



Release Notes for Cisco Cyber Vision Knowledge DB

Release 202604

Compatible device list	2
Links	2
Software Download	2
Related Documentation	3
Database download	3
How to update the database	3
Release contents	4
20260430	4
Snort rules	4
20260424	4
Snort rules	4
Vendor Database	5
Vulnerabilities	5
20260410	9
Snort rules	9
20260403	9
Snort rules	10

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.202604	Description
CiscoCyberVision_knowledgedb_20260403.db	Knowledge DB version 20260403
CiscoCyberVision_knowledgedb_20260410.db	Knowledge DB version 20260410
CiscoCyberVision_knowledgedb_20260424.db	Knowledge DB version 20260424
CiscoCyberVision_knowledgedb_20260430.db	Knowledge DB version 20260430

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

20260430

Snort rules

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

- **Talos Rules 2026-04-28** (<https://www.snort.org/advisories/talos-rules-2026-04-28>)

The new and updated Snort rules span the following categories:

- 3 file-other rules with SIDs 301488, 301487, 301489
- 1 file-pdf rule with SID 301485
- 6 malware-cnc rules with SIDs 66383, 66387, 66385, 66382, 66386, 66384
- 1 malware-other rule with SID 301490
- 1 policy-other rule with SID 301486
- 2 server-webapp rules with SIDs 66381, 59016

20260424

Snort rules

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

- **Talos Rules 2026-04-23** (<https://www.snort.org/advisories/talos-rules-2026-04-23>)
- **Talos Rules 2026-04-21** (<https://www.snort.org/advisories/talos-rules-2026-04-21>)
- **Talos Rules 2026-04-16** (<https://www.snort.org/advisories/talos-rules-2026-04-16>)
- **Talos Rules 2026-04-14** (<https://www.snort.org/advisories/talos-rules-2026-04-14>)

The new and updated Snort rules span the following categories:

- 2 file-multimedia rules with SIDs 66230, 66229
- 1 malware-cnc rule with SID 66252
- 1 malware-other rule with SID 301479
- 13 os-windows rules with SIDs 301398, 301472, 301478, 301480, 301470, 301484, 301475, 301468, 301477, 301469, 301471, 66296, 66340
- 2 policy-other rules with SIDs 66274, 65962
- 3 protocol-scada rules with SIDs 66333, 66334, 66332

- 11 server-other rules with SIDs 66268, 66270, 66269, 66271, 66342, 66343, 66341, 66345, 66344, 66346, 66380
- 1111 server-webapp rules with SIDs 61434, 66292, 66146, 66233, 66232, 66283, 66231, 66285, 66236, 301474, 66253, 66284, 301476, 301467, 65934, 66289, 66295, 66256, 65935, 301481, 66240, 66234, 66235, 66286, 66281, 66280, 66277, 66239, 66261, 66282, 301473, 66241, 301483, 301482, 64426, 63306, 66300, 66302, 66306, 66303, 66297, 66304, 66301, 66299, 66305, 66298,...

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 ABB and Omron.

Vulnerabilities

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

- CVE-2022-45789: Authentication Bypass Vulnerability in Schneider Modicon M340, Momentum, MC80, M580 and M580 CPU Safety
 - An authentication bypass by capture-replay vulnerability exists that could cause execution of unauthorized Modbus functions on the controller when hijacking an authenticated Modbus session.
- CVE-2026-20004: Cisco IOS XE Software TLS Memory Exhaustion Denial of Service Vulnerability
 - A vulnerability in the TLS library of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to exhaust the available memory of an affected device. This vulnerability is due to improper management of memory resources during TLS connection setup. An attacker could exploit this vulnerability by repeatedly triggering the conditions that cause the memory increase. This could be done in a variety of ways, such as by repeatedly attempting Extensible Authentication Protocol (EAP) authentication when local EAP is enabled on an affected device or by using a machine-in-the-middle attack and resetting TLS connections between the affected device and other devices. A successful exploit could allow the attacker to exhaust the available memory on an affected device, resulting in an unexpected reload and a denial of service (DoS) condition.
- CVE-2026-20012: Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerability
 - A vulnerability in the Internet Key Exchange version 2 (IKEv2) feature of Cisco IOS Software, Cisco IOS XE Software, Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a denial of service (DoS) condition on an affected device. This vulnerability is due to improper parsing of IKEv2 packets. An attacker could exploit this vulnerability by sending crafted IKEv2 packets to an affected device. A successful exploit of Cisco IOS Software and IOS XE Software could allow the attacker to cause the affected device to reload, resulting in a DoS condition. A successful exploit of Cisco Secure Firewall ASA Software and Secure FTD Software

could allow the attacker to partially exhaust system memory, resulting in system instability, such as the inability to establish new IKEv2 VPN sessions. A manual reboot of the device is required to recover from this condition.

