Release Notes for Cisco Cyber Vision Knowledge DB

Release 202412

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.202412	**Description**
CiscoCyberVision_knowledgedb_20241206.db	Knowledge DB version 20241206
CiscoCyberVision_knowledgedb_20241213.db	Knowledge DB version 20241213
CiscoCyberVision_knowledgedb_20241220.db	Knowledge DB version 20241220

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

20241220

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

- **Talos Rules 2024-12-19 (https://www.snort.org/advisories/talos-rules-2024-12-19)**
- **Talos Rules 2024-12-17 (https://www.snort.org/advisories/talos-rules-2024-12-17)**

The new and updated Snort rules span the following categories:

- 1 browser-webkit rule with SID 64362
- 1 file-flash rule with SID 41191
- 2 file-image rules with SIDs 64329, 64328
- 3 file-office rules with SIDs 301102, 64384, 64383
- 2 malware-cnc rules with SIDs 64373, 64372
- 5 malware-other rules with SIDs 301098, 64385, 301096, 301099, 301097
- 2 policy-other rules with SIDs 64374, 64358
- 14 server-webapp rules with SIDs 64360, 64359, 64376, 64375, 64361, 64356, 64380, 64363, 301101, 301095, 64357, 301094, 64379, 64355

20241213

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

- **Talos Rules 2024-12-12 (https://www.snort.org/advisories/talos-rules-2024-12-12)**
- **Talos Rules 2024-12-10 (https://www.snort.org/advisories/talos-rules-2024-12-10)**

The new and updated Snort rules span the following categories:

- 1 file-identify rule with SID 301083
- 4 file-image rules with SIDs 64333, 64334, 64328, 64329
- 1 indicator-obfuscation rules with SIDs 301089
- 12 malware-cnc rules with SIDs 64349, 64315, 64340, 64345, 64341, 64344, 64342, 64347, 64348, 64316, 64346, 64343
- 5 malware-other rules with SIDs 301091, 301090, 301093, 301088, 301092
- 2 os-other rules with SIDs 64335, 64336
- 7 os-windows rules with SIDs 301085, 301087, 64312, 301086, 58655, 300987, 301084
- 2 policy-other rules with SIDs 64351, 64353

- 1 server-mail rule with SID 64350
- 2 server-other rules with SIDs 38575, 63952
- 12 server-webapp rules with SIDs 53256, 64330, 62547, 64331, 62546, 64337, 64352, 64327, 300999, 64244, 64303, 64332

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

- CVE-2024-9404: (Denial-of-Service Vulnerability in Moxa VPort 07-3 Series)
    - Moxa's IP Cameras are affected by a medium-severity vulnerability which could lead to a denial-of-service condition or cause a service crash. This vulnerability allows attackers to exploit the Moxa service, commonly referred to as moxa_cmd, originally designed for deployment. Because of insufficient input validation, this service may be manipulated to trigger a denial-of-service.
- CVE-2024-11737: (Improper Input Validation Vulnerability in Schneider Modicon M241 / M251 / M258 / LMC058)
    - A vulnerability exists that could lead to a denial of service and a loss of confidentiality, integrity of the controller when an unauthenticated crafted Modbus packet is sent to the device.
- CVE-2020-28398: (Cross-Site Request Forgery (CSRF) Vulnerability in Siemens RUGGEDCOM ROX II)
    - The CLI feature in the web interface of affected devices is vulnerable to cross-site request forgery (CSRF). This could allow an attacker to read or modify the device configuration by tricking an authenticated legitimate user into accessing a malicious link.
- CVE-2024-53832 : (Insufficiently Protected Credentials Vulnerability in Siemens SICAM A8000 CP-8031 and CP-8050)
    - The affected devices contain a secure element which is connected via an unencrypted SPI bus. This could allow an attacker with physical access to the SPI bus to observe the password used for the secure element authentication, and then use the secure element as an oracle to decrypt all encrypted update files.

20241206

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

- **Talos Rules 2024-12-05 (https://www.snort.org/advisories/talos-rules-2024-12-05)**
- **Talos Rules 2024-12-03 (https://www.snort.org/advisories/talos-rules-2024-12-03)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 301082
- 2 file-image rules with SIDs 64298, 64297
- 2 file-other rules with SIDs 64301, 64302

- 2 malware-cnc rules with SIDs 64295, 64282
- 1 malware-other rule with SID 301080
- 3 policy-other rules with SIDs 64281, 64279, 64299
- 1 server-apache rule with SID 300060
- 1 server-mail rule with SID 64276
- 2 server-other rules with SIDs 64280, 64290
- 8 server-webapp rules with SIDs 64286, 64285, 64300, 64292, 301081, 301079, 64291, 64296