Release Notes for Cisco Cyber Vision Knowledge DB

Release 202509

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.202509	**Description**
CiscoCyberVision_knowledgedb_20250905.db	Knowledge DB version 20250905
CiscoCyberVision_knowledgedb_20250911.db	Knowledge DB version 20250911
CiscoCyberVision_knowledgedb_20250919.db	Knowledge DB version 20250919

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

20250919

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

- **Talos Rules 2025-09-19 (https://www.snort.org/advisories/talos-rules-2025-09-18)**
- **Talos Rules 2025-09-15 (https://www.snort.org/advisories/talos-rules-2025-09-15)**

The new and updated Snort rules span the following categories:

- 2 file-other rules with SIDs 65347, 65348
- 1 malware-cnc rules with SIDs 65346
- 1 malware-other rules with SIDs 65345
- 1 os-windows rules with SIDs 34058
- 4 policy-other rules with SIDs 65342, 65341, 65343, 301316
- 7 server-webapp rules with SIDs 301317, 56162, 65344, 56138, 65337, 65325, 65340

20250911

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

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

The new and updated Snort rules span the following categories:

- 1 indicator-compromise rule with SID 301314
- 2 malware-cnc rules with SIDs 301315, 65336
- 4 os-windows rules with SIDs 301312, 301313, 301310, 301311
- 1 protocol-services rule with SID 606
- 5 server-webapp rules with SIDs 58899, 58900, 65335, 58902, 58901

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

- CVE-2014-5427: Recoverable Passwords Vulnerability in Johnson Controls NAE and NIE
  - A remote attacker may be able to retrieve the password hash for an authorized Metasys user with an unauthenticated post request. Retrieved encrypted passwords could be used by a remote attacker to compromise the Metasys system.

- CVE-2014-5428: Unrestricted Upload of File with Dangerous Type Vulnerability in Johnson Controls NAE and NIE
    - Unrestricted file upload vulnerability in unspecified web services in Johnson Controls Metasys 4.1 through 6.5, as used in Application and Data Server (ADS), Extended Application and Data Server (aka ADX), LonWorks Control Server 85 LCS8520, Network Automation Engine (NAE) 55xx-x, Network Integration Engine (NIE) 5xxx-x, and NxE8500, allows remote attackers to execute arbitrary code by uploading a shell script.
- CVE-2019-10979: Hard-coded Credentials Vulnerability in SICK MSC800
    - The ICS-CERT reported a security vulnerability that affects MSC800 versions before 4.0. The MSC800 uses hard-coded credentials, which potentially allow low-skilled remote attackers to reconfigure settings and /or disrupt the functionality of the device.
- CVE-2019-7593: Reusing a Nonce, Key Pair in Encryption Vulnerability in Johnson Controls NAE/NIE/NCE
    - Metasys® ADS/ADX servers and NAE/NIE/NCE engines prior to 9.0 make use of a shared RSA key pair for certain encryption operations involving the Site Management Portal (SMP).
- CVE-2019-7594: Use of Hard-coded Cryptographic Key Vulnerability in Johnson Controls NAE/NIE/NCE
    - Metasys® ADS/ADX servers and NAE/NIE/NCE engines prior to 9.0 make use of a hardcoded RC2 key for certain encryption operations involving the Site Management Portal (SMP).
- CVE-2020-2075: Improper Handling of Exceptional Conditions Vulnerability in SICK MSC800
    - Improper handling of exceptional conditions in the platform mechanism AutoIP can lead to a reboot of the device, if parsing malformed network packets. This can lead to a temporary impact of the availability of the device. The AutoIP mechanism is used by the SOPAS Engineering Tool (SOPAS-ET), e.g. to detect SICK devices in the network and change their IP configuration. This is intended to simplify the initial setup and the maintenance of the devices. The devices listen on port 30718 for UDP broadcasts.
- CVE-2020-28895: Memory Size Calculation Underflow Vulnerability in Rockwell 1783-NATR
    - In Wind River VxWorks, memory allocator has a possible overflow in calculating the memory block's size to be allocated by calloc(). As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading to memory corruption.
- CVE-2020-9044: XML External Entity Vulnerability in Johnson Controls NAE and NIE
    - Johnson Controls has learned of a vulnerability impacting the Metasys Server software products and some network engines. The Microsoft .NET Framework low-level parser uses unsafe default parameters that makes Metasys software vulnerable to an XML External Entity Injection (XXE) attack.
- CVE-2021-27657: Improper Privilege Management Vulnerability in Johnson Controls NAE, NIE, NCE, SNC and SNE
    - Johnson Controls has confirmed a web services vulnerability impacting Metasys Servers, Engines, and SCT Tools. Successful exploitation of this vulnerability could give an authenticated Metasys user

an unintended level of access to the server file system, allowing them to access or modify system files by sending specifically crafted web messages to the Metasys system.

