Release Notes for Cisco Cyber Vision Knowledge DB

Release 202606

Compatible device list 2

Links 2

Software Download 2

Related Documentation 3

Database download 3

How to update the database 3

Release contents 4

20260626 4

Snort rules 4

Vulnerabilities 4

20260619 5

Snort rules 5

Vendor Database 5

20260612 5

Snort rules 5

Vulnerabilities 6

20260605 7

Snort rules 7

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-5.5.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.5.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.5.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.5.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.5.1.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.5.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.5.1.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.5.1.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.5.1.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.5.1.dat	Knowledge DB embedded in Cisco Cyber Vision 5.5.1
Updates/KDB/KDB.202606	**Description**
CiscoCyberVision_knowledgedb_20260605.db	Knowledge DB version 20260605
CiscoCyberVision_knowledgedb_20260612.db	Knowledge DB version 20260612
CiscoCyberVision_knowledgedb_20260619.db	Knowledge DB version 20260619
CiscoCyberVision_knowledgedb_20260626.db	Knowledge DB version 20260626

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

20260626

Snort rules

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

- **Talos Rules 2026-06-25 (https://www.snort.org/advisories/talos-rules-2026-06-25)**
- **Talos Rules 2026-06-23 (https://www.snort.org/advisories/talos-rules-2026-06-23)**

The new and updated Snort rules span the following categories:

- 2 browser-chrome rules with SIDs 66673, 66672
- 2 os-windows rules with SIDs 301544, 66678
- 1 policy-other rule with SID 62837
- 1 server-mail rule with SID 66674
- 2 server-other rules with SIDs 66670, 66671
- 8 server-webapp rules with SIDs 66669, 66675, 66676, 65439, 66679, 66154, 62621, 66677

Vulnerabilities

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

- CVE-2025-11694: Improper Validation of Integrity Check Value Vulnerability in Rockwell Automation CompactLogix 5370 Controllers
  - A denial-of-service vulnerability exists in 1769 CompactLogix 5370 controllers due to missing validation of CIP sequence numbers and source IP addresses. Exposed Connection IDs visible on the web interface can be abused to cause a minor fault.
- CVE-2026-0646: Missing Release of Memory after Effective Lifetime Vulnerability in Rockwell Automation FLEX I/O EtherNet/IP Adapters
  - A denial-of-service vulnerability exists in the 1794-AENTR FLEX I/O EtherNet/IP adapter due to improper memory handling of CIP protocol requests. The adapter can fault and lose connection to its I/O modules, requiring a manual reset to recover.
- CVE-2026-0647: Missing Authentication for Critical Function Vulnerability in Rockwell Automation FLEX I/O EtherNet/IP Adapters
  - An improper authentication vulnerability exists in the 1794-AENTR FLEX I/O EtherNet/IP adapter's embedded web server. An unauthenticated attacker can change the web interface password via a crafted HTTP GET request, leading to account takeover and loss of web server availability.

- CVE-2026-11317: Improper Resource Shutdown or Release Vulnerability in Rockwell Automation CompactLogix 5370 and ControlLogix 5570
    - A denial-of-service vulnerability exists in CompactLogix 5370 and ControlLogix 5570 controllers. A crafted CIP message can trigger a major non-recoverable fault (MNRF); controllers with less memory are more likely to be affected. A program download is required to recover.
- CVE-2026-9307: Exposure of Sensitive System Information Vulnerability in Rockwell Automation CompactLogix 5370 Controllers
    - A sensitive information disclosure vulnerability exists in CompactLogix 5370 controllers. The web server exposes CIP Connection IDs on the diagnostics page to unauthenticated network users, which can be leveraged to craft malicious packets for denial-of-service.

20260619

Snort rules

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

- **Talos Rules 2026-06-18 (https://www.snort.org/advisories/talos-rules-2026-06-18)**
- **Talos Rules 2026-06-16 (https://www.snort.org/advisories/talos-rules-2026-06-16)**

The new and updated Snort rules span the following categories:

- 4 browser-chrome rules with SIDs 301543, 66662, 301539, 301538
- 2 malware-cnc rules with SIDs 25, 24
- 1 policy-other rule with SID 66661
- 4 server-other rules with SIDs 66084, 301537, 66663, 66648
- 33 server-webapp rules with SIDs 66642, 66622, 301540, 66625, 66628, 66660, 66630, 66627, 66631, 66624, 66635, 66632, 66621, 66629, 66626, 66659, 66634, 66638, 66633, 66666, 66637, 66639, 66623, 66644, 66636, 66658, 66647, 66641, 66643, 66645, 66646, 66614, 66640

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 Siemens.

