Release Notes for Cisco Cyber Vision Knowledge DB

Release 202312

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-4.2.6.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.2.6.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.2.6.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.2.6.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.2.6.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.2.6.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.2.6.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.2.6.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.6.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.2.6.dat	Knowledge DB embedded in Cisco Cyber Vision 4.2.6
Updates/KDB/KDB.202312	**Description**
CiscoCyberVision_knowledgedb_20231201.db	Knowledge DB version 20231201
CiscoCyberVision_knowledgedb_20231208.db	Knowledge DB version 20231208
CiscoCyberVision_knowledgedb_20231215.db	Knowledge DB version 20231215
CiscoCyberVision_knowledgedb_20231222.db	Knowledge DB version 20231222

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

20231222

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

- **Talos Rules 2023-12-21 (https://www.snort.org/advisories/talos-rules-2023-12-21)**
- **Talos Rules 2023-12-19 (https://www.snort.org/advisories/talos-rules-2023-12-19)**

The new and updated Snort rules span the following categories:

- 1 policy-other rule with SID 62792
- 1 protocol-dns rule with SID 254
- 10 server-webapp rules with SIDs 300787, 62629, 62555, 62794, 62793, 62789, 62795, 62796, 300788, 62808

20231215

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

- **Talos Rules 2023-12-14 (https://www.snort.org/advisories/talos-rules-2023-12-14)**
- **Talos Rules 2023-12-12 (https://www.snort.org/advisories/talos-rules-2023-12-12)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 300776
- 1 file-executable rule with SID 300778
- 1 malware-cnc rule with SID 62788
- 3 malware-other rules with SIDs 300783, 300782, 300775
- 3 malware-tools rules with SIDs 56583, 56585, 56584
- 6 os-windows rules with SIDs 300780, 300781, 300779, 300774, 300784, 300777
- 8 server-webapp rules with SIDs 300786, 300785, 61709, 300523, 62761, 62758, 62753, 62776
- 1 policy-other rules with SIDs 62792
- 1 protocol-dns rules with SIDs 254
- 10 server-webapp rules with SIDs 300787, 62629, 62555, 62794, 62793, 62789, 62795, 62796, 300788, 62808

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

- CVE-2022-47375: (Buffer Overflow Vulnerability in the Webserver of Siemens Industrial Products)

  - The affected products do not handle long file names correctly. This could allow an attacker to create a buffer overflow and create a denial of service condition for the device.

- CVE-2022-47374: (Uncontrolled Recursion in the Webserver of Siemens Industrial Products)
  - The affected products do not handle HTTP(S) requests to the web server correctly. This could allow an attacker to exhaust system resources and create a denial of service condition for the device.
- CVE-2023-38380: (Memory Leak Vulnerability in the Web Server of Siemens Industrial Products)
  - The webserver implementation of the affected products does not correctly release allocated memory after it has been used. An attacker with network access could use this vulnerability to cause a denial-of-service condition in the webserver of the affected product.
- CVE-2023-46156: (Use After Free Vulnerability in Siemens SIMATIC S7-1500 CPUs and related products)
  - Affected devices improperly handle specially crafted packets sent to port 102/tcp. This could allow an attacker to create a denial-of-service condition. A restart is needed to restore normal operations.
- CVE-2023-31238: (Improper Authorization Vulnerability in Siemens SICAM Q100 Devices)
  - Affected devices are missing cookie protection flags when using the default settings. An attacker who gains access to a session token can use it to impersonate a legitimate application user.
- CVE-2023-38380: (Memory Leak Vulnerability in the Web Server of Siemens Industrial Products)
  - The webserver implementation of the affected products does not correctly release allocated memory after it has been used. An attacker with network access could use this vulnerability to cause a denial-of-service condition in the webserver of the affected product.
- CVE-2023-30901: (Cross-Site Request Forgery Vulnerability in Siemens SICAM Q100 Devices)
  - The web interface of the affected devices are vulnerable to Cross-Site Request Forgery attacks. By tricking an authenticated victim user to click a malicious link, an attacker could perform arbitrary actions on the device on behalf of the victim user.
- CVE-2023-49692: (OS Command Injection Vulnerability in Siemens SCALANCE M-800/S615)
  - An Improper Neutralization of Special Elements used in an OS Command with root privileges vulnerability exists in the parsing of the IPSEC configuration. This could allow malicious local administrators to issue commands on system level after a new connection is established.
- CVE-2023-44317: (Insufficient Verification of Data Authenticity in Siemens SCALANCE M-800/S615)
  - Affected products do not properly validate the content of uploaded X509 certificates which could allow an attacker with administrative privileges to execute arbitrary code on the device.

20231208

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

- **Talos Rules 2023-12-07 (https://www.snort.org/advisories/talos-rules-2023-12-07)**

- **Talos Rules 2023-12-05 (https://www.snort.org/advisories/talos-rules-2023-12-05)**

The new and updated Snort rules span the following categories:

- 4 file-identify rules with SIDs 62748, 62746, 62745, 62747
- 1 indicator-scan rule with SID 19559
- 3 malware-cnc rules with SIDs 62740, 62721, 62709
- 8 malware-other rules with SIDs 62720, 62722, 300769, 300772, 300771, 300770, 300773, 300768
- 1 server-other rule with SID 62706
- 5 server-webapp rules with SIDs 62741, 62704, 62707, 62708, 62705

20231201

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

- **Talos Rules 2023-11-29 (https://www.snort.org/advisories/talos-rules-2023-11-29)**
- **Talos Rules 2023-11-28 (https://www.snort.org/advisories/talos-rules-2023-11-28)**

The new and updated Snort rules span the following categories:

- 1 file-pdf rule with SID 300767
- 1 malware-backdoor rule with SID 62673
- 2 malware-cnc rules with SIDs 62680, 62676
- 3 malware-other rules with SIDs 300763, 300764, 62685
- 1 os-linux rule with SID 300765
- 2 policy-other rules with SIDs 300766, 62698
- 3 server-other rules with SIDs 300396, 61246, 61247
- 7 server-webapp rules with SIDs 62677, 62678, 62695, 62679, 62674, 62697, 62696