Release Notes for Cisco Cyber Vision Knowledge DB

Release 202507

Compatible device list

Center	Description
All version 4 and 5 centers	All Cisco Cyber Vision center version 4 and 5 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-5.2.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.2.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.2.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.2.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.2.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.2.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.2.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.2.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.2.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.2.0.dat	Knowledge DB embedded in Cisco Cyber Vision 5.2.0
Updates/KDB/KDB.202507	**Description**
CiscoCyberVision_knowledgedb_20250704.db	Knowledge DB version 20250704
CiscoCyberVision_knowledgedb_20250711.db	Knowledge DB version 20250711
CiscoCyberVision_knowledgedb_20250718.db	Knowledge DB version 20250718
CiscoCyberVision_knowledgedb_20250725.db	Knowledge DB version 20250725

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

20250725

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

- **Talos Rules 2025-07-24 (https://www.snort.org/advisories/talos-rules-2025-07-24)**
- **Talos Rules 2025-07-21 (https://www.snort.org/advisories/talos-rules-2025-07-21)**

The new and updated Snort rules span the following categories:

- 1 malware-backdoor rule with SID 65183
- 14 malware-cnc rules with SIDs 65187, 65146, 65182, 65145, 65143, 65142, 65147, 65144, 65148, 65151, 65152, 65150, 65149, 65177
- 14 malware-other rules with SIDs 301290, 301291, 301286, 301287, 301281, 301284, 301283, 301280, 301288, 301278, 301282, 301289, 301285, 301279
- 1 os-solaris rule with SID 10136
- 1 policy-other rule with SID 51377
- 1 server-mail rule with SID 65064
- 1 server-other rule with SID 59881
- 8 server-webapp rules with SIDs 65060, 65092, 65184, 65179, 65178, 65066, 58549, 58550

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

- CVE-2023-52236: Use of a Broken or Risky Cryptographic Algorithm Vulnerability in Siemens RUGGEDCOM ROS Devices
  - The affected products support insecure cryptographic algorithms. An attacker could leverage these legacy algorithms to achieve a man-in-the-middle attack or impersonate communicating parties
- CVE-2018-19036: Buffer Overflow Vulnerability in Bosch IP Cameras
  - The vulnerability can be used to remotely execute code on the device (RCE). This would enable a potential attacker, for example, to bypass access restrictions (e.g. username / password) or to reactivate disabled features (e.g. telnet). A necessary prerequisite for this attack is the network access to the webserver (HTTP / HTTPS) of the device. Despite its critical rating, possible attacks are considered incapable of accessing private keys if they are stored on the devices' Trusted Platform Module (TPM). An affected camera can be restored to its original state by the factory reset button
- CVE-2021-23847: Improper Authentication Vulnerability in Bosch IP Cameras
  - A Missing Authentication in Critical Function in Bosch IP cameras allows an unauthenticated remote attacker to extract sensitive information or change settings of the camera by sending crafted requests to the device.

- CVE-2021-23848: Cross-site Scripting Vulnerability in Bosch IP Cameras
  - An error in the URL handler may lead to a reflected cross site scripting (XSS) in the web-based interface. An attacker with knowledge of the camera address can send a crafted link to a user, which will execute javascript code in the context of the user.
- CVE-2021-23849: Cross Site Request Forgery (CSRF) Vulnerability in Bosch IP Cameras
  - A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery). This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera.
- CVE-2021-23850: Buffer Overflow Vulnerability in Recovery Image of Bosch IP Cameras
  - A specially crafted TCP/IP packet may cause a camera recovery image telnet interface to crash. It may also cause a buffer overflow which could enable remote code execution. The recovery image can only be booted with administrative rights or with physical access to the camera and allows the upload of a new firmware in case of a damaged firmware.
- CVE-2021-23851: Buffer Overflow Vulnerability in Recovery Image of Bosch IP Cameras
  - A specially crafted TCP/IP packet may cause the camera recovery image web interface to crash. It may also cause a buffer overflow which could enable remote code execution. The recovery image can only be booted with administrative rights or with physical access to the camera and allows the upload of a new firmware in case of a damaged firmware.
- CVE-2021-23852: Uncontrolled Resource Consumption Vulnerability in Bosch IP Cameras
  - An authenticated attacker with administrator rights can call an URL with an invalid parameter that causes the camera to become unresponsive for a few seconds and cause a Denial of Service (DoS).
- CVE-2021-23853: Improper Input Validation Vulnerability in Bosch IP Cameras
  - Improper validation of the HTTP header allows an attacker to inject arbitrary HTTP headers through crafted URLs.
- CVE-2021-23854: Cross-site Scripting Vulnerability in Bosch IP Cameras
  - An error in the handling of a page parameter may lead to a reflected cross site scripting (XSS) in the web-based interface.
- CVE-2021-3011: Side Channel Key Extraction Vulnerability in Bosch IP Cameras
  - A recently discovered side channel attack for the NXP P5x security microcontrollers was made public. It allows attackers to extract an ECDSA private key after extensive physical access to the chip. The P5x is used as secure certificate storage on Bosch cameras and encoders built on platforms CPP-ENC, CPP3, CPP4, CPP5, CPP6, CPP7 and CPP7.3. Bosch does not include any ECDSA keys from factory, but ECDSA keys can be installed or generated by the customer. Only the private key of the affected camera can be obtained by the attacker.
- CVE-2022-41677: Information Disclosure Vulnerability in Bosch IP Cameras

