Release Notes for Cisco Cyber Vision Knowledge DB

Release 202402

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-4.3.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.3.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.3.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.3.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.3.1.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.3.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.3.1.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.3.1.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.3.1.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.3.1.dat	Knowledge DB embedded in Cisco Cyber Vision 4.3.1
Updates/KDB/KDB.202402	**Description**
CiscoCyberVision_knowledgedb_20240202.db	Knowledge DB version 20240202
CiscoCyberVision_knowledgedb_20240209.db	Knowledge DB version 20240209
CiscoCyberVision_knowledgedb_20240216.db	Knowledge DB version 20240216
CiscoCyberVision_knowledgedb_20240223.db	Knowledge DB version 20240223

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

20240223

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

- **Talos Rules 2024-02-22 (https://www.snort.org/advisories/talos-rules-2024-02-22)**
- **Talos Rules 2024-02-20 (https://www.snort.org/advisories/talos-rules-2024-02-20)**

20240216

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

- **Talos Rules 2024-02-15 (https://www.snort.org/advisories/talos-rules-2024-02-15)**
- **Talos Rules 2024-02-13 (https://www.snort.org/advisories/talos-rules-2024-02-13)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 300821
- 2 browser-ie rules with SIDs 36950, 36951
- 1 file-office rule with SID 300823
- 5 malware-cnc rules with SIDs 300819, 62997, 62996, 62987, 63013
- 5 malware-other rules with SIDs 300818, 63017, 300820, 300827, 63014
- 4 os-windows rules with SIDs 300822, 300824, 300826, 300825
- 1 server-other rule with SID 40360
- 1 server-webapp rule with SID 63018

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

- CVE-2023-45627: (Improper Input Validation Vulnerability in Siemens Scalance W1750D)
  - An authenticated Denial-of-Service (DoS) vulnerability exists in the CLI service. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point.
- CVE-2023-45626: (Improper Input Validation Vulnerability in Siemens SIMATIC CN 4100)
  - An authenticated vulnerability has been identified allowing an attacker to effectively establish highly privileged persistent arbitrary code execution across boot cycles.
- CVE-2023-45625: (Command Injection Vulnerability in Siemens Scalance W1750D)
  - Multiple authenticated command injection vulnerabilities exist in the command line interface. Successful exploitation of these vulnerabilities results in the ability to execute arbitrary commands as a privileged user on the underlying operating system.

- CVE-2023-45624: (Improper Input Validation Vulnerability in Siemens SIMATIC CN 4100)
    - An unauthenticated Denial-of-Service (DoS) vulnerability exists in the soft ap daemon accessed via the PAPI protocol. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point.
- CVE-2023-45623: (Improper Input Validation Vulnerability in Siemens Scalance W1750D)
    - Unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the Wi-Fi Uplink service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities results in the ability to interrupt the normal operation of the affected access point.
- CVE-2023-45622: (Improper Input Validation Vulnerability in Siemens SIMATIC CN 4100)
    - Unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the BLE daemon service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities results in the ability to interrupt the normal operation of the affected access point.
- CVE-2023-45621: (Command Injection Vulnerability in Siemens Scalance W1750D)
    - Unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the CLI service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities results in the ability to interrupt the normal operation of the affected access point.
- CVE-2023-45620: (Improper Input Validation Vulnerability in Siemens SIMATIC CN 4100)
    - Unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the CLI service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities results in the ability to interrupt the normal operation of the affected access point.
- CVE-2023-45619: (Improper Input Validation Vulnerability in Siemens Scalance W1750D)
    - There is an arbitrary file deletion vulnerability in the RSSI service accessed by PAPI (Aruba's access point management protocol). Successful exploitation of this vulnerability results in the ability to delete arbitrary files on the underlying operating system, which could lead to the ability to interrupt normal operation and impact the integrity of the access point.
- CVE-2023-45618: (Improper Input Validation Vulnerability in Siemens SIMATIC CN 4100)
    - There are arbitrary file deletion vulnerabilities in the AirWave client service accessed by PAPI (Aruba's access point management protocol). Successful exploitation of these vulnerabilities results in the ability to delete arbitrary files on the underlying operating system, which could lead to the ability to interrupt normal operation and impact the integrity of the access point.
- CVE-2023-45617: (Improper Input Validation Vulnerability in Siemens Scalance W1750D)
    - There are arbitrary file deletion vulnerabilities in the CLI service accessed by PAPI (Aruba's access point management protocol). Successful exploitation of these vulnerabilities results in the ability to delete arbitrary files on the underlying operating system, which could lead to the ability to interrupt normal operation and impact the integrity of the access point
- CVE-2023-45616: (Buffer Overflow Vulnerability in Siemens SIMATIC CN 4100)

  - There is a buffer overflow vulnerability in the underlying AirWave client service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system.