- CVE-2022-27577: Use of Insufficiently Random Values Vulnerability in SICK MSC800
  - The vulnerability in the MSC800 in all versions before 4.15 allows for an attacker to predict the TCP initial sequence number. When the TCP sequence is predictable, an attacker can send packets that are forged to appear to come from a trusted computer. These forged packets could compromise services on the MSC800.
- CVE-2023-4486: Uncontrolled Resource Consumption in Johnson Controls NAE55, SNE and SNC
  - Under certain circumstances, invalid authentication credentials could be sent to the login endpoint of Johnson Controls Metasys NAE55, SNE, and SNC engines prior to versions 11.0.6 and 12.0.4 and Facility Explorer F4-SNC engines prior to versions 11.0.6 and 12.0.4 to cause denial-of-service.
- CVE-2023-4523: Cross-site Scripting Vulnerability in Real Time Automation 460 Series
  - Real Time Automation 460 Series products with versions prior to v8.9.8 are vulnerable to cross-site scripting, which could allow an attacker to run any JavaScript reference from the URL string. If this were to occur, the gateway's HTTP interface would redirect to the main page, which is index.htm.
- CVE-2024-8751: Missing Authentication for Critical Function Vulnerability in SICK MSC800
  - A vulnerability in the MSC800 allows an unauthenticated attacker to modify the product's IP address over Sopas ET. This can lead to Denial of Service.
- CVE-2025-20159: Cisco IOS XR Software Management Interface ACL Bypass Vulnerability
  - A vulnerability in the management interface access control list (ACL) processing feature in Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass configured ACLs for the SSH, NetConf, and gRPC features. This vulnerability exists because management interface ACLs have not been supported on Cisco IOS XR Software Packet I/O infrastructure platforms for Linux-handled features such as SSH, NetConf, or gRPC. An attacker could exploit this vulnerability by attempting to send traffic to an affected device. A successful exploit could allow the attacker to bypass an ingress ACL that is applied on the management interface of the affected device.
- CVE-2025-20241: Cisco Nexus 3000 and 9000 Series Switches Intermediate System-to-Intermediate System Denial of Service Vulnerability
  - A vulnerability in the Intermediate System-to-Intermediate System (IS-IS) feature of Cisco NX-OS Software for Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, adjacent attacker to cause the IS-IS process to unexpectedly restart, which could cause an affected device to reload. This vulnerability is due to insufficient input validation when parsing an ingress IS-IS packet. An attacker could exploit this vulnerability by sending a crafted IS-IS packet to an affected device. A successful exploit could allow the attacker to cause the unexpected restart of the IS-IS process, which could cause the affected device to reload, resulting in a denial of service (DoS) condition.
- CVE-2025-20248: Cisco IOS XR Software Image Verification Bypass Vulnerability

  - A vulnerability in the installation process of Cisco IOS XR Software could allow an authenticated, local attacker to bypass Cisco IOS XR Software image signature verification and load unsigned software on an affected device. To exploit this vulnerability, the attacker must have root-system privileges on the affected device. This vulnerability is due to incomplete validation of files during the installation of an .iso file. An attacker could exploit this vulnerability by modifying contents of the .iso image and then installing and activating it on the device. A successful exploit could allow the attacker to load an unsigned file as part of the image activation process.

- CVE-2025-20262: Cisco Nexus 3000 and 9000 Series Switches Protocol Independent Multicast Version 6 Denial of Service Vulnerability
  - A vulnerability in the Protocol Independent Multicast Version 6 (PIM6) feature of Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an authenticated, low-privileged, remote attacker to trigger a crash of the PIM6 process, resulting in a denial of service (DoS) condition. This vulnerability is due to improper processing of PIM6 ephemeral data queries. An attacker could exploit this vulnerability by sending a crafted ephemeral query to an affected device through one of the following methods: NX-API REST, NETCONF, RESTConf, gRPC, or Model Driven Telemetry. A successful exploit could allow the attacker to cause the PIM6 process to crash and restart, causing potential adjacency flaps and resulting in a DoS of the PIM6 and ephemeral query processes.
- CVE-2025-20290: Cisco NX-OS Software Sensitive Log Information Disclosure Vulnerability
  - A vulnerability in the logging feature of Cisco NX-OS Software for Cisco Nexus 3000 Series Switches, Cisco Nexus 9000 Series Switches in standalone NX-OS mode, Cisco UCS 6400 Fabric Interconnects, Cisco UCS 6500 Series Fabric Interconnects, and Cisco UCS 9108 100G Fabric Interconnects could allow an authenticated, local attacker access to sensitive information. This vulnerability is due to improper logging of sensitive information. An attacker could exploit this vulnerability by accessing log files on the file system where they are stored. A successful exploit could allow the attacker to access sensitive information, such as stored credentials.
- CVE-2025-20292: Cisco NX-OS Software Command Injection Vulnerability
  - A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute a command injection attack on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have valid user credentials on the affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by entering crafted input as the argument of an affected CLI command. A successful exploit could allow the attacker to read and write files on the underlying operating system with the privileges of a non-root user account. File system access is limited to the permissions that are granted to that non-root user account.
- CVE-2025-20340: Cisco IOS XR ARP Broadcast Storm Denial of Service Vulnerability
  - A vulnerability in the Address Resolution Protocol (ARP) implementation of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to trigger a broadcast storm, leading to a denial of service (DoS) condition on an affected device. This vulnerability is due to how Cisco IOS XR Software processes a high, sustained rate of ARP traffic hitting the management interface. Under

