



Release Notes for Cisco Cyber Vision Knowledge DB

Release 202510

<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
20251024.....	4
20251017.....	4
20251013.....	10
20251003.....	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-5.3.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.3.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.3.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.3.0.ext	Sensor Management extension installation file
Sensor	Description
CiscoCyberVision-IOx-aarch64-5.3.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.3.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.3.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.3.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.3.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	Description
CiscoCyberVision-Embedded-KDB-5.3.0.dat	Knowledge DB embedded in Cisco Cyber Vision 5.3.0
Updates/KDB/KDB.202510	Description
CiscoCyberVision_knowledgedb_20251003.db	Knowledge DB version 20251003
CiscoCyberVision_knowledgedb_20251013.db	Knowledge DB version 20251013
CiscoCyberVision_knowledgedb_20251017.db	Knowledge DB version 20251017
CiscoCyberVision_knowledgedb_20251024.db	Knowledge DB version 20251024

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

20251024

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

- **Talos Rules 2025-10-23** (<https://www.snort.org/advisories/talos-rules-2025-10-23>)
- **Talos Rules 2025-10-21** (<https://www.snort.org/advisories/talos-rules-2025-10-21>)

The new and updated Snort rules span the following categories:

- 2 file-multimedia rules with SIDs 65458, 65457
- 1 malware-cnc rule with SID 65446
- 1 malware-tools rule with SID 65448
- 1 os-windows rule with SID 301336
- 17 server-webapp rules with SIDs 65456, 65452, 65378, 65377, 301337, 65453, 65443, 65455, 65451, 65439, 65440, 65442, 65454, 65441, 65445, 65444, 65447

20251017

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

- **Talos Rules 2025-10-16** (<https://www.snort.org/advisories/talos-rules-2025-10-16>)
- **Talos Rules 2025-10-14** (<https://www.snort.org/advisories/talos-rules-2025-10-14>)

The new and updated Snort rules span the following categories:

- 2 file-pdf rules with SIDs 65412, 65411
- 4 malware-cnc rules with SIDs 65413, 65414, 65423, 65415
- 1 malware-other rule with SID 301324
- 12 os-windows rules with SIDs 65422, 301334, 301336, 301331, 301328, 301329, 301330, 301333, 301327, 301332, 301325, 301326
- 2 policy-other rules with SIDs 65424, 65436
- 3 server-mail rules with SIDs 44735, 44734, 301335
- 2 server-other rules with SIDs 65425, 65426
- 27 server-webapp rules with SIDs 65386, 65434, 65433, 65431, 65385, 65432, 65384, 65435, 64101, 65383, 65381, 65382, 65427, 65419, 64672, 65429, 65417, 64673, 65416, 65428, 65418, 65387, 65430, 65388, 64671, 65437, 65438

