Release Notes for Cisco Cyber Vision Knowledge DB

Release 202209

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.202209	**Description**
CiscoCyberVision_knowledgedb_20220902.db	Knowledge DB version 20220902
CiscoCyberVision_knowledgedb_20220909.db	Knowledge DB version 20220909
CiscoCyberVision_knowledgedb_20220916.db	Knowledge DB version 20220916
CiscoCyberVision_knowledgedb_20220923.db	Knowledge DB version 20220923
CiscoCyberVision_knowledgedb_20220930.db	Knowledge DB version 20220930

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

20220930

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

- **Talos Rules 2022-09-29 (https://www.snort.org/advisories/talos-rules-2022-09-29)**
  - Talos has added and modified multiple rules in the malware-tools, os-other, policy-other, protocol-rpc, protocol-scada and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-09-27 (https://www.snort.org/advisories/talos-rules-2022-09-27)**
  - Talos has added and modified multiple rules in the file-other, file-pdf, malware-cnc, os-linux and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20220923

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

- **Talos Rules 2022-09-22 (https://www.snort.org/advisories/talos-rules-2022-09-22)**
  - Talos has added and modified multiple rules in the browser-chrome, file-pdf, malware-cnc, malware-other, malware-tools, os-mobile, os-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-09-20 (https://www.snort.org/advisories/talos-rules-2022-09-20)**
  - Talos has added and modified multiple rules in the browser-chrome, file-pdf, malware-cnc, malware-other, malware-tools, os-mobile, os-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20220916

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

- **Talos Rules 2022-09-15 (https://www.snort.org/advisories/talos-rules-2022-09-15)**
  - 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 2022-09-13 (https://www.snort.org/advisories/talos-rules-2022-09-13)**
  - Microsoft Vulnerability CVE-2022-34725: A coding deficiency exists in Microsoft Windows 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: Snort2: GID 1, SIDs 60553 through 60554, Snort3: GID 1, SID 300268.

- Microsoft Vulnerability CVE-2022-34729: A coding deficiency exists in Microsoft Windows GDI that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 60549 through 60550, Snort3: GID 1, SID 300266.
- Microsoft Vulnerability CVE-2022-35803: A coding deficiency exists in Microsoft Windows Common Log File System driver that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 60555 through 60558, Snort3: GID 1, SIDs 300269 through 300270.
- Microsoft Vulnerability CVE-2022-37954: A coding deficiency exists in DirectX Graphics Kernel that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 60551 through 60552, Snort3: GID 1, SID 300267.
- Microsoft Vulnerability CVE-2022-37957: A coding deficiency exists in Microsoft Windows Kernel that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 60546 through 60547, Snort3: GID 1, SID 300265.
- Talos also has added and modified multiple rules in the 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 vulnerability:

- CVE-2022-39158: (Denial of Service Vulnerability in Siemens RUGGEDCOM ROS)
  - RUGGEDCOM ROS-based devices are vulnerable to a denial-of-service attack (Slowloris). By sending partial HTTP requests nonstop, with none completed, the affected web servers will be waiting for the completion of each request, occupying all available HTTP connections. The web server recovers by itself once the attack ends.

20220909

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

- **Talos Rules 2022-09-08 (https://www.snort.org/advisories/talos-rules-2022-09-08)**
  - Talos has added and modified multiple rules in the and file-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-09-06 (https://www.snort.org/advisories/talos-rules-2022-09-06)**
  - Talos has added and modified multiple rules in the file-other, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20220902

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

- **Talos Rules 2022-09-01 (https://www.snort.org/advisories/talos-rules-2022-09-01)**
  - 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 2022-08-30 (https://www.snort.org/advisories/talos-rules-2022-08-30)**
  - Talos has added and modified multiple rules in the file-office, file-other, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.