Release Notes for Cisco Cyber Vision Knowledge DB

Release 202607

Compatible device list *2*

Links *2*

Software Download **2**

Related Documentation **3**

Database download *3*

How to update the database *3*

Release contents *4*

20260731 ..... **4**

Snort rules 4

20260724 ..... **4**

Snort rules 4

20260717 ..... **4**

Snort rules 5

Vulnerabilities 5

20260710 ..... **6**

Snort rules 7

20260703 ..... **7**

Snort rules 7

Vendor Database 7

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-5.5.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.5.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.5.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.5.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.5.1.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.5.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.5.1.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.5.1.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.5.1.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.5.1.dat	Knowledge DB embedded in Cisco Cyber Vision 5.5.1
Updates/KDB/KDB.202607	**Description**
CiscoCyberVision_knowledgedb_20260703.db	Knowledge DB version 20260703
CiscoCyberVision_knowledgedb_20260710.db	Knowledge DB version 20260710
CiscoCyberVision_knowledgedb_20260717.db	Knowledge DB version 20260717
CiscoCyberVision_knowledgedb_20260724.db	Knowledge DB version 20260724
CiscoCyberVision_knowledgedb_20260731.db	Knowledge DB version 20260731

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

20260731

Snort rules

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

- **Talos Rules 2026-07-30 (https://www.snort.org/advisories/talos-rules-2026-07-30)**
- **Talos Rules 2026-07-28 (https://www.snort.org/advisories/talos-rules-2026-07-28)**

The new and updated Snort rules span the following categories:

- 1 browser-webkit rule with SID 66868
- 3 indicator-compromise rules with SIDs 66856, 66854, 66878
- 4 malware-cnc rules with SIDs 66880, 66881, 66872, 66882
- 2 server-other rules with SIDs 66870, 66871
- 21 server-webapp rules with SIDs 66879, 66853, 66855, 66857, 66863, 66864, 66862, 66867, 66859, 66865, 66858, 66861, 66869, 66873, 66866, 66860, 66883, 66877, 66876, 66874, 66875

20260724

Snort rules

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

- **Talos Rules 2026-07-23 (https://www.snort.org/advisories/talos-rules-2026-07-23)**
- **Talos Rules 2026-07-21 (https://www.snort.org/advisories/talos-rules-2026-07-21)**

The new and updated Snort rules span the following categories:

- 2 file-multimedia rules with SIDs 66843, 66842
- 2 file-other rules with SIDs 66852, 66851
- 4 malware-cnc rules with SIDs 66839, 301587, 27, 26
- 1 policy-other rule with SID 66850
- 2 server-other rules with SIDs 66827, 66107
- 22 server-webapp rules with SIDs 66835, 66823, 66836, 66837, 66838, 66834, 66844, 66821, 66847, 66828, 66849, 66833, 66831, 66822, 66848, 66832, 66820, 66846, 66845, 66829, 66819, 66830

20260717

Snort rules

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

- **Talos Rules 2026-07-16 (https://www.snort.org/advisories/talos-rules-2026-07-16)**
- **Talos Rules 2026-07-14 (https://www.snort.org/advisories/talos-rules-2026-07-14)**

The new and updated Snort rules span the following categories:

- 6 file-multimedia rules with SIDs 66794, 66795, 66797, 66796, 66798, 66799
- 2 malware-cnc rules with SIDs 66787, 66788
- 1 malware-other rule with SID 301580
- 34 os-windows rules with SIDs 301582, 301557, 301558, 301577, 301568, 301581, 301566, 301567, 301583, 66793, 301561, 301572, 301563, 66745, 301586, 301584, 301559, 66786, 301579, 301565, 301562, 301574, 301564, 301556, 301571, 66807, 301560, 301576, 301570, 301573, 301575, 301569, 301585, 301555
- 3 policy-other rules with SIDs 66802, 66791, 66792
- 1 server-other rule with SID 66733
- 11 server-webapp rules with SIDs 66816, 66813, 66814, 66808, 301578, 66815, 66744, 301554, 66728, 66732, 66729

Vulnerabilities

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

- CVE-2025-11694: Improper Validation of Integrity Check Value Vulnerability in Rockwell Automation CompactLogix 5370 Controllers
  - A denial-of-service vulnerability exists in 1769 CompactLogix 5370 controllers due to missing validation of CIP sequence numbers and source IP addresses. Exposed Connection IDs visible on the web interface can be abused to cause a minor fault.
- CVE-2025-12011: Buffer Overflow Vulnerability in Rockwell Automation CompactLogix 5370 and ControlLogix 5570 Controllers
  - A denial-of-service vulnerability exists in CompactLogix 5370, Compact GuardLogix 5370, ControlLogix 5570, and GuardLogix 5570 controllers. A remote attacker could load an invalid project and cause a major non-recoverable fault.
- CVE-2025-12012: Buffer Overflow Vulnerability in Rockwell Automation CompactLogix 5380 and ControlLogix 5580 Controllers
  - A denial-of-service vulnerability exists in CompactLogix 5380, Compact GuardLogix 5380, CompactLogix 5480, ControlLogix 5580, and GuardLogix 5580 controllers. A malicious user could write invalid file data to the controller and cause a major non-recoverable fault.

