Release Notes for Cisco Cyber Vision Knowledge DB

Release 202605

Compatible device list *2*

Links *2*

Software Download **2**

Related Documentation **3**

Database download *3*

How to update the database *3*

Release contents *4*

20260529 ..... **4**

Snort rules 4

Vendor Database 4

20260522 ..... **4**

Snort rules 4

20260519 ..... **5**

Snort rules 5

Vulnerabilities 5

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-5.4.2.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.4.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.4.2.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.4.2.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.4.2.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.4.2.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.4.2.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.4.2.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.4.2.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.4.2.dat	Knowledge DB embedded in Cisco Cyber Vision 5.4.2
Updates/KDB/KDB.202605	**Description**
CiscoCyberVision_knowledgedb_20260519.db	Knowledge DB version 20260519
CiscoCyberVision_knowledgedb_20260522.db	Knowledge DB version 20260522
CiscoCyberVision_knowledgedb_20260529.db	Knowledge DB version 20260529

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

20260529

Snort rules

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

- **Talos Rules 2026-05-28 (https://www.snort.org/advisories/talos-rules-2026-05-28)**
- **Talos Rules 2026-05-26 (https://www.snort.org/advisories/talos-rules-2026-05-26)**

The new and updated Snort rules span the following categories:

- 1 browser-ie rule with SIDs 35170
- 5 malware-cnc rules with SIDs 10, 3, 6, 9, 13
- 2 os-linux rules with SIDs 301512, 301510
- 6 server-webapp rules with SIDs 66517, 66524, 301511, 66518, 66519, 66520

Vendor Database

The new UI in Cyber Vision relies on a vendor database included in this Knowledge Base to represent physical assets and give them a type. This release improves support for assets from Schneider.

20260522

Snort rules

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

- **Talos Rules 2026-05-21 (https://www.snort.org/advisories/talos-rules-2026-05-21)**
- **Talos Rules 2026-05-19 (https://www.snort.org/advisories/talos-rules-2026-05-19)**

The new and updated Snort rules span the following categories:

- 6 file-other rules with SIDs 66500, 66499, 66496, 66495, 66497, 66498
- 2 file-pdf rules with SIDs 66494, 66493
- 1 policy-other rule with SID 66503
- 1 server-other rule with SID 66482
- 11 server-webapp rules with SIDs 66501, 66487, 66504, 66490, 66437, 66502, 301509, 301508, 66506, 66505, 66492

20260519

Snort rules

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

- **Talos Rules 2026-05-14 (https://www.snort.org/advisories/talos-rules-2026-05-14)**
- **Talos Rules 2026-05-12 (https://www.snort.org/advisories/talos-rules-2026-05-12)**
- **Talos Rules 2026-05-07 (https://www.snort.org/advisories/talos-rules-2026-05-07)**
- **Talos Rules 2026-05-05 (https://www.snort.org/advisories/talos-rules-2026-05-05)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 301498
- 1 browser-firefox rule with SID 301499
- 2 file-office rules with SIDs 301503, 301506
- 6 malware-cnc rules with SIDs 66432, 66408, 301491, 66433, 66400, 301493
- 4 os-other rules with SIDs 66407, 66406, 66411, 66412
- 10 os-windows rules with SIDs 301501, 301505, 66476, 301495, 301494, 301496, 301502, 301500, 301504, 301497
- 2 policy-other rules with SIDs 66467, 66466
- 3 server-other rules with SIDs 27264, 66483, 66482
- 53 server-webapp rules with SIDs 66413, 66426, 66416, 66417, 66418, 66415, 66419, 64071, 66414, 66405, 65983, 66424, 66437, 66480, 66472, 66473, 301507, 65538, 66463, 66423, 66428, 37890, 65569, 66446, 66422, 66425, 66464, 66421, 66420, 66481, 65568, 66436, 66479, 66465, 66485, 66469, 66462, 66468, 66461, 66484, 66486, 66404, 62779, 66402, 62781, 66427, 66403, 66435, 66429, 66401, 62780, 62782, 66434

Vulnerabilities

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

- CVE-2022-4046: Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability in ABB MV Drives
    - The CODESYS Control runtime system does not restrict the memory access. An improper restriction of operations within the bounds of a memory buffer allows an attacker with access to the drive with user privileges to gain full access of the drive.
- CVE-2023-37545: Improper Input Validation Vulnerability in ABB MV Drives

    - In multiple CODESYS products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition.

- CVE-2023-37546: Improper Input Validation Vulnerability in ABB MV Drives
    - In multiple CODESYS products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2023-37547: Improper Input Validation Vulnerability in ABB MV Drives
    - In multiple CODESYS products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2023-37548: Improper Input Validation Vulnerability in ABB MV Drives
    - In multiple CODESYS products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2023-37549: Improper Input Validation Vulnerability in ABB MV Drives
    - In multiple CODESYS products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2023-37550: Improper Input Validation Vulnerability in ABB MV Drives
    - In multiple CODESYS products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2023-37552: Improper Input Validation Vulnerability in ABB MV Drives
    - In multiple versions of multiple CODESYS products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2023-37553: Improper Input Validation Vulnerability in ABB MV Drives
    - In multiple versions of multiple CODESYS products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP

component to read internally from an invalid address, potentially leading to a denial-of-service condition.

