# Release Notes for Cisco Cyber Vision Knowledge DB

# Release 202609


*Compatible device list* ..... 1

*Links* ..... 2

**Software Download** ..... 2

**Related Documentation** ..... 2

*Database download* ..... 3

*How to update the database* ..... 3

*Release contents* ..... 3

**20260924** ..... 4

Snort rules ..... 4

**20260918** ..... 4

Snort rules ..... 4

**20260911** ..... 4

Snort rules ..... 4

**20260904** ..... 5

Snort rules ..... 5

Vendor Database ..... 5

Vulnerabilities ..... 6

# 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-5.5.2.ova** | VMWare OVA file, for Center setup |
| **CiscoCyberVision-center-5.5.2.vhdx** | Hyper-V VHDX file, for Center setup |
| **CiscoCyberVision-center-with-DPI-5.5.2.ova** | VMWare OVA file, for Center with DPI setup |
| **CiscoCyberVision-sensor-management-5.5.2.ext** | Sensor Management extension installation file |
| **Sensor** | **Description** |
| **CiscoCyberVision-IOx-aarch64-5.5.2.tar** | Cisco IE3400 and Cisco IR1101 installation and update file |
| **CiscoCyberVision-IOx-IC3000-5.5.2.tar** | Cisco IC3000 sensor installation and update file |
| **CiscoCyberVision-IOx-x86-64-5.5.2.tar** | Cisco Catalyst 9300 installation and update file |
| **CiscoCyberVision-IOx-Active-Discovery-aarch64-5.5.2.tar** | Cisco IE3400 installation and update file, for Sensor with Active Discovery |
| **CiscoCyberVision-IOx-Active-Discovery-x86-64-5.5.2.tar** | Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery |
| **Updates** | **Description** |
| **CiscoCyberVision-Embedded-KDB-5.5.2.dat** | Knowledge DB embedded in Cisco Cyber Vision 5.5.2 |
| **Updates/KDB/KDB.202609** | **Description** |
| **CiscoCyberVision_knowledgedb_20260904.db** | Knowledge DB version 20260904 |
| **CiscoCyberVision_knowledgedb_20260911.db** | Knowledge DB version 20260911 |
| **CiscoCyberVision_knowledgedb_20260918.db** | Knowledge DB version 20260918 |
| **CiscoCyberVision_knowledgedb_20260924.db** | Knowledge DB version 20260924 |

## 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

## 20260924

### Snort rules

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

- **Talos Rules 2026-09-22 (https://www.snort.org/advisories/talos-rules-2026-09-22)**

The new and updated Snort rules span the following categories:

- 1 server-mail rules with SIDs 67136
- 1 server-other rules with SIDs 67152
- 16 server-webapp rules with SIDs 67147, 67148, 67138, 67139, 67145, 67137, 67146, 67142, 67143, 67140, 67141, 67144, 67129, 67151, 67150, 67149

## 20260918

### Snort rules

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

- **Talos Rules 2026-09-17 (https://www.snort.org/advisories/talos-rules-2026-09-17)**
- **Talos Rules 2026-09-15 (https://www.snort.org/advisories/talos-rules-2026-09-15-9-16-2026)**
- **Talos Rules 2026-09-15 (https://www.snort.org/advisories/talos-rules-2026-09-15)**

The new and updated Snort rules span the following categories:

- 1 malware-other rules with SIDs 29
- 2 os-linux rules with SIDs 301661, 301660
- 1 server-mssql rules with SIDs 67123
- 2 server-other rules with SIDs 67110, 67109
- 27 server-webapp rules with SIDs 67126, 67102, 67104, 67103, 67127, 67120, 67113, 67128, 67135, 67114, 67118, 67129, 67119, 67112, 67125, 67115, 67124, 67132, 67134, 67131, 67133, 67117, 67121, 67116, 60856, 67130, 67122

## 20260911

### Snort rules

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

- **Talos Rules 2026-09-10 (https://www.snort.org/advisories/talos-rules-2026-09-10)**
- **Talos Rules 2026-09-08 (https://www.snort.org/advisories/talos-rules-2026-09-08)**

The new and updated Snort rules span the following categories:

- 6 browser-webkit rules with SIDs 67095, 67098, 67096, 67097, 67094, 67099
- 1 malware-other rules with SIDs 301630
- 2 netbios rules with SIDs 67101, 67100
- 41 os-windows rules with SIDs 301658, 301623, 301655, 301632, 301650, 301619, 301647, 301624, 301622, 301621, 301640, 301652, 301645, 301642, 301635, 301656, 301638, 301634, 301654, 301620, 301639, 301646, 301625, 301636, 67046, 301643, 301629, 301626, 67091, 301627, 301648, 301644, 301641, 301649, 301659, 301651, 301633, 301653, 301637, 301657, 301628
- 1 server-other rules with SIDs 66972
- 2 server-webapp rules with SIDs 67033, 301631

