Release Notes for Cisco Cyber Vision Knowledge DB

Release 202408

Compatible device list *2*

Links *2*

Software Download 2

Related Documentation 3

Database download *3*

How to update the database *3*

Release contents *4*

20240823 4

20240814 4

20240809 5

20240805 6

20240802 6

Compatible device list

Center	Description
All version 4 centers	All Cisco Cyber Vision center version 4 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-5.0.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.0.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.0.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.0.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.0.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.0.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.0.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.0.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.0.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.0.0.dat	Knowledge DB embedded in Cisco Cyber Vision 5.0.0
Updates/KDB/KDB.202408	**Description**
CiscoCyberVision_knowledgedb_20240802.db	Knowledge DB version 20240802
CiscoCyberVision_knowledgedb_20240805.db	Knowledge DB version 20240805
CiscoCyberVision_knowledgedb_20240809.db	Knowledge DB version 20240809
CiscoCyberVision_knowledgedb_20240814.db	Knowledge DB version 20240814
CiscoCyberVision_knowledgedb_20240823.db	Knowledge DB version 20240823

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

20240823

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

- **Talos Rules 2024-08-22 (https://www.snort.org/advisories/talos-rules-2024-08-22)**
- **Talos Rules 2024-08-20 (https://www.snort.org/advisories/talos-rules-2024-08-20)**
- **Talos Rules 2024-08-15 (https://www.snort.org/advisories/talos-rules-2024-08-15)**

The new and updated Snort rules span the following categories:

- 4 browser-plugins rules with SIDs 31408, 31410, 31409, 31407
- 7 malware-cnc rules with SIDs 63913, 63917, 63899, 63900, 63902, 63901, 63898
- 6 malware-other rules with SIDs 300998, 300996, 300994, 300995, 300997, 300991
- 1 malware-tools rules with SIDs 300993
- 1 policy-other rules with SIDs 300992
- 1 protocol-scada rules with SIDs 63887
- 2 protocol-voip rules with SIDs 63931, 63930
- 1 server-apache rules with SIDs 63919
- 19 server-webapp rules with SIDs 300989, 63895, 63918, 63914, 63886, 63884, 63910, 300990, 63885, 63908, 63889, 63890, 63903, 63888, 63904, 63905, 63907, 63906, 63909

20240814

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

- **Talos Rules 2024-08-13 (https://www.snort.org/advisories/talos-rules-2024-08-13)**

The new and updated Snort rules span the following categories:

- 1 browser-ie rule with SID 300982
- 6 file-pdf rules with SIDs 32815, 39799, 39922, 32816, 39798, 39923
- 2 malware-cnc rules with SIDs 63862, 63863
- 9 os-windows rules with SIDs 300981, 300985, 63878, 300986, 300983, 300980, 300988, 300984, 300987
- 2 policy-other rules with SIDs 63882, 63881
- 6 server-webapp rules with SIDs 63855, 63857, 63856, 63879, 63880, 63883

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

- CVE-2024-39922: (Plaintext Storage of a Password Vulnerability in Siemens LOGO! V8.3 BM Devices)
    - LOGO! V8.3 BM (incl. SIPLUS variants) devices contain a plaintext storage of a password vulnerability. This could allow an attacker with phyiscal access to an affected device to extract user-set passwords from an embedded storage IC.
- CVE-2023-44321: (Uncontrolled Resource Consumption Vulnerability in Siemens SCALANCE M-800 Family)
    - Affected devices do not properly validate the length of inputs when performing certain configuration changes in the web interface allowing an authenticated attacker to cause a denial of service condition. The device needs to be restarted for the web interface to become available again.
- CVE-2024-41976: (Improper Input Validation Vulnerability in Siemens SCALANCE M-800 Family)
    - Affected devices do not properly validate input in specific VPN configuration fields. This could allow an authenticated remote attacker to execute arbitrary code on the device.
- CVE-2024-41977: (Exposure of Data Element to Wrong Session Vulnerability in Siemens SCALANCE M-800 Family)
    - Affected devices do not properly enforce isolation between user sessions in their web server component. This could allow an authenticated remote attacker to escalate their privileges on the devices.
- CVE-2024-41978: (Insertion of Sensitive Information into Log File Vulnerability in Siemens SCALANCE M-800 Family)
    - Affected devices insert sensitive information about the generation of 2FA tokens into log files. This could allow an authenticated remote attacker to forge 2FA tokens of other users.

20240809

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

- **Talos Rules 2024-08-08 (https://www.snort.org/advisories/talos-rules-2024-08-08)**
- **Talos Rules 2024-08-06 (https://www.snort.org/advisories/talos-rules-2024-08-06)**
- **Talos Rules 2024-08-02 (https://www.snort.org/advisories/talos-rules-2024-08-02)**

The new and updated Snort rules span the following categories:

- 1 file-office rule with SID 47565
- 1 indicator-obfuscation rule with SID 63845
- 15 server-webapp rules with SIDs 63849, 63853, 63851, 60911, 63850, 300979, 63848, 62046, 60910, 63852, 62043, 2381, 62044, 62045, 63854

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

- CVE-2024-6387: (Signal Handler Race Condition in Multiple Moxa Product Series)

- CVE-2024-6387 is a remote unauthenticated code execution vulnerability in OpenSSH, specifically related to a race condition in the OpenSSH server (sshd). The issue arises when a client fails to authenticate within the LoginGraceTime period (default is 120 seconds, or 600 seconds in older OpenSSH versions). In this case, the sshd's SIGALRM signal handler is invoked asynchronously. However, this signal handler calls several functions that are unsafe to use in asynchronous signal contexts, such as syslog().

20240805

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

- CVE-2024-6242: (Chassis Restrictions Bypass Vulnerability in Select Rockwell Logix Devices)
  - A vulnerability exists in the affected products that allows a threat actor to bypass the Trusted® Slot feature in a ControlLogix® controller. If exploited on any affected module in a 1756 chassis, a threat actor could potentially execute CIP commands that modify user projects and/or device configuration on a Logix controller in the chassis.

20240802

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

- **Talos Rules 2024-08-01 (https://www.snort.org/advisories/talos-rules-2024-08-01)**
- **Talos Rules 2024-07-30 (https://www.snort.org/advisories/talos-rules-2024-07-30)**

The new and updated Snort rules span the following categories:

- 2 malware-cnc rules with SIDs 63838, 63840
- 3 policy-other rules with SIDs 63839, 63843, 63499
- 4 server-other rules with SIDs 35093, 63812, 35092, 63844
- 33 server-webapp rules with SIDs 63809, 63836, 300978, 63837, 62045, 62044, 63813, 62043, 62046, 63833, 63823, 63826, 63815, 63825, 63842, 63817, 63831, 63835, 63819, 63827, 63814, 63824, 63821, 63818, 63829, 63832, 63820, 63834, 63830, 63841, 63828, 63822, 63816