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

- CVE-2025-20149: Cisco IOS and IOS XE Software CLI Denial of Service Vulnerability
 - A vulnerability in the CLI of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to a buffer overflow. An attacker with a low-privileged account could exploit this vulnerability by using crafted commands at the CLI prompt. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.
- CVE-2025-20160: Cisco IOS and IOS XE Software TACACS+ Authentication Bypass Vulnerability
 - A vulnerability in the implementation of the TACACS+ protocol in Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to view sensitive data or bypass authentication. This vulnerability exists because the system does not properly check whether the required TACACS+ shared secret is configured. A machine-in-the-middle attacker could exploit this vulnerability by intercepting and reading unencrypted TACACS+ messages or impersonating the TACACS+ server and falsely accepting arbitrary authentication requests. A successful exploit could allow the attacker to view sensitive information in a TACACS+ message or bypass authentication and gain access to the affected device.
- CVE-2025-20240: Cisco IOS XE Software Web Authentication Reflected Cross-Site Scripting Vulnerability
 - A vulnerability in the Web Authentication feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting attack (XSS) on an affected device. This vulnerability is due to improper sanitization of user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to execute a reflected XSS attack and steal user cookies from the affected device.
- CVE-2025-20293: Cisco IOS XE Software for Catalyst 9800 Series Wireless Controller for Cloud Unauthenticated Access to Certificate Enrollment Service Vulnerability
 - A vulnerability in the Day One setup process of Cisco IOS XE Software for Catalyst 9800 Series Wireless Controllers for Cloud (9800-CL) could allow an unauthenticated, remote attacker to access the public-key infrastructure (PKI) server that is running on an affected device. This vulnerability is due to incomplete cleanup upon completion of the Day One setup process. An attacker could exploit this vulnerability by sending Simple Certificate Enrollment Protocol (SCEP) requests to an affected device. A successful exploit could allow the attacker to request a certificate from the virtual wireless controller and then use the acquired certificate to join an attacker-controlled device to the virtual wireless controller.
- CVE-2025-20311: Cisco IOS XE Software for Catalyst 9000 Series Switches Denial of Service Vulnerability
 - A vulnerability in the handling of certain Ethernet frames in Cisco IOS XE Software for Catalyst 9000 Series Switches could allow an unauthenticated, adjacent attacker to cause an egress port to become blocked and drop all outbound traffic. This vulnerability is due to improper handling of crafted Ethernet frames. An attacker could exploit this vulnerability by sending crafted Ethernet frames through an affected switch. A successful exploit could allow the attacker to cause the egress

port to which the crafted frame is forwarded to start dropping all frames, resulting in a denial of service (DoS) condition.

- CVE-2025-20312: Cisco IOS XE Software Simple Network Management Protocol 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 a denial of service (DoS) condition on an affected device. This vulnerability is due to improper error handling when parsing a specific SNMP request. An attacker could exploit this vulnerability by sending a specific SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition. This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMPv2c or earlier, the attacker must know a valid read-write or read-only SNMP community string for the affected system. To exploit this vulnerability through SNMPv3, the attacker must have valid SNMP user credentials for the affected system.
- CVE-2025-20313: Cisco IOS XE Software Secure Boot Bypass Vulnerabilities
 - Multiple vulnerabilities in Cisco IOS XE Software could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to an affected device to execute persistent code at boot time and break the chain of trust. These vulnerabilities are due to improper validation of software packages. An attacker could exploit these vulnerabilities by placing a crafted file into a specific location on an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Because these vulnerabilities allow an attacker to bypass a major security feature of a device, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.
- CVE-2025-20314: Cisco IOS XE Software Secure Boot Bypass Vulnerabilities
 - Multiple vulnerabilities in Cisco IOS XE Software could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to an affected device to execute persistent code at boot time and break the chain of trust. These vulnerabilities are due to improper validation of software packages. An attacker could exploit these vulnerabilities by placing a crafted file into a specific location on an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Because these vulnerabilities allow an attacker to bypass a major security feature of a device, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.
- CVE-2025-20315: Cisco IOS XE Software Network-Based Application Recognition Denial of Service Vulnerability
 - A vulnerability in the Network-Based Application Recognition (NBAR) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, causing a denial of service (DoS) condition. This vulnerability is due to improper handling of malformed Control and Provisioning of Wireless Access Points (CAPWAP) packets. An attacker could exploit this vulnerability by sending malformed CAPWAP packets through an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.

