



# Release Notes for Cisco Cyber Vision Knowledge DB

## Release 202302

<b><i>Compatible device list</i></b> .....	<b>2</b>
<b><i>Links</i></b> .....	<b>2</b>
Software Download .....	2
Related Documentation .....	3
<b><i>Database download</i></b> .....	<b>3</b>
<b><i>How to update the database</i></b> .....	<b>3</b>
<b><i>Release contents</i></b> .....	<b>4</b>
20230224.....	4
20230217.....	4
20230210.....	6
20230203.....	7

## 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-4.1.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.1.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.1.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.1.0.ext	Sensor Management extension installation file
Sensor	Description
CiscoCyberVision-IOx-aarch64-4.1.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.1.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.1.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	Description
CiscoCyberVision-Embedded-KDB-4.1.0.dat	Knowledge DB embedded in Cisco Cyber Vision 4.1.0
Updates/KDB/KDB.202302	Description
CiscoCyberVision_knowledgedb_20230203.db	Knowledge DB version 20230203
CiscoCyberVision_knowledgedb_20230210.db	Knowledge DB version 20230210
CiscoCyberVision_knowledgedb_20230217.db	Knowledge DB version 20230217
CiscoCyberVision_knowledgedb_20230224.db	Knowledge DB version 20230224

## 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](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

### 20230224

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

- **Talos Rules 2023-02-23** (<https://www.snort.org/advisories/talos-rules-2023-02-23>)
  - Talos has added and modified multiple rules in the browser-chrome, file-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2023-02-21** (<https://www.snort.org/advisories/talos-rules-2023-02-21>)
  - Microsoft Talos has added and modified multiple rules in the file-office, file-other, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies

### 20230217

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

- **Talos Rules 2023-02-16** (<https://www.snort.org/advisories/talos-rules-2023-02-16>)
  - Talos has added and modified multiple rules in the file-image, file-other, malware-backdoor, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2023-02-14** (<https://www.snort.org/advisories/talos-rules-2023-02-14>)
  - Microsoft Vulnerability CVE-2023-21529: A coding deficiency exists in Microsoft Exchange Server that may lead to remote code execution.
    - A previously released rule will detect attacks targeting these vulnerabilities and has been updated with the appropriate reference information. It is included in this release and is identified with: Snort2: GID 1, SID 57907, Snort3: GID 1, SID 57907.
  - Microsoft Vulnerability CVE-2023-21688: A coding deficiency exists in NT OS Kernel that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 61312 through 61313, Snort3: GID 1, SID 300416.
  - Microsoft Vulnerability CVE-2023-21689: A coding deficiency exists in Microsoft Protected Extensible Authentication Protocol (PEAP) that may lead to remote code execution.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort3: GID 1, SID 300438.
  - Microsoft Vulnerability CVE-2023-21690: A coding deficiency exists in Microsoft Protected Extensible Authentication Protocol (PEAP) that may lead to remote code execution.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort3: GID 1, SID 300438 through 300439.
  - Microsoft Vulnerability CVE-2023-21706: A coding deficiency exists in Microsoft Exchange Server that may lead to remote code execution.

- A rule to detect attacks targeting this vulnerability is included in this release and is identified with: Snort2: GID 1, SID 61359, Snort3: GID 1, SID 61359.
- Microsoft Vulnerability CVE-2023-21819: A coding deficiency exists in Microsoft Windows Secure Channel that may lead to a Denial of Service (DoS).
  - A rule to detect attacks targeting this vulnerability is included in this release and is identified with: Snort2: GID 1, SID 61357, Snort3: GID 1, SID 61357.
- Microsoft Vulnerability CVE-2023-21823: A coding deficiency exists in Microsoft Graphics Component that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 61314 through 61315, Snort3: GID 1, SID 300417.
- Microsoft Vulnerability CVE-2023-23376: A coding deficiency exists in Microsoft Windows Common Log File System Driver that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 61320 through 61321, Snort3: GID 1, SID 300420.
- Talos also has added and modified multiple rules in the file-other, indicator-compromise, malware-tools, os-windows, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

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

- CVE-2022-33907: (Race Condition Vulnerability in Siemens RUGGEDCOM APE1808 Product Family)
  - DMA transactions which are targeted at input buffers used for the software SMI handler used by the IdeBusDxe driver could cause SMRAM corruption through a TOCTOU attack.
- CVE-2022-33906: (Race Condition Vulnerability in Siemens RUGGEDCOM APE1808 Product Family)
  - DMA transactions which are targeted at input buffers used for the FwBlockServiceSmm software SMI handler could cause SMRAM corruption through a TOCTOU attack
- CVE-2022-33982: (Race Condition Vulnerability in Siemens RUGGEDCOM APE1808 Product Family)
  - DMA attacks on the parameter buffer used by the Int15ServiceSmm software SMI handler could lead to a TOCTOU attack on the SMI handler and lead to corruption of SMRAM.
- CVE-2022-33984: (Race Condition Vulnerability in Siemens RUGGEDCOM APE1808 Product Family)
  - DMA transactions which are targeted at input buffers used for the SdMmcDevice software SMI handler could cause SMRAM corruption through a TOCTOU attack.
- CVE-2022-30774: (Race Condition Vulnerability in Siemens RUGGEDCOM APE1808 Product Family)
  - DMA attacks on the parameter buffer used by the PnpSmm driver could change the contents after parameter values have been checked but before they are used (a TOCTOU attack).
- CVE-2022-21198: (Race Condition Vulnerability in Siemens Industrial Products using Intel CPUs)

