Release Notes for Cisco Cyber Vision Knowledge DB

Release 202403

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-4.3.2.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.3.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.3.2.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.3.2.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.3.2.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.3.2.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.3.2.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.3.2.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.3.2.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.3.2.dat	Knowledge DB embedded in Cisco Cyber Vision 4.3.2
Updates/KDB/KDB.202403	**Description**
CiscoCyberVision_knowledgedb_20240301.db	Knowledge DB version 20240301
CiscoCyberVision_knowledgedb_20240308.db	Knowledge DB version 20240308
CiscoCyberVision_knowledgedb_20240315.db	Knowledge DB version 20240315
CiscoCyberVision_knowledgedb_20240322.db	Knowledge DB version 20240322
CiscoCyberVision_knowledgedb_20240329.db	Knowledge DB version 20240329

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

20240329

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

- **Talos Rules 2024-03-28 (https://www.snort.org/advisories/talos-rules-2024-03-28)**
- **Talos Rules 2024-03-26 (https://www.snort.org/advisories/talos-rules-2024-03-26)**

The new and updated Snort rules span the following categories:

- 1 malware-cnc rule with SIDs 63215
- 4 malware-other rules with SIDs 300869, 300870, 300867, 300868
- 2 server-other rules with SIDs 43790, 63214

20240322

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

- **Talos Rules 2024-03-21 (https://www.snort.org/advisories/talos-rules-2024-03-21)**
- **Talos Rules 2024-03-19 (https://www.snort.org/advisories/talos-rules-2024-03-19)**

The new and updated Snort rules span the following categories:

- 2 browser-chrome rules with SIDs 300864, 300865
- 1 indicator-compromise rules with SID 39866
- 4 malware-cnc rules with SIDs 63197, 63194, 63198, 63192
- 1 policy-other rules with SID 63193
- 5 server-webapp rules with SIDs 62934, 63203, 63195, 63196, 300866

20240315

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

- **Talos Rules 2024-03-14 (https://www.snort.org/advisories/talos-rules-2024-03-14)**
- **Talos Rules 2024-03-12 (https://www.snort.org/advisories/talos-rules-2024-03-12)**

The new and updated Snort rules span the following categories:

- 1 file-java rule with SID 300863
- 1 file-other rule with SID 300859
- 1 malware-cnc rule with SID 63188

- 1 malware-other rule with SID 300861
- 5 os-windows rules with SIDs 300855, 300858, 300856, 300860, 300862
- 1 server-apache rule with SID 63187
- 4 server-other rules with SIDs 63147, 63149, 63148, 63146
- 14 server-webapp rules with SIDs 63142, 63154, 63183, 63182, 300857, 63181, 59340, 59341, 63143, 63138, 63184, 44667, 43279, 59339

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

- CVE-2023-44318: (Use of Hard-coded Cryptographic Key in Siemens Scalance XB-200/XC-200/XP-200/XF-200BA/XR-300WG family)
    - Affected devices use a hardcoded key to obfuscate the configuration backup that an administrator can export from the device. This could allow an authenticated attacker with administrative privileges or an attacker that obtains a configuration backup to extract configuration information from the exported file.
- CVE-2023-44321: (Uncontrolled Resource Consumption in Siemens Scalance XB-200/XC-200/XP-200/XF-200BA/XR-300WG 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-2024-1220: (Stack-based Buffer Overflow Vulnerability in Moxa NPort W2150A/W2250A)
    - A stack-based buffer overflow in the built-in web server in Moxa NPort W2150A/W2250A Series firmware version 2.3 and prior allows a remote attacker to exploit the vulnerability by sending crafted payload to the web service. Successful exploitation of the vulnerability could result in denial of service.
- CVE-2024-2050: (Cross-site Scripting Vulnerability in Schneider Easergy T200)
    - A cross-site scripting vulnerability exists when an attacker injects then executes arbitrary malicious JavaScript code within the context of the product.
- CVE-2024-2051: (Improper Restriction of Excessive Authentication Attempts Vulnerability in Schneider Easergy T200)
    - Improper restriction of excessive authentication attempts could cause account takeover and unauthorized access to the system when an attacker conducts brute-force attacks against the login form.
- CVE-2024-2052: (Access Control Vulnerability in Schneider Easergy T200)
    - An access control vulnerability exists that could allow unauthenticated files and logs exfiltration and download of files when an attacker modifies the URL to download to a different location.

