Release Notes for Cisco Cyber Vision Knowledge DB

Release 202501

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-5.0.2.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.0.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.0.2.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.0.2.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.0.2.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.0.2.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.0.2.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.0.2.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.0.2.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.0.2.dat	Knowledge DB embedded in Cisco Cyber Vision 5.0.2
Updates/KDB/KDB.202501	**Description**
CiscoCyberVision_knowledgedb_20250110.db	Knowledge DB version 20250110
CiscoCyberVision_knowledgedb_20250117.db	Knowledge DB version 20250117
CiscoCyberVision_knowledgedb_20250124.db	Knowledge DB version 20250124

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

20250124

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

- **Talos Rules 2025-01-23 (https://www.snort.org/advisories/talos-rules-2025-01-23)**
- **Talos Rules 2025-01-21 (https://www.snort.org/advisories/talos-rules-2025-01-21)**
- **Talos Rules 2025-01-16 (https://www.snort.org/advisories/talos-rules-2025-01-16)**

The new and updated Snort rules span the following categories:

- 6 malware-cnc rules with SIDs 64460, 64466, 64465, 64458, 64459, 64467
- 2 malware-other rules with SIDs 301124, 64469
- 1 policy-spam rule with SID 64468
- 5 server-webapp rules with SIDs 60885, 64464, 24339, 64463, 64470

20250117

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

- **Talos Rules 2025-01-14 (https://www.snort.org/advisories/talos-rules-2025-01-14)**

The new and updated Snort rules span the following categories:

- 2 file-office rules with SIDs 301117, 301114
- 2 file-other rules with SIDs 301116, 300253
- 2 malware-cnc rules with SIDs 64439, 64440
- 1 malware-other rule with SID 301115
- 8 os-windows rules with SIDs 301123, 301122, 301119, 301121, 301118, 301113, 64432, 301120
- 1 server-other rule with SID 64441
- 1 server-webapp rule with SID 62789

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

- CVE-2024-11497: (Improper File Permission Vulnerability in Phoenix Contact CHARX-SEC3xxx Charge controllers)
  - Improper file permission handling allows an authenticated low privileged user to gain root access.
- CVE-2024-12142: (Information Exposure Vulnerability in Schneider Modicon M340 and several communication modules)

    - An information exposure vulnerability exists that could cause information disclosure of restricted web page, modification of web page and denial of service when specific web pages are modified and restricted functions are invoked.
- CVE-2024-11425: (Denial of Service Vulnerability in Schneider Modicon M580 PLCs, BMENOR2200H and EVLink Pro AC)
    - A vulnerability exists that could cause Denial-of-Service of the product when an unauthenticated user is sending a crafted HTTPS packet to the webserver.
- CVE-2024-53649: (Improper Authorization Vulnerability in Siemens SIPROTEC 5)
    - Affected devices do not properly limit the path accessible via their webserver. This could allow an authenticated remote attacker to read arbitrary files from the filesystem of affected devices.
- CVE-2024-47100: (Cross-Site Request Forgery (CSRF) Vulnerability in Siemens SIMATIC S7-1200 CPUs)
    - The web interface of the affected devices is vulnerable to Cross-Site Request Forgery (CSRF) attacks. This could allow an unauthenticated attacker to change the CPU mode by tricking a legitimate and authenticated user with sufficient permissions on the target CPU to click on a malicious link.

20250110

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

- **Talos Rules 2025-01-09 (https://www.snort.org/advisories/talos-rules-2025-01-09)**
- **Talos Rules 2025-01-07 (https://www.snort.org/advisories/talos-rules-2025-01-07)**
- **Talos Rules 2025-01-02 (https://www.snort.org/advisories/talos-rules-2025-01-02)**
- **Talos Rules 2024-12-23 (https://www.snort.org/advisories/talos-rules-2024-12-23)**

The new and updated Snort rules span the following categories:

- 4 file-identify rules with SIDs 64386, 64387, 64389, 64388
- 4 file-office rules with SIDs 64430, 64409, 64431, 64408
- 8 file-other rules with SIDs 301105, 46055, 301107, 46059, 301104, 46056, 46058, 301106
- 3 malware-cnc rules with SIDs 64416, 64402, 64417
- 5 malware-other rules with SIDs 64407, 301111, 301110, 301109, 301108
- 1 os-windows rule with SID 301112
- 4 policy-other rules with SIDs 64410, 64415, 64414, 64425
- 2 protocol-imap rules with SIDs 43067, 64398
- 1 server-other rule with SID 43068
- 11 server-webapp rules with SIDs 64420, 64399, 64421, 64428, 64426, 64412, 64427, 64429, 64413, 64411, 64424