Release Notes for Cisco Cyber Vision Knowledge DB

Release 202409

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-5.0.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.0.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.0.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.0.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.0.1.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.0.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.0.1.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.0.1.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.0.1.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.0.1.dat	Knowledge DB embedded in Cisco Cyber Vision 5.0.1
Updates/KDB/KDB.202409	**Description**
CiscoCyberVision_knowledgedb_20240920.db	Knowledge DB version 20240920
CiscoCyberVision_knowledgedb_20240913.db	Knowledge DB version 20240913
CiscoCyberVision_knowledgedb_20240906.db	Knowledge DB version 20240906

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

20240920

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

- **Talos Rules 2024-09-19 (https://www.snort.org/advisories/talos-rules-2024-09-19)**
- **Talos Rules 2024-09-17 (https://www.snort.org/advisories/talos-rules-2024-09-17)**

The new and updated Snort rules span the following categories:

- 4 malware-other rules with SIDs 301016, 301019, 301017, 301020
- 1 malware-tools rules with SIDs 301018
- 2 os-other rules with SIDs 63960, 63959
- 6 server-webapp rules with SIDs 64012, 64013, 64011, 64007, 64008, 64006

20240913

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

- **Talos Rules 2024-09-12 (https://www.snort.org/advisories/talos-rules-2024-09-12)**
- **Talos Rules 2024-09-10 (https://www.snort.org/advisories/talos-rules-2024-09-10)**

The new and updated Snort rules span the following categories:

- 3 browser-ie rules with SIDs 63980, 63981, 63982
- 1 malware-backdoor rule with SID 63997
- 4 malware-other rules with SIDs 301006, 301007, 301005, 301014
- 6 os-windows rules with SIDs 301009, 301011, 301008, 301010, 301012, 301013
- 3 policy-other rules with SIDs 64001, 63986, 63985
- 11 server-webapp rules with SIDs 61423, 61425, 61422, 64004, 64003, 301015, 63995, 64000, 63996, 61424, 64005

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

- CVE-2024-7698: (Insufficient Sensitive Information Removal Vulnerability in Phoenix Contact mGuard devices)
    - Confidential data in HTTP query string of user requests. Incomplete sanitation of user input in administrative web interface.

- CVE-2024-7734: (Insufficient Sensitive Information Removal Vulnerability in Phoenix Contact mGuard devices)
    - Uncontrolled Resource Consumption Vulnerability in Phoenix Contact mGuard devices.
- CVE-2024-45825: (Denial-of-Service Vulnerability in Rockwell 5015-U8IHFT)
    - A denial-of-service vulnerability exists in the affected products. The vulnerability occurs when a malformed CIP packet is sent over the network to the device and results in a major nonrecoverable fault causing a denial-of-service.
- CVE-2023-44373: (Injection Vulnerability in Siemens SCALANCE W700 802.11 AX Family)
    - Affected devices do not properly sanitize an input field. This could allow an authenticated remote attacker with administrative privileges to inject code or spawn a system root shell.
- CVE-2023-28827: (NULL Pointer Dereference Vulnerability in multiple Siemens SIMATIC products)
    - The web server of the affected devices do not properly handle certain requests, causing a timeout in the watchdog, which could lead to the clean-up of pointers.
- CVE-2023-30755: (NULL Pointer Dereference Vulnerability in multiple Siemens SIMATIC products)
    - The web server of the affected devices do not properly handle the shutdown or reboot request, which could lead to the clean up of certain resources. This could allow a remote attacker with elevated privileges to cause a denial of service condition in the system.
- CVE-2023-30756: (NULL Pointer Dereference Vulnerability in multiple Siemens SIMATIC products)
    - The web server of the affected devices do not properly handle certain errors when using the Expect HTTP request header, resulting in NULL dereference. This could allow a remote attacker with no privileges to cause a denial of service condition in the system.

20240906

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

- **Talos Rules 2024-09-04 (https://www.snort.org/advisories/talos-rules-2024-09-04)**
- **Talos Rules 2024-08-29 (https://www.snort.org/advisories/talos-rules-2024-08-29)**
- **Talos Rules 2024-08-27 (https://www.snort.org/advisories/talos-rules-2024-08-27)**

The new and updated Snort rules span the following categories:

- 2 malware-backdoor rules with SIDs 301003, 301000
- 11 malware-cnc rules with SIDs 63940, 63942, 63933, 63941, 63938, 63932, 63937, 63953, 63954, 63963, 63968
- 7 malware-other rules with SIDs 63970, 63967, 63965, 63966, 301004, 63969, 63964
- 2 os-other rules with SIDs 63594, 63595, 63959, 63960
- 2 policy-other rules with SIDs 63934, 63939

- 18 server-webapp rules with SIDs 301002, 301001, 300951, 300999, 63387, 300857, 300846, 300946, 63943, 63957, 63951, 63949, 63956, 63955, 63958, 63962, 63961, 63950
- 1 server-other rules with SID 63952