Release Notes for Cisco Cyber Vision Knowledge DB

Release 202608

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.202608	**Description**
CiscoCyberVision_knowledgedb_20260807.db	Knowledge DB version 20260807
CiscoCyberVision_knowledgedb_20260814.db	Knowledge DB version 20260814

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

20260807

Snort rules

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

- **Talos Rules 2026-08-06 (https://www.snort.org/advisories/talos-rules-2026-08-06)**
- **Talos Rules 2026-08-04 (https://www.snort.org/advisories/talos-rules-2026-08-04)**

The new and updated Snort rules span the following categories:

- 1 file-other rule with SID 301588
- 1 policy-other rule with SID 66899
- 1 server-other rule with SID 25619
- 14 server-webapp rules with SIDs 66890, 66884, 66885, 66891, 66895, 66894, 66892, 66896, 66893, 66897, 66889, 66875, 66888, 66898

20260814

Snort rules

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

- **Talos Rules 2026-08-13 (https://www.snort.org/advisories/talos-rules-2026-08-13-8-13-2026)**
- **Talos Rules 2026-08-13 (https://www.snort.org/advisories/talos-rules-2026-08-13)**
- **Talos Rules 2026-08-11 (https://www.snort.org/advisories/talos-rules-2026-08-11)**

The new and updated Snort rules span the following categories:

- 2 file-other rules with SIDs 66933, 66934
- 7 malware-cnc rules with SIDs 66926, 66924, 66927, 66925, 66961, 66928, 66960
- 1 netbios rule with SID 24973
- 24 os-windows rules with SIDs 301604, 301593, 301609, 301592, 301596, 301598, 301599, 301601, 301606, 301589, 301591, 301594, 301603, 301602, 301610, 301595, 301607, 301611, 301608, 301590, 66902, 301597, 301605, 301600
- 1 policy-other rule with SID 66900
- 2 protocol-dns rules with SIDs 21355, 21354

- 4 server-other rules with SIDs 66959, 31361, 41548, 59880
- 10 server-webapp rules with SIDs 301612, 66967, 66901, 66962, 66911, 66965, 66966, 46897, 66949, 66950

Vulnerabilities

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

- CVE-2026-59693: Improper Check for Unusual or Exceptional Conditions Vulnerability in Siemens Desigo DXR and PXC Controllers
    - The affected devices are vulnerable to a denial-of-service (DoS) vulnerability. An attacker can exploit this issue by sending a malformed BACnet packet, causing the device to stop responding to BACnet queries. Recovery requires a device reset or reboot to restore normal functionality.
- CVE-2026-20124: Cisco IOS XE Software SNMP Denial of Service Vulnerability
    - A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to improper error handling when parsing SNMP requests. This vulnerability affects all versions of SNMP — Versions 1, 2c, and 3. An attacker could exploit this vulnerability by sending a malformed SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. The attacker must have the SNMPv1 or v2c read-only or read-write community string or valid SNMPv3 user credentials on the affected device.
- CVE-2026-20263: Cisco IOS XE Software Blocks Extensible Exchange Protocol Denial of Service Vulnerability
    - A vulnerability in the Blocks Extensible Exchange Protocol (BEEP) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling when parsing a specific BEEP SOAP request. An attacker could exploit this vulnerability by sending a specific BEEP SOAP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.
- CVE-2026-20267: Improper Access Control Vulnerability in Cisco IOS XE Software
    - CVE-2026-20267 groups multiple internally discovered issues involving improper access control (CWE-284) in Cisco IOS XE Software. Cisco states that this vulnerability class covers authorization, authentication, privileges, and bypasses. The most severe underlying issue has a CVSS 3.1 base score of 9.0 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H); the attack is network-based, has high attack complexity, requires no privileges, requires no user interaction, may have high impact on confidentiality, integrity and availability, can affect resources beyond the vulnerable security scope. Cisco found these issues during internal testing and is not aware of active exploitation.
- CVE-2026-20268: Improper Restriction of Operations Within the Bounds of a Memory Buffer Vulnerability in Cisco IOS XE Software

  - CVE-2026-20268 groups multiple internally discovered issues involving improper restriction of operations within the bounds of a memory buffer (CWE-119) in Cisco IOS XE Software. Cisco states that this vulnerability class covers buffer overflows and out-of-bounds writes. The most severe underlying issue has a CVSS 3.1 base score of 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H); the attack is network-based, has low attack complexity, requires no privileges, requires no user interaction, may have high impact on availability, can affect resources beyond the vulnerable security scope. Cisco found these issues during internal testing and is not aware of active exploitation.