certain conditions, an attacker could exploit this vulnerability by sending an excessive amount of traffic to the management interface of an affected device, overwhelming its ARP processing capabilities. A successful exploit could result in degraded device performance, loss of management connectivity, and complete unresponsiveness of the system, leading to a DoS condition.

- CVE-2025-40594: Improper Privilege Management in Siemens SINAMICS Drives
  - The affected devices allow a factory reset to be executed without the required privileges due to improper privilege management as well as manipulation of configuration data because of leaked privileges of previous sessions. This could allow an unauthorized attacker to escalate their privileges.
- CVE-2025-40757: Information Disclosure Vulnerability in Siemens Apogee PXC and Talon TC Devices
  - Affected devices connected to the network allow unrestricted access to sensitive files, such as databases. This could allow an attacker to download encrypted .db file containing passwords.
- CVE-2025-7746: Cross-site Scripting Vulnerability in Schneider Altivar Process Drives and Communication Modules
  - A Cross-site Scripting vulnerability exists that could cause an unvalidated data injected by a malicious user potentially leading to modify or read data in a victim’s browser.
- CVE-2025-9160: Improper Authentication Vulnerability in Rockwell CompactLogix 5480
  - A code execution security issue exists in the affected product. An attacker with physical access could abuse the maintenance menu of the controller with a crafted payload. The security issue can result in arbitrary code execution.
- CVE-2025-9166: Denial of Service Vulnerability in Rockwell ControlLogix 5580
  - A denial-of-service security issue exists in the affected product and version. The security issue stems from the controller repeatedly attempting to forward messages. The issue could result in a major nonrecoverable fault on the controller.
- CVE-2025-9996: OS Command Injection Vulnerability in Schneider Saitel DR & Saitel DP Remote Terminal Unit
  - An OS command injection vulnerability exists that could cause the execution of any shell command when executing a netstat command using BLMon Console in an SSH session.
- CVE-2025-9997: OS Command Injection Vulnerability in Schneider Saitel DR & Saitel DP Remote Terminal Unit
  - An OS command injection vulnerability exists that could cause command injection in BLMon that is executed in the operating system console when in a SSH session.

20250905

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

- **Talos Rules 2025-09-04 (https://www.snort.org/advisories/talos-rules-2025-09-04)**

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

The new and updated Snort rules span the following categories:

- 2 file-pdf rules with SIDs 35240, 35239
- 8 malware-cnc rules with SIDs 65322, 65317, 65320, 65318, 65316, 65319, 65321, 65315
- 1 policy-other rule with SID 65326
- 1 server-other rule with SID 65314
- 3 server-webapp rules with SIDs 65323, 65325, 65324

Vulnerabilities Update Notice

A set of previously unknown vulnerabilities in the Treck TCP/IP stack implementation were disclosed on June 16, 2020. The vulnerabilities are collectively known as Ripple20. Exploitation of these vulnerabilities could result in remote code execution, denial of service (DoS), or information disclosure, depending on the specific vulnerability.

Upon their disclosure in 2020, the Cisco development team added all these vulnerabilities to Cyber Vision to alert users. It was decided to broadly list the vulnerabilities across a large number of products using loose matching, as the impacted firmware versions were not clearly communicated by the manufacturers at the time. This included a number of Rockwell Automation devices, among other prominent OT vendors.

In the following years, manufacturers have included fixes to their firmware images, typically by embedding newer versions of Treck wholesale, not by fixing targeted vulnerabilities. As a result, they typically don’t list fixed versions in security advisories originally published in 2020, rather the fixes get rolled up in new major releases of individual firmware, making it difficult to identify which devices have been fixed. The Cisco team has therefore concluded that to minimize false positives, the best compromise was to no longer list these vulnerabilities widely, as newer firmware released in the last 5 years are likely to include a silent update to the TCP/IP stack