Release Notes for Cisco Cyber Vision Knowledge DB

Release 202306

Compatible device list *2*

Links *2*

Software Download 2

Related Documentation 3

Database download *3*

How to update the database *3*

Release contents *4*

20230630 4

20230623 4

20230609 6

20230602 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-4.2.2.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.2.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.2.2.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.2.2.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.2.2.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.2.2.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.2.2.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.2.2.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.2.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.2.2.dat	Knowledge DB embedded in Cisco Cyber Vision 4.2.1
Updates/KDB/KDB.202306	**Description**
CiscoCyberVision_knowledgedb_20230602.db	Knowledge DB version 20230602
CiscoCyberVision_knowledgedb_20230609.db	Knowledge DB version 20230609
CiscoCyberVision_knowledgedb_20230623.db	Knowledge DB version 20230623
CiscoCyberVision_knowledgedb_20230630.db	Knowledge DB version 20230630

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

20230630

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

- **Talos Rules 2023-06-29 (https://www.snort.org/advisories/talos-rules-2023-06-29)**
- **Talos Rules 2023-06-27 (https://www.snort.org/advisories/talos-rules-2023-06-27)**

The new and updated Snort rules span the following categories:

- 1 indicator-compromise rules with SID 300603
- 2 malware-backdoor rules with SIDs 300582, 300583
- 1 os-windows rules with SID 300604

20230623

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

- **Talos Rules 2023-06-22 (https://www.snort.org/advisories/talos-rules-2023-06-22)**
- **Talos Rules 2023-06-20 (https://www.snort.org/advisories/talos-rules-2023-06-20)**
- **Talos Rules 2023-06-15 (https://www.snort.org/advisories/talos-rules-2023-06-15)**
- **Talos Rules 2023-06-13 (https://www.snort.org/advisories/talos-rules-2023-06-13)**

The new and updated Snort rules span the following categories:

- 2 file-other rules with SIDs 300590, 16295
- 1 malware-backdoor rule with SID 57287
- 2 malware-cnc rules with SIDs 300588, 300589
- 3 malware-other rules with SIDs 300600, 300601, 300602
- 1 malware-tools rule with SID 300594
- 4 os-windows rules with SIDs 300591, 300592, 300593, 300595
- 3 policy-other rules with SIDs 300444, 61945, 61946
- 1 server-mail rule with SID 61933
- 1 server-other rule with SID 51181
- 21 server-webapp rules with SIDs 43268, 300442, 300443, 61865, 61897, 61898, 61899, 61900, 300596, 300597, 300598, 300599, 61936, 61937, 61938, 61939, 61940, 61941, 61942, 61943, 61944

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

- CVE-2023-33919: (Command Injection Vulnerability in Siemens SICAM Q200 Devices)
    - The web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges
- CVE-2023-33920: (Use of Hard-coded Credentials Vulnerability in Siemens SICAM Q200 Devices)
    - The affected devices contain the hash of the root password in a hard-coded form, which could be exploited for UART console login to the device. An attacker with direct physical access could exploit this vulnerability.
- CVE-2023-33921: (Exposed Dangerous Method or Function Vulnerability in Siemens SICAM Q200 Devices)
    - The affected devices contain an exposed UART console login interface. An attacker with direct physical access could try to bruteforce or crack the root password to login to the device.
- CVE-2022-43398: (Session Fixation Vulnerability in Siemens SICAM Q200 Devices)
    - Affected devices do not renew the session cookie after login/logout and also accept user defined session cookies. An attacker could overwrite the stored session cookie of a user. After the victim logged in, the attacker is given access to the user's account through the activated session.
- CVE-2022-43439: (Improper Input Validation Vulnerability in Siemens SICAM Q200 Devices)
    - Affected devices do not properly validate the Language-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.
- CVE-2022-43545: (Improper Input Validation Vulnerability in Siemens SICAM Q200 Devices)
    - Affected devices do not properly validate the RecordType-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.
- CVE-2022-43546: (Improper Input Validation Vulnerability in Siemens SICAM Q200 Devices)
    - Affected devices do not properly validate the EndTime-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.
- CVE-2023-30901: (Cross-Site Request Forgery Vulnerability in Siemens SICAM Q200 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-2023-31238: (Incorrect Permission Assignment for Critical Resource Vulnerability in Siemens SICAM Q200 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-2022-4304: (Timing-based Side Channel Vulnerability in Phoenix Contact FL MGUARD family)

  - The OpenSSL library contains a bug that leads to a timing oracle when RSA based ciphers are used without forward secrecy for network communication. By sending a very large number of trial messages, an attacker can try to achieve a decryption of encrypted network packets. This affects TLS connections to and from the FL MGUARD as well as VPN connections. The highest risk arises from deferred attempts to decrypt pre-recorded network sessions. The throttling feature of the FL MGUARD can impede but not prevent the attack.

- CVE-2023-2673: (Improper Input Validation Vulnerability in Phoenix Contact FL MGUARD family)
  - Improper Input Validation vulnerability in PHOENIX CONTACT FL/TC MGUARD Family in multiple versions may allow UDP packets to bypass the filter rules and access the solely connected device behind the MGUARD which can be used for flooding attacks.

20230609

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

- **Talos Rules 2023-06-08 (https://www.snort.org/advisories/talos-rules-2023-06-08)**
- **Talos Rules 2023-06-06 (https://www.snort.org/advisories/talos-rules-2023-06-06)**
- **Talos Rules 2023-06-02 (https://www.snort.org/advisories/talos-rules-2023-06-02)**
- **Talos Rules 2023-06-01 (https://www.snort.org/advisories/talos-rules-2023-06-01)**

The new and updated Snort rules span the following categories:

- 2 file-identify rules with SIDs 300579, 61894
- 2 indicator-compromise rules with SIDs 300584, 61893
- 4 indicator-obfuscation rules with SIDs 61861, 61862, 61863, 61864
- 2 indicator-shellcode rules with SIDs 300580, 300581
- 2 malware-backdoor rules with SIDs 300582, 300583
- 1 malware-cnc rules with SID 61880
- 2 malware-other rules with SIDs 61840, 300578
- 3 malware-tools rules with SIDs 300585, 300586, 300587
- 3 server-webapp rules with SIDs 61865, 61866, 61867

20230602

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

- **Talos Rules 2023-05-30 (https://www.snort.org/advisories/talos-rules-2023-05-30)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rules with SID 300555
- 8 malware-cnc rules with SIDs 61839, 300569, 300571, 300572, 300573, 300574, 300575, 300576
- 16 malware-other rules with SIDs 300556, 300557, 300558, 300559, 300560, 300561, 300562, 300563, 300564, 300565, 300566, 300567, 300568, 61840, 300570, 300577
- 1 os-windows rules with SID 61836
- 6 server-webapp rules with SIDs 61832, 61833, 61834, 61835, 61837, 61838