- CVE-2025-20316: Cisco IOS XE Software on Cisco Catalyst 9500X and 9600X Series Switches Virtual Interface Access Control List Bypass Vulnerability
 - A vulnerability in the access control list (ACL) programming of Cisco IOS XE Software for Cisco Catalyst 9500X and 9600X Series Switches could allow an unauthenticated, remote attacker to bypass a configured ACL on an affected device. This vulnerability is due to the flooding of traffic from an unlearned MAC address on a switch virtual interface (SVI) that has an egress ACL applied. An attacker could exploit this vulnerability by causing the VLAN to flush its MAC address table. This condition can also occur if the MAC address table is full. A successful exploit could allow the attacker to bypass an egress ACL on an affected device.
- CVE-2025-20327: Cisco IOS Software Industrial Ethernet Switch Device Manager Denial of Service Vulnerability
 - A vulnerability in the web UI of Cisco IOS 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 improper input validation. An attacker could exploit this vulnerability by sending a crafted URL in an HTTP request. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.
- CVE-2025-20334: Cisco IOS XE Software HTTP API Command Injection Vulnerability
 - A vulnerability in the HTTP API subsystem of Cisco IOS XE Software could allow a remote attacker to inject commands that will execute with root privileges into the underlying operating system. This vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by authenticating to an affected system and performing an API call with crafted input. Alternatively, an unauthenticated attacker could persuade a legitimate user with administrative privileges who is currently logged in to the system to click a crafted link. A successful exploit could allow the attacker to execute arbitrary commands as the root user.
- CVE-2025-20338: Cisco IOS XE Software CLI Argument Injection Vulnerability
 - A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with administrative privileges to execute arbitrary commands as root on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by logging in to the device CLI with valid administrative (level 15) credentials and using crafted commands at the CLI prompt. A successful exploit could allow the attacker to execute arbitrary commands as root.
- CVE-2025-20352: Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability
 - A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software could allow the following: An authenticated, remote attacker with low privileges could cause a denial of service (DoS) condition on an affected device that is running Cisco IOS Software or Cisco IOS XE Software. To cause the DoS, the attacker must have the SNMPv2c or earlier read-only community string or valid SNMPv3 user credentials. An authenticated, remote attacker with high privileges could execute code as the root user on an affected device that is running Cisco IOS XE Software. To execute code as the root user, the attacker

must have the SNMPv1 or v2c read-only community string or valid SNMPv3 user credentials and administrative or privilege 15 credentials on the affected device. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device over IPv4 or IPv6 networks. This vulnerability is due to a stack overflow condition in the SNMP subsystem of the affected software. A successful exploit could allow a low-privileged attacker to cause the affected system to reload, resulting in a DoS condition, or allow a high-privileged attacker to execute arbitrary code as the root user and obtain full control of the affected system.

- CVE-2025-20363: Cisco Secure Firewall Adaptive Security Appliance Software, Secure Firewall Threat Defense Software, IOS Software, IOS XE Software, and IOS XR Software Web Services Remote Code Execution Vulnerability
 - A vulnerability in the web services of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, Cisco Secure Firewall Threat Defense (FTD) Software, Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an unauthenticated, remote attacker (Cisco ASA and FTD Software) or authenticated, remote attacker (Cisco IOS, IOS XE, and IOS XR Software) with low user privileges to execute arbitrary code on an affected device. This vulnerability is due to improper validation of user-supplied input in HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted web service on an affected device after obtaining additional information about the system, overcoming exploit mitigations, or both. A successful exploit could allow the attacker to execute arbitrary code as root, which may lead to the complete compromise of the affected device.
- CVE-2025-40771: Missing Authentication for Critical Function in Siemens SIMATIC ET 200SP Communication Processors
 - SIMATIC ET 200SP communication processors (CP 1542SP-1, CP 1542SP-1 IRC and CP 1543SP-1, incl. SIPLUS variants) contain an authentication vulnerability that could allow an unauthenticated remote attacker to access the configuration data.
- CVE-2025-41699: Code Injection Vulnerability in Phoenix Contact CHARX SEC-3xxx charging controllers
 - An low privileged remote attacker with an account for the Web-based management can change the system configuration to perform a command injection as root, resulting in a total loss of confidentiality, availability and integrity due to improper control of generation of code ('Code Injection').
- CVE-2025-41703: Denial of Service Vulnerability in Phoenix Contact QUINT4-UPS EIP
 - An unauthenticated remote attacker can cause a Denial of Service by turning off the output of the UPS via Modbus command.
- CVE-2025-41704: Denial of Service Vulnerability in Phoenix Contact QUINT4-UPS EIP
 - An unauthenticated remote attacker can perform a DoS of the Modbus service by sending a specific function and sub-function code without affecting the core functionality.
- CVE-2025-41705: Man In The Middle Vulnerability in Phoenix Contact QUINT4-UPS EIP
 - An unauthenticated remote attacker (MITM) can intercept the websocket messages to gain access to the login credentials for the Webfrontend.