- CVE-2025-11698: Buffer Overflow Vulnerability in Rockwell Automation 5380, 5480, and 5580 Recovery Image Boot Firmware
    - A denial-of-service vulnerability exists in the recovery-image boot firmware for CompactLogix 5380, Compact GuardLogix 5380, CompactLogix 5480, ControlLogix 5580, and GuardLogix 5580 controllers. A malicious user could write invalid file data to the controller and cause a major non-recoverable fault.
- CVE-2026-9653: Denial-of-Service Vulnerability in Rockwell Automation 1756-EN2, 1756-EN3, and 1756-ENBT Modules
    - A denial-of-service vulnerability exists in 1756-EN2, 1756-EN3, and 1756-ENBT communication modules due to improper validation of CIP implicit connection packets. Crafted packets can continuously disrupt device connections.
- CVE-2026-10573: Denial-of-Service Vulnerability in Rockwell Automation 1734 POINT I/O Modules
    - A denial-of-service vulnerability exists in the 1734-OB8 POINT I/O module. Crafted CIP messages can cause the module to enter a faulted state requiring a restart.
- CVE-2026-9140: Denial-of-Service Vulnerability in Rockwell Automation 1718-AENTR and 1719-AENTR Adapters
    - A denial-of-service vulnerability exists in 1718-AENTR and 1719-AENTR EtherNet/IP adapters. A UDP unicast network storm can overload the device and cause loss of communication until power cycle.
- CVE-2026-10577: Missing Authentication Vulnerability in Rockwell Automation 1715 Redundant I/O
    - A missing-authentication vulnerability exists in the 1715-AENTR EtherNet/IP adapter. An unauthenticated remote attacker can access intrusive command-line functions that may affect confidentiality, integrity, and availability.
- CVE-2026-9636: Improper Certificate Revocation Check Vulnerability in Rockwell Automation CompactLogix 5380 and ControlLogix 5580
    - A certificate revocation handling vulnerability exists in CompactLogix 5380, Compact GuardLogix 5380, ControlLogix 5580, GuardLogix 5580, and 1756-EN4TR communication modules. A network attacker could establish a connection with a certificate that should be untrusted when CRL features and intermediary certificates are used.
- CVE-2026-12659: Denial-of-Service Vulnerability in Rockwell Automation FLEX 5000 Adapters
    - A denial-of-service vulnerability exists in FLEX 5000 EtherNet/IP adapters. Crafted CIP packets can trigger improper exceptional condition handling; a power cycle is required to recover the module and associated I/O.

20260710

Snort rules

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

- **Talos Rules 2026-07-09 (https://www.snort.org/advisories/talos-rules-2026-07-09)**
- **Talos Rules 2026-07-07 (https://www.snort.org/advisories/talos-rules-2026-07-07)**

The new and updated Snort rules span the following categories:

- 2 file-multimedia rules with SIDs 66721, 66722
- 2 file-pdf rules with SIDs 66712, 66713
- 2 os-other rules with SIDs 64087, 64088
- 2 os-windows rules with SIDs 66716, 59052
- 1 policy-other rule with SID 66720
- 6 server-other rules with SIDs 66711, 66718, 66717, 66715, 66719, 301552
- 3 server-webapp rules with SIDs 66714, 66725, 301553

20260703

Snort rules

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

- **Talos Rules 2026-07-02 (https://www.snort.org/advisories/talos-rules-2026-07-02)**
- **Talos Rules 2026-06-30 (https://www.snort.org/advisories/talos-rules-2026-06-30)**

The new and updated Snort rules span the following categories:

- 3 file-other rules with SIDs 301545, 66710, 66709
- 1 malware-cnc rule with SID 66690
- 2 malware-other rules with SIDs 66697, 66696
- 1 os-linux rule with SID 301546
- 8 server-other rules with SIDs 66708, 66693, 66682, 66683, 66692, 66687, 66695, 66694
- 14 server-webapp rules with SIDs 66691, 66703, 66702, 301551, 301549, 66705, 66704, 66686, 66700, 301550, 66701, 66707, 301547, 66706

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.