. This release improves support for assets from Siemens.

20260220

Snort rules

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

- **Talos Rules 2026-02-19 (https://www.snort.org/advisories/talos-rules-2026-02-19)**
- **Talos Rules 2026-02-17 (https://www.snort.org/advisories/talos-rules-2026-02-17)**

The new and updated Snort rules span the following categories:

- 1 file-office rule with SID 301102
- 2 file-pdf rules with SIDs 65361, 65362

- 1 malware-cnc rule with SID 65949
- 3 malware-other rules with SIDs 301405, 301406, 301407
- 2 policy-other rules with SIDs 65494, 65962
- 2 server-other rules with SIDs 65938, 65958
- 13 server-webapp rules with SIDs 65961, 65959, 65943, 65952, 65944, 65941, 65940, 301408, 301409, 65955, 65939, 65942, 65960

Vulnerabilities

Vulnerability matching based on SMBv1 has been removed from Cyber Vision due to inconsistencies and inaccurate detection results. As a result, assets or devices that were previously assigned vulnerabilities solely based on SMBv1 identification may now show a reduced vulnerability count.

Vendor Database

The new UI in Cyber Vision relies on a vendor database included in this Knowledge Base to represent physical assets and give them a type. This release adds initial typing support for assets from Wago. It also improves support for assets from ABB, Keyence, Mitsubishi, Palo Alto, Prosoft, Rockwell, Siemens, Turck.

20260213

Snort rules

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

- **Talos Rules 2026-02-12 (https://www.snort.org/advisories/talos-rules-2026-02-12)**
- **Talos Rules 2026-02-10 (https://www.snort.org/advisories/talos-rules-2026-02-10)**

The new and updated Snort rules span the following categories:

- 1 browser-other rule with SID 65929
- 11 file-flash rules with SIDs 48494, 48491, 48496, 48493, 48567, 48492, 50537, 50535, 50534, 50536, 48495
- 1 file-office rule with SID 301402
- 1 file-other rule with SID 301394
- 1 file-pdf rule with SID 50862
- 8 malware-cnc rules with SIDs 65919, 65918, 65922, 65917, 65920, 65921, 65915, 65916

- 9 os-windows rules with SIDs 301404, 301398, 301397, 301395, 301400, 301401, 301396, 301403, 301399
- 1 policy-other rule with SID 64374
- 2 server-other rules with SIDs 25550, 25549
- 24 server-webapp rules with SIDs 301340, 65933, 65544, 65932, 65930, 65625, 65912, 65928, 65901, 59017, 65925, 65927, 65904, 65934, 65926, 65931, 59016, 65935, 65905, 65888, 65889, 65891, 65892, 65890

Vulnerabilities

This release adds support for the detection of vulnerabilities on Festo and Inductive Automation products:

- CVE-2024-12297: Frontend Authorization Logic Disclosure Vulnerability in Moxa Ethernet Switches
    - Moxa's Ethernet switch is vulnerable to an authentication bypass because of flaws in its authorization mechanism. Although both client-side and back-end server verification are involved in the process, attackers can exploit weaknesses in its implementation. These vulnerabilities may enable brute-force attacks to guess valid credentials or MD5 collision attacks to forge authentication hashes, potentially compromising the security of the device.

20260206

Snort rules

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

- **Talos Rules 2026-02-05 (https://www.snort.org/advisories/talos-rules-2026-02-05)**
- **Talos Rules 2026-02-03 (https://www.snort.org/advisories/talos-rules-2026-02-03)**

The new and updated Snort rules span the following categories:

- 1 file-pdf rule with SID 301393
- 7 malware-cnc rules with SIDs 65838, 65835, 65836, 65837, 65834, 65883, 65859
- 5 malware-other rules with SIDs 301388, 301389, 301390, 301391, 301392
- 2 os-windows rules with SIDs 65872, 65868
- 3 policy-other rules with SIDs 65876, 65875, 65874
- 2 protocol-snmp rules with SIDs 65881, 1412
- 5 server-other rules with SIDs 65425, 65849, 65426, 65424, 65870
- 30 server-webapp rules with SIDs 65873, 65871, 65864, 65844, 65832, 65833, 65867, 65865, 65845, 65866, 65869, 65831, 65884, 65878, 65846, 65843, 65863, 65847, 65886, 65850, 65861, 65887, 65885, 65860, 65862, 65882, 65877, 65848, 65851, 65858