# Release Notes for Cisco Cyber Vision Knowledge DB

# Release 202406

# 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-4.4.0.ova** | VMWare OVA file, for Center setup |
| **CiscoCyberVision-center-4.4.0.vhdx** | Hyper-V VHDX file, for Center setup |
| **CiscoCyberVision-center-with-DPI-4.4.0.ova** | VMWare OVA file, for Center with DPI setup |
| **CiscoCyberVision-sensor-management-4.4.0.ext** | Sensor Management extension installation file |
| **Sensor** | **Description** |
| **CiscoCyberVision-IOx-aarch64-4.4.0.tar** | Cisco IE3400 and Cisco IR1101 installation and update file |
| **CiscoCyberVision-IOx-IC3K-4.4.0.tar** | Cisco IC3000 sensor installation and update file |
| **CiscoCyberVision-IOx-x86-64-4.4.0.tar** | Cisco Catalyst 9300 installation and update file |
| **CiscoCyberVision-IOx-Active-Discovery-aarch64-4.4.0.tar** | Cisco IE3400 installation and update file, for Sensor with Active Discovery |
| **CiscoCyberVision-IOx-Active-Discovery-x86-64-4.4.0.tar** | Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery |
| **Updates** | **Description** |
| **CiscoCyberVision-Embedded-KDB-4.4.0.dat** | Knowledge DB embedded in Cisco Cyber Vision 4.4.0 |
| **Updates/KDB/KDB.202406** | **Description** |
| **CiscoCyberVision_knowledgedb_20240607.db** | Knowledge DB version 20240607 |
| **CiscoCyberVision_knowledgedb_20240614.db** | Knowledge DB version 20240614 |
| **CiscoCyberVision_knowledgedb_20240621.db** | Knowledge DB version 20240621 |

### 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

## 20240621

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

- **Talos Rules 2024-06-20 (https://www.snort.org/advisories/talos-rules-2024-06-20)**
- **Talos Rules 2024-06-18 (https://www.snort.org/advisories/talos-rules-2024-06-18)**

The new and updated Snort rules span the following categories:

- 1 browser-plugins rule with SID 26182
- 3 server-webapp rules with SIDs 63604, 63599, 63605

## 20240614

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

- **Talos Rules 2024-06-13 (https://www.snort.org/advisories/talos-rules-2024-06-13)**
- **Talos Rules 2024-06-11 (https://www.snort.org/advisories/talos-rules-2024-06-11)**

The new and updated Snort rules span the following categories:

- 36 app-detect rules with SIDs 24397, 26286, 27990, 27992, 32850, 31302, 25981, 32847, 27988, 32848, 27984, 27995, 32851, 27989, 32845, 27982, 28000, 28001, 32846, 27986, 27993, 27991, 27541, 27987, 27983, 27999, 21488, 27998, 27996, 32849, 26287, 27540, 13359, 27985, 27997, 27994
- 2 browser-ie rules with SIDs 300934, 41956
- 4 browser-plugins rules with SIDs 26181, 63575, 26182, 63576
- 2 malware-other rules with SIDs 300935, 300936
- 7 os-windows rules with SIDs 300942, 300939, 63587, 300938, 300937, 300940, 300941
- 4 server-webapp rules with SIDs 63598, 63570, 63571, 63572

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

- CVE-2023-44373: (Injection Vulnerability in Siemens SCALANCE W700 802.11 AX 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-2023-44319: ( Use of Weak Hash Vulnerability in Siemens SCALANCE W700 802.11 AX 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-2023-44318: (Use of Hard-coded Cryptographic Key Vulnerability in Siemens SCALANCE W700 802.11 AX 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-2023-44317: ( Insufficient Verification of Data Authenticity Vulnerability in Siemens SCALANCE W700 802.11 AX 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-2022-46144: (Improper Control of a Resource in Siemens SCALANCE W700 802.11 AX Family)
    - SCALANCE W-700 products are wireless communication devices based on IEEE 802.11ax or 802.11n standard. They are used to connect all to sorts of WLAN devices (Access Points or Clients, depending on the operating mode) with a strong focus on industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs) and others.
- CVE-2024-35292: (Use of Insufficiently Random Values in Siemens SIMATIC S7-200 SMART Devices)
    - SIMATIC S7-200 SMART devices contain an information disclosure vulnerability which leaves the system susceptible to a family of attacks which rely on the use of predictable IP ID sequence numbers as their base method of attack and eventually could allow an attacker to create a denial of service condition.
- CVE-2024-5659: (Multicast Request Causes major nonrecoverable fault on Select Rockwell Controllers)
    - Rockwell Automation was made aware of a vulnerability that causes all affected controllers on the same network to result in a major nonrecoverable fault (MNRF/Assert). This vulnerability could be exploited by sending abnormal packets to the mDNS port. If exploited, the availability of the device would be compromised.

## 20240607

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

- **Talos Rules 2024-06-06 (https://www.snort.org/advisories/talos-rules-2024-06-06)**
- **Talos Rules 2024-06-04 (https://www.snort.org/advisories/talos-rules-2024-06-04)**

The new and updated Snort rules span the following categories:

- 2 browser-chrome rules with SIDs 300933, 300932
- 4 browser-ie rules with SIDs 29671, 35125, 300931, 37571
- 1 file-java rule with SID 300930
- 5 malware-cnc rules with SIDs 63522, 63521, 63523, 63538, 63524

- 1 malware-other rule with SID 63555
- 6 malware-tools rules with SIDs 300926, 300928, 300927, 300929, 300925, 300924
- 1 os-windows rule with SID 40759
- 2 policy-other rules with SIDs 300923, 63533
- 2 server-oracle rules with SIDs 53744, 63527
- 4 server-other rules with SIDs 21248, 63525, 63526, 34889
- 17 server-webapp rules with SIDs 63532, 34879, 34878, 34880, 300913, 63343, 63531, 63530, 63344, 57367, 63528, 63537, 63529, 63558, 63536, 300007, 63559