- Time-of-check time-of-use race condition in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2022-31243: (Race Condition Vulnerability in Siemens RUGGEDCOM APE1808 Product Family)
  - Update description and links DMA transactions which are targeted at input buffers used for the software SMI handler used by the FvbServicesRuntimeDxe driver could cause SMRAM corruption through a TOCTOU attack.
- CVE-2022-33908: (Race Condition Vulnerability in Siemens RUGGEDCOM APE1808 Product Family)
  - DMA transactions which are targeted at input buffers used for the SdHostDriver software SMI handler could cause SMRAM corruption through a TOCTOU attack.
- CVE-2007-5846: (Improper Input Validation in Siemens SCALANCE X-200IRT Products)
  - Products of the SCALANCE X-200IRT switch family are affected by a denial of service vulnerability in the SNMP agent that could allow remote attackers to cause a denial of service condition.

## 20230210

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

- **Talos Rules 2023-02-09** (<https://www.snort.org/advisories/talos-rules-2023-02-09>)
  - Talos has added and modified multiple rules in the indicator-compromise, malware-cnc, malware-other, malware-tools, os-linux, os-windows and server-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2023-02-06** (<https://www.snort.org/advisories/talos-rules-2023-02-06>)
  - Talos has added and modified multiple rules in the file-image, malware-cnc, malware-other, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

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

- CVE-2022-3086: (Improper Physical Access Control Vulnerability in Moxa UC Series)
  - An attacker with physical access to the device can restart the device and gain access to its BIOS. Then, command line options can be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device authentication files to create a new user profile and gain full access to the system.
- CVE-2022-40693: (Cleartext Transmission of Sensitive Information Vulnerability in Moxa SDS-3008 Series)
  - A cleartext transmission vulnerability exists in the web application functionality of Moxa SDS-3008 Series Industrial Ethernet Switch 2.1. A specially-crafted network sniffing can lead to a disclosure of sensitive information. An attacker can sniff network traffic to trigger this vulnerability.
- CVE-2022-40224: (Insufficient Resource Pool Vulnerability in Moxa SDS-3008 Series)

- A denial-of-service vulnerability exists in the web server functionality of Moxa's SDS-3008 Series Industrial Ethernet switch v2.1. A specially crafted HTTP message header can lead to a denial-of-service attack. An attacker can send an HTTP request to trigger this vulnerability.
- CVE-2022-41311: (Improper Input Validation Vulnerability in Moxa SDS-3008 Series)
  - A stored cross-site scripting vulnerability exists in the web application functionality of Moxa's SDS-3008 Series Industrial Ethernet switch v2.1. A specially crafted HTTP request can lead to arbitrary JavaScript code being executed. An attacker can send an HTTP request to trigger this vulnerability.
- CVE-2022-41312: (Cross-site Scripting Vulnerability in Moxa SDS-3008 Series)
  - A stored cross-site scripting vulnerability exists in the web application functionality of Moxa's SDS-3008 Series Industrial Ethernet switch v2.1. A specially crafted HTTP request can lead to arbitrary JavaScript code being executed. An attacker can send an HTTP request to trigger this vulnerability.
- CVE-2022-41313: (Cross-site Scripting Vulnerability in Moxa SDS-3008 Series)
  - A stored cross-site scripting vulnerability exists in the web application functionality of Moxa SDS-3008 Series Industrial Ethernet Switch 2.1. A specially-crafted HTTP request can lead to arbitrary Javascript execution. An attacker can send an HTTP request to trigger this vulnerability
- CVE-2022-40691: (Information Exposure Vulnerability in Moxa SDS-3008 Series)
  - An information disclosure vulnerability exists in the web application functionality of Moxa's SDS-3008 Series Industrial Ethernet switch v2.1. A specially crafted HTTP request can lead to disclosure of sensitive information. An attacker can send an HTTP request to trigger this vulnerability.

## 20230203

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

- **Talos Rules 2023-02-02** (<https://www.snort.org/advisories/talos-rules-2023-02-02>)
  - Talos has added and modified multiple rules in the indicator-compromise, malware-cnc, malware-tools, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2023-01-31** (<https://www.snort.org/advisories/talos-rules-2023-01-31>)
  - Talos has added and modified multiple rules in the malware-cnc, malware-other, malware-tools and server-webapp rule sets to provide coverage for emerging threats from these technologies.

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

- CVE-2023-20076: (Cisco IOx Application Hosting Environment Command Injection Vulnerability)
  - A vulnerability in the Cisco IOx application hosting environment could allow an authenticated, remote attacker to execute arbitrary commands as root on the underlying host operating system. This vulnerability is due to incomplete sanitization of parameters that are passed in for activation of an application. An attacker could exploit this vulnerability by deploying and activating an application in the Cisco IOx application hosting environment with a crafted activation payload

file. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying host operating system.