Release Notes for Cisco Cyber Vision Knowledge DB

Release 202301

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-4.1.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.1.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.1.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.1.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.1.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.1.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.1.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.1.0.dat	Knowledge DB embedded in Cisco Cyber Vision 4.1.0
Updates/KDB/KDB.202301	**Description**
CiscoCyberVision_knowledgedb_20230106.db	Knowledge DB version 20230106
CiscoCyberVision_knowledgedb_20230113.db	Knowledge DB version 20230113
CiscoCyberVision_knowledgedb_20230120.db	Knowledge DB version 20230120
CiscoCyberVision_knowledgedb_20230127.db	Knowledge DB version 20230127

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

20230127

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

- **Talos Rules 2023-01-26 (https://www.snort.org/advisories/talos-rules-2023-01-26)**
  - Talos has added and modified multiple rules in the malware-tools, os-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2023-01-24 (https://www.snort.org/advisories/talos-rules-2023-01-24)**
  - Talos has added and modified multiple rules in the deleted, malware-cnc, malware-other, os-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20230120

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

- **Talos Rules 2023-01-19 (https://www.snort.org/advisories/talos-rules-2023-01-19)**
  - Talos has added and modified multiple rules in the and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2023-01-17 (https://www.snort.org/advisories/talos-rules-2023-01-17)**
  - Talos has added and modified multiple rules in the browser-chrome, file-office, malware-cnc, malware-other, os-linux, os-windows, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20230113

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

- **Talos Rules 2023-01-12 (https://www.snort.org/advisories/talos-rules-2023-01-12)**
  - Talos has added and modified multiple rules in the file-office, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2023-01-10 (https://www.snort.org/advisories/talos-rules-2023-01-10)**
  - Microsoft Vulnerability CVE-2023-21552: A coding deficiency exists in Microsoft Windows GDI that may lead to elevation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort 2: GID 1, SIDs 61060 through 61061, Snort 2: GID 1, SID 300358.
  - Microsoft Vulnerability CVE-2023-21674: A coding deficiency exists in Microsoft Windows Advanced Local Procedure Call (ALPC) that may lead to an escalation of privilege.

        - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort 2: GID 1, SIDs 61062 through 61063, Snort 3: GID 1, SID 300359.
    - Microsoft Vulnerability CVE-2023-21768: A coding deficiency exists in Microsoft Windows Ancillary Function Driver for WinSock that may lead to an escalation of privilege.
        - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort 2: GID 1, SIDs 61064 through 61065, Snort 3: GID 1, SID 300360.
    - Talos also has added and modified multiple rules in the malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

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

- CVE-2022-38773: (Missing Immutable Root of Trust in Siemens S7-1500 CPU devices)
    - Affected devices do not contain an Immutable Root of Trust in Hardware. With this the integrity of the code executed on the device cannot be validated during load-time. An attacker with physical access to the device could use this to replace the boot image of the device and execute arbitrary code.
- CVE-2008-1160: (Use of Hard-coded Credentials Vulnerability in Moxa TN-4900 series)
    - An attacker may be able to gain privileges if an embedded credential is used

20230106

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

- **Talos Rules 2023-01-05 (https://www.snort.org/advisories/talos-rules-2023-01-05)**
    - Talos has added and modified multiple rules in the and malware-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-12-28 (https://www.snort.org/advisories/talos-rules-2022-12-28)**
    - Talos has added and modified multiple rules in the malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-12-23 (https://www.snort.org/advisories/talos-rules-2022-12-23)**
    - Talos is releasing the following SID to protect against a critical vulnerability in ksmbd (CVE-2022-47939), 61041. Talos has added and modified a rule in the os-linux rule sets to provide coverage for emerging threats from these technologies.