- CVE-2023-45615: (Buffer Overflow Vulnerability in Siemens Scalance W1750D)
  - There are buffer overflow vulnerabilities in the underlying CLI service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system
- CVE-2023-45614: (Buffer Overflow Vulnerability in Siemens SIMATIC CN 4100)
  - There are buffer overflow vulnerabilities in the underlying CLI service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system.
- CVE-2023-49692: (OS Command Injection Vulnerability in Siemens SCALANCE SC-600 Family)
  - 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-2023-49691: (OS Command Injection Vulnerability in Siemens SCALANCE SC-600 Family)
  - An Improper Neutralization of Special Elements used in an OS Command with root privileges vulnerability exists in the handling of the DDNS configuration. This could allow malicious local administrators to issue commands on system level after a successful IP address update.
- CVE-2023-44373: (Improper Input Validation Vulnerability in Siemens SCALANCE SC-600 Family)
  - Affected devices do not properly sanitize an input field. This could allow an authenticated remote attacker with administrative privileges to inject code or spawn a system root shell.
- CVE-2023-44322: (Unchecked Return Value Vulnerability in Siemens SCALANCE SC-600 Family)
  - Affected devices can be configured to send emails when certain events occur on the device. When presented with an invalid response from the SMTP server, the device triggers an error that disrupts email sending. An attacker with access to the network can use this to do disable notification of users when certain events occur.
- CVE-2023-44321: (Forced Browsing Vulnerability in Siemens SCALANCE SC-600 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-2023-44320: (Forced Browsing Vulnerability in Siemens SCALANCE SC-600 Family)
  - Affected devices do not properly validate the authentication when performing certain modifications in the web interface allowing an authenticated attacker to influence the user interface configured by an administrator.
- CVE-2023-44319: (Use of Weak Hash Vulnerability in Siemens SCALANCE SC-600 Family)
  - Affected devices use a weak checksum algorithm to protect the configuration backup that an administrator can export from the device. This could allow an authenticated attacker with administrative privileges or an attacker that tricks a legitimate administrator to upload a modified configuration file to change the configuration of an affected device.
- CVE-2023-44317: (Data Integrity Vulnerability in Siemens SCALANCE SC-600 Family)
  - 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.
- CVE-2024-21916: (Denial-of-service Vulnerability in Rockwell ControlLogix and GuardLogix Controllers)
  - A denial-of-service vulnerability exists in the affected products, listed above. If exploited, the product could potentially experience a major nonrecoverable fault (MNRF). The device will restart itself to recover from the MNRF.
- CVE-2020-11896: (Ripple20 vulnerability in Siemens SIMATIC RTLS Gateways)
  - The Treck TCP/IP stack on affected devices improperly handles length parameter inconsistencies. Unauthenticated remote attackers may be able to send specially crafted IP packets which could lead to a denial-of-service condition or remote code execution.
- CVE-2023-51440: (TCP Sequence Number Validation Vulnerability in Siemens CP343-1 Devices)
  - Affected products incorrectly validate TCP sequence numbers. This could allow an unauthenticated remote attacker to create a denial-of-service condition by injecting spoofed TCP RST packets.

20240209

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

- **Talos Rules 2024-02-08 (https://www.snort.org/advisories/talos-rules-2024-02-08)**
- **Talos Rules 2024-02-05 (https://www.snort.org/advisories/talos-rules-2024-02-05)**

The new and updated Snort rules span the following categories:

- 3 file-office rules with SIDs 300816, 300815, 300817
- 2 malware-cnc rules with SIDs 62975, 62976
- 1 os-windows rules with SIDs 62948
- 7 server-webapp rules with SIDs 62951, 62950, 62964, 62960, 62961, 62963, 62962

20240202

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

- **Talos Rules 2024-02-01 (https://www.snort.org/advisories/talos-rules-2024-02-01)**
- **Talos Rules 2024-01-30 (https://www.snort.org/advisories/talos-rules-2024-01-30)**

The new and updated Snort rules span the following categories:

- 1 browser-ie rules with SID 62936
- 1 file-other rules with SID 300814
- 1 indicator-compromise rules with SID 62944
- 1 malware-cnc rules with SID 62937
- 1 os-windows rules with SID 62948
- 1 server-mysql rules with SID 3672
- 3 server-other rules with SIDs 62947, 62946, 62945
- 2 server-webapp rules with SIDs 62934, 62935