## 20260904

### Snort rules

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

- **Talos Rules 2026-09-03 (https://www.snort.org/advisories/talos-rules-2026-09-03)**
- **Talos Rules 2026-09-01 (https://www.snort.org/advisories/talos-rules-2026-09-01)**

The new and updated Snort rules span the following categories:

- 1 indicator-compromise rules with SID 67007
- 1 malware-other rules with SID 301618
- 1 server-apache rules with SID 66996
- 7 server-other rules with SIDs 67004, 67001, 66997, 67000, 66998, 67005, 67010
- 6 server-webapp rules with SIDs 67002, 67003, 301616, 301617, 67006, 66999

### 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 Lenze.

## Vulnerabilities

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

- CVE-2026-20212: Cisco Nexus 9000 Series Switches Silicon One Remote Code Execution Vulnerability
  - Crafted input sent through exposed TCP ports 43210 or 43211 can enable remote code execution with root privileges or cause a device reload.
- CVE-2026-20274: Improper Control of a Resource Through Its Lifetime Vulnerability in Cisco IOS XR Software
  - Multiple resource-lifetime issues can cause memory corruption, resource exhaustion, or code execution.
- CVE-2026-20275: Incorrect Calculation Vulnerability in Cisco IOS XR Software
  - Incorrect buffer-size calculations and integer overflows can affect confidentiality, integrity, and availability.
- CVE-2026-20276: Insufficient Control Flow Management Vulnerability in Cisco IOS XR Software
  - Reachable assertions and loops with unreachable exit conditions can cause a denial of service.
- CVE-2026-20277: Protection Mechanism Failure Vulnerability in Cisco IOS XR Software
  - Insufficiently random values can be exploited over the network to cause a denial of service.
- CVE-2026-20278: Improper Neutralization Vulnerability in Cisco IOS XR Software
  - Improper neutralization and input validation can allow a low-privileged remote attacker to compromise the system.
- CVE-2026-20279: Improper Access Control Vulnerability in Cisco IOS XR Software
  - Authentication, authorization, and certificate-validation weaknesses can expose protected functionality.
- CVE-2026-20280: Improper Check or Handling of Exceptional Conditions Vulnerability in Cisco IOS XR Software
  - Length inconsistencies and insecure failure handling can allow a low-privileged remote attacker to compromise the system.
- CVE-2016-9343: Stack-Based Buffer Overflow Vulnerability in Rockwell Logix5000 Controllers
  - Malformed CIP packets can overflow a stack buffer, enabling code execution or causing a denial of service.
- CVE-2024-6077: Crafted CIP Message Denial-of-Service Vulnerability in Rockwell Logix Controllers and 1756-EN4 Modules
  - Specially crafted packets sent to the CIP Security Object can make the device unavailable and require a factory reset.
- CVE-2024-8626: Denial-of-Service Vulnerability in Rockwell Logix Controllers and 1756-EN4TR Modules

    - Repeated actions on certain product web pages can exploit a memory leak, making affected products unavailable until power-cycled.
- CVE-2025-8007: Concurrent Forward Close Denial-of-Service Vulnerability in Rockwell 1756-EN4TR and 1756-EN4TRXT Modules
    - A Concurrent Forward Close operation can trigger a major non-recoverable fault and cause unexpected system crashes.
- CVE-2026-19471: Stored Cross-Site Scripting Vulnerability in Rockwell Automation ArmorStart LT
    - Unsanitized input can be stored on the server and executed in another user's browser.
- CVE-2026-19472: Denial-of-Service Vulnerability in Rockwell Automation ArmorStart LT
    - A crafted HTTP PUT request can cause the embedded web server to become unavailable.
- CVE-2026-9637: Denial-of-Service Vulnerability in Rockwell Automation 5380 and 5580 Logix Controllers
    - Improper input-length validation during CIP processing can cause a major non-recoverable fault requiring a power cycle.
- CVE-2021-42260: Denial-of-Service Vulnerability in Rockwell Automation Logix Controllers
    - Corrupt crafted data can trigger a major non-recoverable fault and require a reset or program download for recovery.
- CVE-2026-84235: Denial-of-Service Vulnerability in Rockwell Automation 1756-ENBT Module
    - A crafted CIP packet can crash the module; migration to a supported module is recommended because no corrected firmware is available.
- PVT-2026-00008: Improper Input Validation Vulnerability in CID File Processing on Schweitzer Engineering Laboratories SEL-400 Series Relays
    - A maliciously crafted CID file can disable affected SEL-400 series relays and merging units.