- CVE-2023-37554: Improper Input Validation Vulnerability in ABB MV Drives
    - In multiple versions of multiple CODESYS products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2023-37555: Improper Input Validation Vulnerability in ABB MV Drives
    - In multiple versions of multiple CODESYS products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2023-37556: Improper Input Validation Vulnerability in ABB MV Drives
    - In multiple versions of multiple CODESYS products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2023-37557: Out-of-bounds Write Vulnerability in ABB MV Drives
    - After successful authentication as a user in multiple CODESYS products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition.
- CVE-2023-37558: Improper Input Validation Vulnerability in ABB MV Drives
    - After successful authentication as a user in multiple CODESYS products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2023-37559: Improper Input Validation Vulnerability in ABB MV Drives
    - After successful authentication as a user in multiple CODESYS products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2024-54017: Small Space of Random Values Vulnerability in Siemens Session Identifier Vulnerability in SIPROTEC 5
    - Affected devices do not use sufficiently random values to create session identifiers. This could allow an unauthenticated remote attacker to brute force a session identifier and gain read access to limited information from the web server without authorization.
- CVE-2025-40833: NULL Pointer Dereference Vulnerability in Siemens Industrial Devices

  - The affected devices contain a null pointer dereference vulnerability while processing specially crafted IPv4 requests. This could allow an attacker to cause denial of service condition. A manual restart is required to recover the system.

- CVE-2025-40947: OS Command Injection Vulnerability in Siemens Ruggedcom Rox
  - Affected devices do not properly sanitize user-supplied input during the feature key installation process. This could allow an authenticated remote attacker to inject arbitrary commands, resulting in remote code execution with root privileges on the underlying operating system.
- CVE-2025-40948: Argument Injection Vulnerability in Siemens Ruggedcom Rox
  - Affected devices do not properly validate input in the web server's JSON-RPC interface. This could allow an authenticated remote attacker to read arbitrary files from the underlying operating system's filesystem with root privileges.
- CVE-2025-40949: OS Command Injection Vulnerability in Siemens Ruggedcom Rox
  - Affected devices do not properly sanitize user-supplied input in the Scheduler functionality of the Web UI, allowing commands to be injected into the task scheduling backend. This could allow an authenticated remote attacker to execute arbitrary commands with root privileges on the underlying operating system.
- CVE-2026-22924: Missing Authentication for Critical Function Vulnerability in Siemens SIMATIC CN 4100
  - The affected application does not properly restrict unauthenticated connections and is susceptible to resource exhaustion conditions. This could allow an attacker to disrupt normal operations or perform unauthorized actions, potentially impacting system availability and integrity.
- CVE-2026-22925: Allocation of Resources Without Limits or Throttling Vulnerability in Siemens SIMATIC CN 4100
  - The affected application is susceptible to resource exhaustion when subjected to high volume of TCP SYN packets. This could allow an attacker to render the service unavailable and cause denial-of-service conditions by overwhelming system resources.
- CVE-2026-25786: Cross-site Scripting Vulnerability in Siemens SIMATIC S7 PLCs Web Server
  - Affected devices do not properly validate and sanitize PLC/station name rendered on the "communication" parameters page of the web interface. This could allow an authenticated attacker who is authorized to download a TIA project into the product, to inject malicious scripts into the page. If a benign user with appropriate rights accesses the "communication" parameters page, the malicious code would be executed in the scope of their web session.
- CVE-2026-25787: Cross-site Scripting Vulnerability in Siemens SIMATIC S7 PLCs Web Server
  - Affected devices do not properly validate and sanitize Technology Object (TO) name rendered on the "Motion Control Diagnostics" page of the web interface. This could allow an authenticated attacker who is authorized to download a TIA project into the product, to inject malicious scripts into the page. If a benign user with appropriate rights accesses the "Motion Control Diagnostics" parameters page, the malicious code would be executed in the scope of their web session.

- CVE-2026-25789: Cross-site Scripting Vulnerability in Siemens SIMATIC S7 PLCs Web Server
    - Affected devices do not properly validate and sanitize filenames on the Firmware Update page. This could allow a remote attacker to social engineer the user into selecting the modified firmware file to be uploaded. This would result in malitcious JavaScript execution in the context of the authenticated user's session without requiring the file to be uploaded, potentially leading to session hijacking or credential theft.
- CVE-2026-27662: Initialization of a Resource with an Insecure Default Vulnerability in Siemens SIMATIC HMI Unified Comfort
    - Affected devices do not properly restrict access to the web browser via the Control Panel when no corresponding security mechanisms are in place. This could allow an unauthenticated attacker to gain unauthorized access to the web browser, potentially enabling the discovery of backdoors, performing unauthorized actions, or exploiting misconfigurations that may lead to further system compromise.
- CVE-2026-4827: Insufficient Entropy Vulnerability in Schneider Electric EcoStruxure Panel Server
    - Schneider Electric is aware of vulnerabilities in its PowerChute™ Serial Shutdown product. The [PowerChute Serial Shutdown](https://www.se.com/ww/en/product-range/137943580-powerchute-serial-shutdown/#products) product is a UPS management software enabling graceful system shutdown and energy management capabilities for desktop, servers and workstations. Failure to apply the remediation provided below may risk improper input validation which could result in disruption of operations and access to system data.
- CVE-2026-6866: Initialization of a Resource with an Insecure Default Vulnerability in Schneider Electric EcoStruxure Panel Server
    - Schneider Electric is aware of its vulnerability in its EcoStruxure Panel Server offer. The EcoStruxure Panel Server is a high performance, modular gateway with enhanced cybersecurity that provides easy and fast connections to multiple concurrent edge control or cloud applications. Failure to apply the remediations provided below may risk unauthorized authentication, which could lead to access to sensitive information.