- CVE-2026-20269: Improper Control of a Resource Through Its Lifetime Vulnerability in Cisco IOS XE Software
  - CVE-2026-20269 groups multiple internally discovered issues involving improper control of a resource through its lifetime (CWE-664) in Cisco IOS XE Software. Cisco states that this vulnerability class covers memory and file handlers, null pointer dereferences, invalid frees. The most severe underlying issue has a CVSS 3.1 base score of 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H); the attack is network-based, has low attack complexity, requires no privileges, requires no user interaction, may have high impact on availability, can affect resources beyond the vulnerable security scope. Cisco found these issues during internal testing and is not aware of active exploitation.
- CVE-2026-20270: Incorrect Calculation Vulnerability in Cisco IOS XE Software
  - CVE-2026-20270 groups multiple internally discovered issues involving incorrect calculation (CWE-682) in Cisco IOS XE Software. Cisco states that this vulnerability class covers arithmetic or numeric conversion errors including integer overflow, underflow, truncation. The most severe underlying issue has a CVSS 3.1 base score of 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H); the attack is network-based, has low attack complexity, requires no privileges, requires no user interaction, may have high impact on availability, can affect resources beyond the vulnerable security scope. Cisco found these issues during internal testing and is not aware of active exploitation.
- CVE-2026-20271: Insufficient Control Flow Management Vulnerability in Cisco IOS XE Software
  - CVE-2026-20271 groups multiple internally discovered issues involving insufficient control flow management (CWE-691) in Cisco IOS XE Software. Cisco states that this vulnerability class covers infinite loops, uncontrolled recursion, race conditions. The most severe underlying issue has a CVSS 3.1 base score of 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H); the attack is network-based, has low attack complexity, requires no privileges, requires no user interaction, may have high impact on availability, can affect resources beyond the vulnerable security scope. Cisco found these issues during internal testing and is not aware of active exploitation.
- CVE-2026-20272: Improper Neutralization of Special Elements Vulnerability in Cisco IOS XE Software
  - CVE-2026-20272 groups multiple internally discovered issues involving improper neutralization of special elements (CWE-74) in Cisco IOS XE Software. Cisco states that this vulnerability class covers command, OS, argument injection. The most severe underlying issue has a CVSS 3.1 base score of 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H); the attack is network-based, has low attack complexity, requires no privileges, requires no user interaction, may have high impact on

confidentiality, integrity and availability. Cisco found these issues during internal testing and is not aware of active exploitation.

- CVE-2026-20273: Improper Input Validation Vulnerability in Cisco IOS XE Software
    - CVE-2026-20273 groups multiple internally discovered issues involving improper input validation (CWE-20) in Cisco IOS XE Software. Cisco states that this vulnerability class covers input validation, path traversal, and external path control. The most severe underlying issue has a CVSS 3.1 base score of 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H); the attack is network-based, has low attack complexity, requires no privileges, requires no user interaction, may have high impact on availability, can affect resources beyond the vulnerable security scope. Cisco found these issues during internal testing and is not aware of active exploitation.
- CVE-2026-20301: Cisco IOS Software and IOS XE Software Extensible Messaging Client Protocol Denial of Service Vulnerability
    - A vulnerability in the Extensible Messaging Client Protocol (XMCP), also referred to as the External Client protocol, of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of malformed XMCP packets. An attacker could exploit this vulnerability by sending a malformed XMCP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload unexpectedly, resulting in a DoS condition. The attacker does not need the XMCP client username to exploit this vulnerability.
- CVE-2026-20308: Cisco IOS XE Software Web-Based Management Interface Denial of Service Vulnerability
    - A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an authenticated, remote attacker with low privileges to perform a denial of service (DoS) attack against an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web-based management interface of an affected device. A successful exploit could allow the attacker to cause the web-based management interface to become unresponsive.
- CVE-2026-20311: Cisco IOS XE Software Web-Based Management Interface Denial of Service Vulnerability
    - A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an authenticated, remote attacker with low privileges to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient error handling in the web-based management interface. An attacker could exploit this vulnerability by authenticating with a malformed certificate. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.
- CVE-2025-41769: Buffer Overflow vulnerability in Phoenix Contact PLCnext Control devices
    - The device's PROFINET service is affected by a buffer overflow vulnerability that exists in the default configuration. An unauthenticated remote attacker could exploit this vulnerability to reboot the device or execute arbitrary code.
- CVE-2025-41770: Denial of Service vulnerability in Phoenix Contact PLCnext Control devices

  - An unauthenticated denial-of-service vulnerability in the device's PLCnext Engineer communication interface allows an remote attacker to interrupt access via the client application. Successful exploitation prevents communication until the PLCnext service is manually restarted.

- CVE-2025-41771: SQL Injection vulnerability in Phoenix Contact PLCnext Control devices
  - An authenticated attacker with low privileges can access an endpoint in the controller’s web interface that is vulnerable to SQL injection. The vulnerability affects a SQLite database used only for storing notification messages. Therefore, the impact is limited to the system’s notification functionality.