- CVE-2026-20083: Cisco IOS XE Software Secure Copy Protocol Server Denial of Service Vulnerability
 - A vulnerability in the Secure Copy Protocol (SCP) server feature of Cisco IOS XE Software could allow an authenticated, local attacker with low privileges to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of a malformed SCP request. An attacker could exploit this vulnerability by issuing a crafted command through SSH. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.
- CVE-2026-20084: Cisco IOS XE Software for Catalyst 9000 Series Switches DHCP Snooping Denial of Service Vulnerability
 - A vulnerability in the DHCP snooping feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause BOOTP packets to be forwarded between VLANs, resulting in a denial of service (DoS) condition. This vulnerability is due to improper handling of BOOTP packets on Cisco Catalyst 9000 Series Switches. An attacker could exploit this vulnerability by sending BOOTP request packets to an affected device. A successful exploit could allow an attacker to forward BOOTP packets from one VLAN to another, resulting in BOOTP VLAN leakage and potentially leading to high CPU utilization. This makes the device unreachable (either through console or remote management) and unable to forward traffic, resulting in a DoS condition.
- CVE-2026-20086: Cisco IOS XE Wireless Controller Software for the Catalyst CW9800 Family CAPWAP Denial of Service Vulnerability
 - A vulnerability in the processing of Control and Provisioning of Wireless Access Points (CAPWAP) packets of Cisco IOS XE Wireless Controller Software for the Catalyst CW9800 Family 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 a malformed CAPWAP packet. An attacker could exploit this vulnerability by sending a malformed CAPWAP 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.
- CVE-2026-20104: Cisco IOS XE Software for Cisco Catalyst and Rugged Series Switches Secure Boot Bypass Vulnerability
 - A vulnerability in the bootloader of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches, Cisco Catalyst ESS9300 Embedded Series Switches, Cisco Catalyst IE9310 and IE9320 Rugged Series Switches, and Cisco IE3500 and IE3505 Rugged Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to an affected device to execute arbitrary code at boot time and break the chain of trust. This vulnerability is due to insufficient validation of software at boot time. An attacker could exploit this vulnerability by manipulating the loaded binaries on an affected device to bypass some of the integrity checks that are performed during the boot process. A successful exploit could allow the attacker to execute code that bypasses the requirement to run Cisco-signed images.

- CVE-2026-20110: Cisco IOS XE Software Denial of Service Vulnerability
 - A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because incorrect privileges are associated with the start maintenance command. An attacker could exploit this vulnerability by accessing the management CLI of the affected device as a low-privileged user and using the start maintenance command. A successful exploit could allow the attacker to put the device in maintenance mode, which shuts down interfaces, resulting in a denial of service (DoS) condition. In case of exploitation, a device administrator can connect to the CLI and use the stop maintenance command to restore operations.
- CVE-2026-20112: Cisco IOx Application Hosting Environment Stored Cross-Site Scripting Vulnerability
 - A vulnerability in the web-based Cisco IOx application hosting environment management interface of Cisco IOS XE Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid administrative credentials.
- CVE-2026-20113: Cisco IOx Application Hosting Environment Carriage Return Line Feed Injection Vulnerability
 - A vulnerability in the web-based Cisco IOx application hosting environment management interface of Cisco IOS XE Software could allow an unauthenticated, remote attacker to perform a carriage return line feed (CRLF) injection attack against a user. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by sending crafted packets to an affected device. A successful exploit could allow the attacker to arbitrarily inject log entries, manipulate the structure of log files, or obscure legitimate log events.
- CVE-2026-20114: Cisco IOS XE Software Lobby Ambassador Privilege Escalation Vulnerability
 - A vulnerability in the Lobby Ambassador web-based management API of Cisco IOS XE Software could allow an authenticated, remote attacker to elevate their privileges and access management APIs that would not normally be available for Lobby Ambassador users. This vulnerability exists because parameters that are received by an API endpoint are not sufficiently validated. An attacker could exploit this vulnerability by authenticating as a Lobby Ambassador user and sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to create a new user with privilege level 1 access to the web-based management API. The attacker would then be able to access the device with these new credentials and privileges.
- CVE-2026-20115: Cisco IOS XE Software Secure Channel for Meraki Information Disclosure Vulnerability
 - A vulnerability in Cisco IOS XE Software for Cisco Meraki could allow a remote, unauthenticated attacker to view confidential device information. This vulnerability is due to a device configuration upload being performed over an insecure tunnel. An attacker could exploit this vulnerability by

conducting an on-path attack between the affected device and the Cisco Meraki Dashboard. A successful exploit could allow the attacker to view sensitive device configuration information.

