



Release Notes for Cisco Cyber Vision Knowledge DB

Release 202603

<i>Compatible device list</i>	2
<i>Links</i>	2
Software Download	2
Related Documentation	3
<i>Database download</i>	3
<i>How to update the database</i>	3
<i>Release contents</i>	4
20260327	4
Snort rules	4
20260320	4
Snort rules	4
20260313	5
Snort rules	5
Vendor Database	5
Vulnerabilities	5
20260306	7
Snort rules	7
Vendor Database	8

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-5.4.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.4.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.4.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.4.1.ext	Sensor Management extension installation file
Sensor	Description
CiscoCyberVision-IOx-aarch64-5.4.1.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.4.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.4.1.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.4.1.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.4.1.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	Description
CiscoCyberVision-Embedded-KDB-5.4.1.dat	Knowledge DB embedded in Cisco Cyber Vision 5.4.1
Updates/KDB/KDB.202603	Description
CiscoCyberVision_knowledgedb_20260306.db	Knowledge DB version 20260306
CiscoCyberVision_knowledgedb_20260313.db	Knowledge DB version 20260313
CiscoCyberVision_knowledgedb_20260320.db	Knowledge DB version 20260320
CiscoCyberVision_knowledgedb_20260327.db	Knowledge DB version 20260327

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

20260327

Snort rules

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

- **Talos Rules 2026-03-26** (<https://www.snort.org/advisories/talos-rules-2026-03-26>)
- **Talos Rules 2026-03-24** (<https://www.snort.org/advisories/talos-rules-2026-03-24>)

The new and updated Snort rules span the following categories:

- 4 file-image rules with SIDs 66177, 66175, 66176, 66178
- 5 malware-cnc rules with SIDs 66170, 66172, 66174, 66167, 66171
- 2 malware-other rules with SIDs 301455, 301456
- 2 malware-tools rules with SIDs 301458, 301457
- 1 netbios rule with SID 24973
- 1 policy-other rule with SID 65876
- 2 protocol-dns rules with SIDs 21354, 21355
- 3 server-other rules with SIDs 41548, 31361, 59880
- 20 server-webapp rules with SIDs 65619, 66155, 66162, 66179, 65517, 66184, 66164, 66159, 301454, 66156, 66154, 65586, 66161, 66160, 66166, 66188, 65518, 66163, 66165, 66187

20260320

Snort rules

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

- **Talos Rules 2026-03-19** (<https://www.snort.org/advisories/talos-rules-2026-03-19>)
- **Talos Rules 2026-03-17** (<https://www.snort.org/advisories/talos-rules-2026-03-17>)

The new and updated Snort rules span the following categories:

- 4 file-image rules with SIDs 66131, 66132, 66133, 66134
- 1 file-other rule with SID 301451
- 1 malware-other rule with SID 301450
- 2 server-other rules with SIDs 301449, 301452

- 2 server-samba rules with SIDs 66130, 66129
- 20 server-webapp rules with SIDs 66146, 66135, 66136, 66149, 301453, 66144, 66150, 66143, 66126, 66145, 66123, 66147, 66139, 66148, 66151, 66152, 66153, 66142, 66141, 66140

20260313

Snort rules

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

- **Talos Rules 2026-03-12** (<https://www.snort.org/advisories/talos-rules-2026-03-12>)
- **Talos Rules 2026-03-10** (<https://www.snort.org/advisories/talos-rules-2026-03-10>)

The new and updated Snort rules span the following categories:

- 6 file-image rules with SIDs 66122, 66100, 66120, 66121, 66119, 66099
- 3 file-other rules with SIDs 300156, 300161, 300151
- 2 malware-cnc rules with SIDs 66118, 2
- 2 malware-other rules with SIDs 301447, 301448
- 5 os-windows rules with SIDs 301444, 301443, 301442, 301446, 301445
- 2 policy-other rules with SIDs 66086, 66085
- 1 protocol-other rule with SID 66112
- 4 server-other rules with SIDs 66084, 66106, 66105, 66107
- 14 server-webapp rules with SIDs 66115, 65388, 66088, 66098, 66113, 66087, 66116, 66114, 65387, 66094, 66093, 66117, 61367, 66095

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 SICK.

Vulnerabilities

This release adds support for the detection of vulnerabilities on Festo and Inductive Automation products:

- CVE-2025-13901: Improper Resource Shutdown or Release in Multiple Schneider Products (Modicon M241/M251/M262)
 - Schneider Electric is aware of a vulnerability in its Modicon Controllers M241 / M251, and M262 products. Failure to apply the remediation may risk Denial of Service attack which could result in loss of availability of the controller (CWE-404).