- CVE-2025-41706: Buffer Overflow Vulnerability in Phoenix Contact QUINT4-UPS EIP
 - The webserver is vulnerable to a denial of service condition. An unauthenticated remote attacker can craft a special GET request with an over-long content-length to trigger the issue without affecting the core functionality.
- CVE-2025-41707: Buffer Overflow Vulnerability in Phoenix Contact QUINT4-UPS EIP
 - The websocket handler is vulnerable to a denial of service condition. An unauthenticated remote attacker can send a crafted websocket message to trigger the issue without affecting the core functionality.
- CVE-2025-7328: Improper Authentication Vulnerability in Rockwell 1783-NATR
 - Multiple Broken Authentication security issues exist in the affected product. The security issues are due to missing authentication checks on critical functions. These could result in potential denial-of-service, admin account takeover, or NAT rule modifications. Devices would no longer be able to communicate through NATR as a result of denial-of-service or NAT rule modifications. NAT rule modification could also result in device communication to incorrect endpoints. Admin account takeover could allow modification of configuration and require physical access to restore.
- CVE-2025-7329: Cross-site Scripting Vulnerability in Rockwell 1783-NATR
 - A Stored Cross-Site Scripting security issue exists in the affected product that could potentially allow a malicious user to view and modify sensitive data or make the webpage unavailable. The vulnerability stems from missing special character filtering and encoding. Successful exploitation requires an attacker to be able to update configuration fields behind admin login.
- CVE-2025-7330: Cross-Site Request Forgery Vulnerability in Rockwell 1783-NATR
 - A cross-site request forgery security issue exists in the product and version listed. The vulnerability stems from missing CSRF checks on the impacted form. This allows for unintended configuration modification if an attacker can convince a logged in admin to visit a crafted link.
- CVE-2025-9124: Denial-Of-Service Vulnerability in Rockwel Compact GuardLogix 5370
 - A denial-of-service security issue in the affected product. The security issue stems from a fault occurring when a crafted CIP unconnected explicit message is sent. This can result in a major non-recoverable fault.
- CVE-2025-9177: Denial of Service Vulnerability in Rockwell 1715 EtherNet/IP Comms Module
 - A denial-of-service security issue exists in the affected product and version. The security issue stems from a high number of requests sent to the web server. This could result in a web server crash however; this does not impact I/O control or communication . A power cycle is required to recover and utilize the webpage.
- CVE-2025-9178: Denial of Service Vulnerability in Rockwell 1715 EtherNet/IP Comms Module
 - A denial-of-service security issue exists in the affected product and version. The security issue is caused through CIP communication using crafted payloads. The security issue could result in no CIP communication with 1715 EtherNet/IP Adapter. A restart is required to recover.

20251013

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

- **Talos Rules 2025-10-09** (<https://www.snort.org/advisories/talos-rules-2025-10-09>)
- **Talos Rules 2025-10-07** (<https://www.snort.org/advisories/talos-rules-2025-10-07>)

The new and updated Snort rules span the following categories:

- 2 file-image rules with SIDs 65380, 65379
- 1 file-other rule with SID 51093
- 3 indicator-compromise rules with SIDs 65364, 65365, 65363
- 1 malware-tools rule with SID 301321
- 3 policy-other rules with SIDs 65368, 65369, 65370
- 10 server-webapp rules with SIDs 65378, 65377, 65376, 65374, 65373, 301323, 301322, 65375, 65371, 65372

20251003

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

- **Talos Rules 2025-10-02** (<https://www.snort.org/advisories/talos-rules-2025-10-02>)
- **Talos Rules 2025-09-30** (<https://www.snort.org/advisories/talos-rules-2025-09-30>)

The new and updated Snort rules span the following categories:

- 1 browser-ie rules with SIDs 301318
- 2 file-pdf rules with SIDs 65362, 65361
- 1 policy-other rules with SIDs 57459
- 3 server-webapp rules with SIDs 301320, 64071, 301319