- CVE-2026-20125: Cisco IOS Software and IOS XE Software Release 3E HTTP Server Denial of Service Vulnerability
 - A vulnerability in the HTTP Server feature of Cisco IOS Software and Cisco IOS XE Software Release 3E could allow an authenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending malformed HTTP requests to an affected device. A successful exploit could allow the attacker to cause a watchdog timer to expire and the device to reload, resulting in a DoS condition. To exploit this vulnerability, the attacker must have a valid user account.
- CVE-2026-22316: Denial of Service Vulnerability in Phoenix Contact FL SWITCH 2xxx, FL SWITCH TSN 23xx, FL SWITCH 59xx and FL NAT
 - A remote attacker with user privileges for the webUI can use the setting of the TFTP Filename with a POST Request to trigger a stack-based Buffer Overflow, resulting in a DoS attack.
- CVE-2026-22317: Command Injection Vulnerability in Phoenix Contact FL SWITCH 2xxx, FL SWITCH TSN 23xx, FL SWITCH 59xx and FL NAT
 - A command injection vulnerability in the device's Root CA certificate transfer workflow allows a high-privileged attacker to send crafted HTTP POST requests that result in arbitrary command execution on the underlying Linux OS with root privileges.
- CVE-2026-22318: Denial of Service Vulnerability in Phoenix Contact FL SWITCH 2xxx, FL SWITCH TSN 23xx, FL SWITCH 59xx and FL NAT
 - A stack-based buffer overflow vulnerability in the device's file transfer parameter workflow allows a high-privileged attacker to send oversized POST parameters, causing memory corruption in an internal process, resulting in a DoS attack.
- CVE-2026-22319: Denial of Service Vulnerability in Phoenix Contact FL SWITCH 2xxx, FL SWITCH TSN 23xx, FL SWITCH 59xx and FL NAT
 - A stack-based buffer overflow in the device's file installation workflow allows a high-privileged attacker to send oversized POST parameters that overflow a fixed-size stack buffer within an internal process, resulting in a DoS attack.
- CVE-2026-22320: Denial of Service Vulnerability in Phoenix Contact FL SWITCH 2xxx, FL SWITCH TSN 23xx, FL SWITCH 59xx and FL NAT
 - A stack-based buffer overflow in the CLI's TFTP file-transfer command handling allows a low-privileged attacker with Telnet/SSH access to trigger memory corruption by supplying unexpected or oversized filename input. Exploitation results in the corruption of the internal buffer, causing the CLI and web dashboard to become unavailable and leading to a denial of service.
- CVE-2026-22321: Denial of Service Vulnerability in Phoenix Contact FL SWITCH 2xxx, FL SWITCH TSN 23xx, FL SWITCH 59xx and FL NAT

- A stack-based buffer overflow in the device's Telnet/SSH CLI login routine occurs when a unauthenticated attacker send an oversized or unexpected username input. An overflow condition crashes the thread handling the login attempt, forcing the session to close. Because other CLI sessions remain unaffected, the impact is limited to a low-severity availability disruption.
- CVE-2026-22322: Cross-Site Scripting Vulnerability in Phoenix Contact FL SWITCH 2xxx, FL SWITCH TSN 23xx, FL SWITCH 59xx and FL NAT
 - A stored cross-site scripting (XSS) vulnerability in the Link Aggregation configuration interface allows an unauthenticated remote attacker to create a trunk entry containing malicious HTML/JavaScript code. When the affected page is viewed, the injected script executes in the context of the victim's browser, enabling unauthorized actions such as interface manipulation. The session cookie is secured by the httpOnly Flag. Therefore an attacker is not able to take over the session of an authenticated user.
- CVE-2026-22323: Cross-Site Request Forgery Vulnerability in Phoenix Contact FL SWITCH 2xxx, FL SWITCH TSN 23xx, FL SWITCH 59xx and FL NAT
 - A CSRF vulnerability in the Link Aggregation configuration interface allows an unauthenticated remote attacker to trick authenticated users into sending unauthorized POST requests to the device by luring them to a malicious webpage. This can silently alter the device's configuration without the victim's knowledge or consent. Availability impact was set to low because after a successful attack the device will automatically recover without external intervention.

20260410

Snort rules

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

- Talos Rules 2026-04-09 (<https://www.snort.org/advisories/talos-rules-2026-04-09>)
- Talos Rules 2026-04-07 (<https://www.snort.org/advisories/talos-rules-2026-04-07>)

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 301466
- 5 malware-cnc rules with SIDs 66224, 66225, 66222, 66218, 66219
- 1 malware-other rule with SID 301465
- 1 malware-tools rule with SID 301464
- 8 server-webapp rules with SIDs 66212, 66211, 63914, 66226, 66214, 66213, 66210, 66217

20260403

Snort rules

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

- **Talos Rules 2026-04-02** (<https://www.snort.org/advisories/talos-rules-2026-04-02>)
- **Talos Rules 2026-03-31** (<https://www.snort.org/advisories/talos-rules-2026-03-31>)

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 300328
- 1 file-image rule with SID 301459
- 3 malware-cnc rules with SIDs 301462, 66200, 66192
- 1 malware-other rule with SID 301461
- 5 policy-other rules with SIDs 66208, 66196, 66197, 66209, 66195
- 1 server-mail rule with SID 301460
- 10 server-webapp rules with SIDs 66205, 301463, 66206, 66198, 66199, 66189, 66204, 66207, 66194, 66193