- CVE-2025-13902: Improper Neutralization in Multiple Schneider Products (Modicon M241/M251/M258, LMC058)
 - Schneider Electric is aware of a vulnerability in its Modicon Controllers M241 / M251, M258, and LMC058 products. Failure to apply the remediation or mitigations may risk a Cross-site Scripting or an open redirect attack which could result in an account takeover scenario or the execution of code in the user browser (CWE-79).
- CVE-2025-40943: Cross-site Scripting Vulnerability in Siemens SIMATIC S7-1500
 - SIMATIC S7-1500 devices contain a vulnerability that could allow an attacker to inject code by tricking a legitimate user into importing a specially crafted trace file in the web interface. Affected devices do not properly sanitize contents of trace files (CWE-79: Cross-site Scripting).
- CVE-2026-20010: Cisco NX-OS Software Link Layer Discovery Protocol Denial of Service Vulnerability
 - A vulnerability in the Link Layer Discovery Protocol (LLDP) feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause the LLDP process to restart, which could cause an affected device to reload unexpectedly. This vulnerability is due to improper handling of specific fields in an LLDP frame. An attacker could exploit this vulnerability by sending a crafted LLDP packet to an interface of an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition.
- CVE-2026-20040: Cisco IOS XR Software CLI Privilege Escalation Vulnerabilities
 - Multiple vulnerabilities in Cisco IOS XR Software could allow an authenticated, local attacker to execute commands as root on an underlying operating system or gain full administrative control of an affected device.
- CVE-2026-20046: Cisco IOS XR Software CLI Privilege Escalation Vulnerabilities
 - Multiple vulnerabilities in Cisco IOS XR Software could allow an authenticated, local attacker to execute commands as root on an underlying operating system or gain full administrative control of an affected device.
- CVE-2026-20051: Cisco Nexus 3600 and 9500-R Series Switching Platforms Layer 2 Loop Denial of Service Vulnerability
 - A vulnerability with the Ethernet VPN (EVPN) Layer 2 ingress packet processing of Cisco Nexus 3600 Platform Switches and Cisco Nexus 9500-R Series Switching Platforms could allow an unauthenticated, adjacent attacker to trigger a Layer 2 traffic loop. This vulnerability is due to a logic error when processing a crafted Layer 2 ingress frame. An attacker could exploit this vulnerability by sending a stream of crafted Ethernet frames through the targeted device. A successful exploit could allow the attacker to cause a Layer 2 Virtual eXtensible LAN (VxLAN) traffic loop, which, in turn, could result in a denial of service (DoS) condition. This Layer 2 loop could oversubscribe the bandwidth on network interfaces, which would result in all data plane traffic being dropped. To exploit this vulnerability, the attacker must be Layer 2-adjacent to the affected device.
- CVE-2026-20074: Cisco IOS XR Software Multi-Instance Intermediate System-to-Intermediate System Denial of Service Vulnerability

- A vulnerability in the Intermediate System-to-Intermediate System (IS-IS) multi-instance routing feature of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause the IS-IS process to restart unexpectedly. This vulnerability is due to insufficient input validation of ingress IS-IS packets. An attacker could exploit this vulnerability by sending crafted IS-IS packets to an affected device after forming an adjacency. A successful exploit could allow the attacker to cause the IS-IS process to restart unexpectedly, resulting in a temporary loss of connectivity to advertised networks and a denial of service (DoS) condition.
- CVE-2026-20118: Cisco IOS XR Egress Packet Network Interface Aligner Interrupt Denial of Service Vulnerability
 - A vulnerability in the handling of an Egress Packet Network Interface (EPNI) Aligner interrupt in Cisco IOS XR Software for Cisco Network Convergence System (NCS) 5500 Series with NC57 line cards and Cisco NCS 5700 Routers and Cisco IOS XR Software for Third Party Software could allow an unauthenticated, remote attacker to cause the network processing unit (NPU) and ASIC to stop processing, preventing traffic from traversing the interface. This vulnerability is due to the corruption of packets in specific cases when an EPNI Aligner interrupt is triggered while an affected device is experiencing heavy transit traffic. An attacker could exploit this vulnerability by sending a continuous flow of crafted packets to an interface of the affected device. A successful exploit could allow the attacker to cause persistent, heavy packet loss, resulting in a denial of service (DoS) condition.

20260306

Snort rules

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

- **Talos Rules 2026-03-05** (<https://www.snort.org/advisories/talos-rules-2026-03-05>)
- **Talos Rules 2026-03-03** (<https://www.snort.org/advisories/talos-rules-2026-03-03>)

The new and updated Snort rules span the following categories:

- 1 file-flash rule with SID 301441
- 2 file-image rules with SIDs 66058, 66059
- 2 file-other rules with SIDs 66037, 66036
- 3 indicator-shellcode rules with SIDs 66033, 66034, 66032
- 3 malware-cnc rules with SIDs 66055, 66035, 66054
- 21 malware-other rules with SIDs 301417, 301421, 301437, 301436, 301433, 301434, 301427, 301431, 301425, 301416, 301420, 301414, 301426, 301432, 301415, 301435, 301418, 301422, 301419, 301428, 301423

- 1 netbios rule with SID 24973
- 2 protocol-dns rules with SIDs 21355, 21354
- 1 server-mail rule with SID 301430
- 4 server-other rules with SIDs 301424, 41548, 31361, 59880
- 27 server-webapp rules with SIDs 59017, 66021, 66070, 301429, 66068, 66073, 301438, 59016, 66071, 66030, 301439, 66074, 301440, 66031, 66056, 66069, 66072, 66057, 66080, 66083, 66082, 66075, 66078, 66076, 66079, 66077, 66081

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 adds initial typing support for assets from Automation Direct. It also improves support for assets from Siemens and Rockwell.