  - An information disclosure vulnerability was discovered in Bosch IP camera devices allowing an unauthenticated attacker to retrieve information about the device itself (like capabilities) and network settings of the device, disclosing possibly internal network settings if the device is connected to the internet.

- CVE-2023-32229: Uncontrolled Resource Consumption Vulnerability in Bosch IP Cameras
  - Due to an error in the software interface to the secure element chip on the cameras, the chip can be permanently damaged leading to an unusable camera when enabling the Stream security option (signing of the video stream) on Bosch CPP13 and CPP14 cameras. The default setting for this option is "off".
- CVE-2023-39509: Command Injection Vulnerability in Bosch IP Cameras
  - A command injection vulnerability exists in Bosch IP cameras that allows an authenticated user with administrative rights to run arbitrary commands on the OS of the camera.

20250718

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

- **Talos Rules 2025-07-17 (https://www.snort.org/advisories/talos-rules-2025-07-17)**
- **Talos Rules 2025-07-15 (https://www.snort.org/advisories/talos-rules-2025-07-15)**

The new and updated Snort rules span the following categories:

- 2 malware-cnc rules with SIDs 65136, 65124
- 4 malware-other rules with SIDs 301274, 301277, 301273, 301276
- 1 policy-other rule with SID 25977
- 1 server-mail rule with SID 65123
- 8 server-webapp rules with SIDs 65138, 301275, 65137, 65140, 65139, 65127, 65141, 65075

20250711

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

- **Talos Rules 2025-07-10 (https://www.snort.org/advisories/talos-rules-2025-07-10)**
- **Talos Rules 2025-07-08 (https://www.snort.org/advisories/talos-rules-2025-07-08)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 65122
- 2 file-office rules with SIDs 301114, 301268

- 1 os-linux rule with SID 301267
- 8 os-windows rules with SIDs 65105, 65106, 65104, 301272, 301270, 301191, 301271, 301269
- 1 policy-other rule with SID 65119
- 2 server-mssql rules with SIDs 65102, 65103
- 1 server-other rule with SID 64788
- 12 server-webapp rules with SIDs 65092, 65093, 65120, 65117, 65118, 65114, 65107, 65116, 65115, 65121, 65109, 65108