- CVE-2024-21483: (Improper Access Control in Siemens Sentron 7KM PAC3x20 Devices)
    - The read-out protection of the internal flash of affected devices was not properly set at the end of the manufacturing process. An attacker with physical access to the device could read out the data.
- CVE-2024-25994: (Improper Input Validation Vulnerability in Phoenix Contact CHARX SEC-3xxx charge controllers)
    - An unauthenticated remote attacker can upload a arbitrary script file due to improper input validation. The upload destination is fixed and is write only.
- CVE-2024-25995: (Missing Authentication Vulnerability in Phoenix Contact CHARX SEC-3xxx charge controllers)
    - An unauthenticated remote attacker can modify configurations to perform a remote code execution due to a missing authentication for a critical function.
- CVE-2024-25996: (Improper Access Control Vulnerability in Phoenix Contact CHARX SEC-3xxx charge controllers)
    - An unauthenticated remote attacker can perform a remote code execution due to an origin validation error. The access is limited to the service user.
- CVE-2024-25997: (Improper Input Validation Vulnerability in Phoenix Contact CHARX SEC-3xxx charge controllers)
    - An unauthenticated remote attacker can perform a log injection due to improper input validation. Only a certain log file is affected.
- CVE-2024-25998: (Improper Input Validation Vulnerability in Phoenix Contact CHARX SEC-3xxx charge controllers)
    - An unauthenticated remote attacker can perform a command injection in the OCPP Service with limited privileges due to improper input validation.
- CVE-2024-25999: (Improper Input Validation Vulnerability in Phoenix Contact CHARX SEC-3xxx charge controllers)
    - An unauthenticated local attacker can perform a privilege escalation due to improper input validation in the OCPP agent service.
- CVE-2024-26000: (Improper Input Validation Vulnerability in Phoenix Contact CHARX SEC-3xxx charge controllers)
    - An unauthenticated remote attacker can read memory out of bounds due to improper input validation in the MQTT stack. The brute force attack is not always successful because of memory randomization.
- CVE-2024-26001: (Improper Input Validation Vulnerability in Phoenix Contact CHARX SEC-3xxx charge controllers)

    - An unauthenticated remote attacker can write memory out of bounds due to improper input validation in the MQTT stack. The brute force attack is not always successful because of memory randomization.

- CVE-2024-26002: (Improper Input Validation Vulnerability in Phoenix Contact CHARX SEC-3xxx charge controllers)
    - An unauthenticated remote attacker can write memory out of bounds due to improper input validation in the MQTT stack. The brute force attack is not always successful because of memory randomization.
- CVE-2024-26003: (Out-of-bounds Read Vulnerability in Phoenix Contact CHARX SEC-3xxx charge controllers)
    - An unauthenticated remote attacker can DoS the control agent due to an out-of-bounds read which may prevent or disrupt the charging functionality.
- CVE-2024-26004: (Access of Uninitialized Pointer Vulnerability in Phoenix Contact CHARX SEC-3xxx charge controllers)
    - An unauthenticated remote attacker can DoS a control agent due to access of an uninitialized pointer which may prevent or disrupt the charging functionality.
- CVE-2024-26005: (Incomplete Cleanup Vulnerability in Phoenix Contact CHARX SEC-3xxx charge controllers)
    - An unauthenticated remote attacker can gain service level privileges through an incomplete cleanup during service restart after a DoS.
- CVE-2024-26288: (Missing Encryption of Sensitive Information Vulnerability in Phoenix Contact CHARX SEC-3xxx charge controllers)
    - An unauthenticated remote attacker can influence the communication due to the lack of encryption of sensitive data via a MITM. Charging is not affected.

20240308

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

- **Talos Rules 2024-03-07 (https://www.snort.org/advisories/talos-rules-2024-03-07-3-8-2024)**
- **Talos Rules 2024-03-07 (https://www.snort.org/advisories/talos-rules-2024-03-07)**
- **Talos Rules 2024-03-05 (https://www.snort.org/advisories/talos-rules-2024-03-05)**

The new and updated Snort rules span the following categories:

- 1 file-image rule with SID 300854
- 1 file-other rule with SID 300850
- 1 malware-cnc rule with SID 63106

- 12 malware-other rules with SIDs 63121, 63122, 63129, 63119, 63120, 300852, 63124, 300853, 63123, 63126, 63118, 63125
- 1 os-mobile rule with SID 300849
- 3 policy-other rules with SIDs 44678, 300851, 63117
- 1 server-other rule with SID 45380
- 4 server-webapp rules with SIDs 63105, 34646, 63116, 63113

20240301

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

- **Talos Rules 2024-02-29 (https://www.snort.org/advisories/talos-rules-2024-02-29)**
- **Talos Rules 2024-02-27 (https://www.snort.org/advisories/talos-rules-2024-02-27)**

The new and updated Snort rules span the following categories:

- 1 file-other rule with SID 300845
- 1 indicator-compromise rule with SID 43687
- 1 malware-cnc rule with SID 63088
- 1 os-windows rule with SID 63103
- 1 policy-other rule with SID 44484
- 2 server-apache rules with SIDs 14771, 15511
- 1 server-iis rule with SID 34061
- 5 server-other rules with SIDs 9790, 300078, 300076, 38575, 300077
- 9 server-webapp rules with SIDs 63087, 300847, 300848, 63104, 300846, 63082, 44565, 58346, 63081