20260612

Snort rules

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

- **Talos Rules 2026-06-11 (https://www.snort.org/advisories/talos-rules-2026-06-11)**
- **Talos Rules 2026-06-09 (https://www.snort.org/advisories/talos-rules-2026-06-09)**

The new and updated Snort rules span the following categories:

- 1 app-detect rule with SID 301190
- 1 file-other rule with SID 300063
- 1 indicator-compromise rule with SID 66613
- 4 malware-cnc rules with SIDs 23, 22, 21, 20
- 1 os-linux rule with SID 66591
- 14 os-windows rules with SIDs 301523, 301534, 301529, 301533, 301524, 301532, 66581, 301535, 301527, 301525, 301528, 301531, 66619, 66620
- 1 protocol-other rule with SID 53214
- 1 protocol-rpc rule with SID 66586
- 1 server-mail rule with SID 66592
- 8 server-other rules with SIDs 301530, 66585, 52343, 66593, 301536, 301526, 66618, 58623
- 17 server-webapp rules with SIDs 66570, 50504, 62648, 56551, 301522, 66569, 54583, 66588, 66600, 66583, 66611, 66614, 66584, 66599, 66612, 66587, 66582

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-2025-40808: Unrestricted Upload of File with Dangerous Type Vulnerability in Siemens SIPROTEC 5 Using DIGSI5 Protocol
  - The affected application allows authenticated users to upload arbitrary files using DIGSI 5 protocol. This could allow an attacker to upload malicious configuration files, that could cause denial of service condition and potentially lead to code execution.
- CVE-2026-20171: Cisco Nexus 3000 and 9000 Series Switches Border Gateway Protocol Denial of Service Vulnerability
  - A vulnerability in the Border Gateway Protocol (BGP) enforce-first-as feature of Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, remote attacker to trigger BGP peer flaps, resulting in a denial of service (DoS)

condition. This vulnerability is due to incorrect parsing of a transitive BGP attribute. An attacker could exploit this vulnerability by sending a crafted BGP update through an established BGP peer session. If the update propagates to an affected device, it could cause the device to drop the BGP session and flap with the BGP peer that is forwarding this update, resulting in a DoS condition.

- CVE-2026-9650: Insufficiently Protected Credentials Vulnerability in Schneider EasyLogic T150 and Saitel DP Remote Terminal Unit
    - Insufficiently Protected Credentials vulnerability that could cause unauthorized access and exposure of sensitive information when unauthenticated attacker accesses credentials stored within firmware or system files. With this credential an attacker could subsequently compromise the device if they have physical access to the device.
- CVE-2026-9651: Incorrect Permission Assignment for Critical Resource Vulnerability in Schneider EasyLogic T150 and Saitel DP Remote Terminal Unit
    - Incorrect Permission Assignment for Critical Resource vulnerability that could cause unauthorized disclosure of password hashes and potential account compromise when an attacker with privileged local access reads improperly protected system files.
- CVE-2026-9716: NULL Pointer Dereference Vulnerability in Schneider PowerLogic P7
    - NULL Pointer Dereference vulnerability exists that could cause a denial-of-service condition, rendering the device's HMI and configuration functionality unavailable when malformed requests are received over exposed network interfaces.
- CVE-2026-9717: OS Command Injection Vulnerability in Schneider PowerLogic P7
    - Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that could allow unauthorized execution of commands with elevated privileges, impacting system integrity, confidentiality, and availability when a privileged authenticated user interacts with a vulnerable network-exposed service.
- CVE-2026-9718: Reachable Assertion Vulnerability in Schneider PowerLogic P7
    - Reachable Assertion vulnerability exists that could allow an authenticated attacker to trigger a denial-of-service condition, impacting system availability when a specially crafted request is sent to a vulnerable network-exposed service.

20260605

Snort rules

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

- **Talos Rules 2026-06-04 (https://www.snort.org/advisories/talos-rules-2026-06-04)**
- **Talos Rules 2026-06-02 (https://www.snort.org/advisories/talos-rules-2026-06-02)**

The new and updated Snort rules span the following categories:

- 2 file-identify rules with SIDs 18274, 66560
- 4 file-other rules with SIDs 301514, 301412, 66564, 66563
- 5 malware-cnc rules with SIDs 16, 19, 18, 17, 15
- 1 os-windows rule with SID 301513
- 2 policy-other rules with SIDs 66531, 66530
- 1 server-apache rule with SID 66553
- 1 server-mail rule with SID 65064
- 7 server-other rules with SIDs 66538, 301516, 301515, 65991, 301517, 65992, 301518
- 8 server-webapp rules with SIDs 301519, 301520, 66532, 66561, 66562, 66565, 301521, 66566