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

- CVE-2023-52236: Use of a Broken or Risky Cryptographic Algorithm Vulnerability in Siemens RUGGEDCOM ROS Devices
  - The affected products support insecure cryptographic algorithms. An attacker could leverage these legacy algorithms to achieve a man-in-the-middle attack or impersonate communicating parties
- CVE-2025-24002: Improper Input Validation Vulnerability in Phoenix Contact CHARX SEC-3xxx charging controllers
  - An unauthenticated remote attacker can use MQTT messages to crash a service on charging stations complying with German Calibration Law, resulting in a temporary denial-of-service for these stations until they got restarted by the watchdog.
- CVE-2025-24003: Buffer Overflow Vulnerability in Phoenix Contact CHARX SEC-3xxx charging controllers
  - An unauthenticated remote attacker can use MQTT messages to trigger out-of-bounds writes in charging stations complying with German Calibration Law, resulting in a loss of integrity for only EichrechtAgents and potential denial-of-service for these stations.
- CVE-2025-24004: Buffer Overflow Vulnerability in Phoenix Contact CHARX SEC-3xxx charging controllers
  - A physical attacker with access to the device display via USB-C can send a message to the device which triggers an unsecure copy to a buffer resulting in loss of integrity and a temporary denial-of-service for the stations until they got restarted by the watchdog.
- CVE-2025-24005: Improper Input Validation Vulnerability in Phoenix Contact CHARX SEC-3xxx charging controllers
  - A local attacker with a local user account can leverage a vulnerable script via SSH to escalate privileges to root due to improper input validation.
- CVE-2025-24006: Improper Privilege Management Vulnerability in Phoenix Contact CHARX SEC-3xxx charging controllers
  - A low privileged local attacker can leverage insecure permissions via SSH on the affected devices to escalate privileges to root.

- CVE-2025-25268: Missing Authentication for Critical Function Vulnerability in Phoenix Contact CHARX SEC-3xxx charging controllers
  - An unauthenticated adjacent attacker can modify configuration by sending specific requests to an API endpoint resulting in read and write access due to missing authentication.
- CVE-2025-25269: Missing Authentication for Critical Function Vulnerability in Phoenix Contact CHARX SEC-3xxx charging controllers
  - An unauthenticated local attacker can inject a command that is subsequently executed as root, leading to a privilege escalation.
- CVE-2025-25270: Improper Control of Resources Vulnerability in Phoenix Contact CHARX SEC-3xxx charging controllers
  - An unauthenticated remote attacker can alter the device configuration in a way to get remote code execution as root with specific configurations.
- CVE-2025-25271: Improper Initialization Vulnerability in Phoenix Contact CHARX SEC-3xxx charging controllers
  - An unauthenticated adjacent attacker is able to configure a new OCPP backend, due to insecure defaults for the configuration interface.
- CVE-2025-40593: Denial of Service Vulnerability in Siemens SIMATIC CN 4100
  - The affected application allows to control the device by storing arbitrary files in the SFTP folder of the device. This could allow an attacker to cause a denial of service condition.
- CVE-2025-40742: Sensitive Data Exposure Vulnerability in Siemens SIPROTEC 5 Devices
  - A sensitive data exposure vulnerability in SIPROTEC 5 can allow an attacker to retrieve sensitive session data from browser history, logs, or other storage mechanisms, potentially leading to unauthorized access.
- CVE-2025-41222: Improper Handling of Exceptional Conditions Vulnerability in Siemens RUGGEDCOM ROS Devices
  - Affected devices do not properly handle malformed TLS handshake messages. This could allow an attacker with network access to the webserver to cause a denial of service resulting in the web server and the device to crash.
- CVE-2025-41223: Use of a Broken or Risky Cryptographic Algorithm Vulnerability in Siemens RUGGEDCOM ROS Devices
  - The affected devices support the TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 cipher suite, which uses CBC (Cipher Block Chaining) mode that is known to be vulnerable to timing attacks. This could allow an attacker to compromise the integrity and confidentiality of encrypted communications.
- CVE-2025-41224: Protection Mechanism Failure Vulnerability in Siemens RUGGEDCOM ROS Devices

  - The affected products do not properly enforce interface access restrictions when changing from management to non-management interface configurations until a system reboot occurs, despite configuration being saved. This could allow an attacker with network access and credentials to gain access to device through non-management and maintain SSH access to the device until reboot.

20250704

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

  - **Talos Rules 2025-07-03 (https://www.snort.org/advisories/talos-rules-2025-07-03)**
  - **Talos Rules 2025-07-01 (https://www.snort.org/advisories/talos-rules-2025-07-01)**

The new and updated Snort rules span the following categories:

- 1 browser-other rule with SID 301264
- 2 malware-backdoor rules with SIDs 301263, 301262
- 2 malware-other rules with SIDs 301265, 301266
- 2 netbios rules with SIDs 46637, 16418
- 7 server-webapp rules with SIDs 44454, 65082, 65084, 65083, 65086, 65085, 65087