Release Notes for Cisco Cyber Vision Knowledge DB

Release 202505

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-5.1.3.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.1.3.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.1.3.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.1.3.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.1.3.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.1.3.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.1.3.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.1.3.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.1.3.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.1.3.dat	Knowledge DB embedded in Cisco Cyber Vision 5.1.3
Updates/KDB/KDB.202505	**Description**
CiscoCyberVision_knowledgedb_20250509.db	Knowledge DB version 20250509
CiscoCyberVision_knowledgedb_20250520.db	Knowledge DB version 20250520
CiscoCyberVision_knowledgedb_20250523.db	Knowledge DB version 20250523

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

20250523

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

- **Talos Rules 2025-05-22 (https://www.snort.org/advisories/talos-rules-2025-05-22)**

The new and updated Snort rules span the following categories:

- 1 browser-webkit rule with SID 64924
- 1 file-other rule with SID 301208
- 1 indicator-compromise rule with SID 64908
- 1 malware-backdoor rule with SID 301215
- 3 malware-cnc rules with SIDs 64930, 64931, 64932
- 4 malware-other rules with SIDs 301210, 301209, 301212, 301211
- 1 os-windows rule with SID 64921
- 7 server-other rules with SIDs 301216, 301214, 51839, 37017, 51838, 301213, 301217
- 10 server-webapp rules with SIDs 64926, 64917, 64919, 46624, 64918, 64929, 64927, 64925, 64928, 64920

20250520

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

- **Talos Rules 2025-05-20 (https://www.snort.org/advisories/talos-rules-2025-05-20)**
- **Talos Rules 2025-05-15 (https://www.snort.org/advisories/talos-rules-2025-05-15)**
- **Talos Rules 2025-05-13 (https://www.snort.org/advisories/talos-rules-2025-05-13)**

The new and updated Snort rules span the following categories:

- 1 browser-ie rule with SID 301195
- 1 file-image rule with SID 301194
- 2 file-office rules with SIDs 301200, 301196
- 1 file-other rule with SID 300742
- 6 malware-cnc rules with SIDs 64894, 64874, 64893, 64892, 64870, 64873
- 7 malware-other rules with SIDs 301204, 64896, 301207, 301206, 301202, 301201, 301205
- 8 os-windows rules with SIDs 301197, 301192, 64853, 301193, 301199, 301198, 301203, 64852
- 1 policy-other rule with SID 64889
- 8 protocol-other rules with SIDs 64881, 64905, 64877, 64904, 64903, 64880, 64879, 64878

- 1 server-other rule with SID 64888
- 7 server-webapp rules with SIDs 64895, 64884, 64887, 64886, 64885, 64876, 64875

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

- CVE-2025-24007: (Use of a Broken or Risky Cryptographic Algorithm Vulnerability in Siemens SIRIUS 3SK2 Safety Relays and 3RK3 Modular Safety Systems)
    - SIRIUS 3SK2 Safety Relays and 3RK3 Modular Safety Systems only provide weak password obfuscation. An attacker with access to the PROFINET or serial interface of the device could eavesdrop or read the stored password from the device and de-obfuscate it. The safety passwords work as protection against unauthorized operation (i.e., protection against inadvertent operating errors) but not as protection against malicious access attempts.)
- CVE-2025-24008: (Missing Encryption of Sensitive Data Vulnerability in Siemens SIRIUS 3SK2 Safety Relays and 3RK3 Modular Safety Systems)
    - The affected devices do not encrypt data in transit. An attacker with network access could eavesdrop the connection and retrieve sensitive information, including obfuscated safety passwords.)
- CVE-2025-24009: (Incorrect Permission Assignment for Critical Resource Vulnerability in Siemens SIRIUS 3SK2 Safety Relays and 3RK3 Modular Safety Systems)
    - The affected devices do not require authentication to access critical resources. An attacker with network access could retrieve sensitive information from certain data records, including obfuscated safety passwords.)
- CVE-2025-40572: (Incorrect Permission Assignment for Critical Resource Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices do not properly assign permissions to critical ressources. This could allow a non-privileged local attacker to access sensitive information stored on the device.)
- CVE-2025-40573: (Path Traversal Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices are vulnerable to path traversal attacks. This could allow a privileged local attacker to restore backups that are outside the backup folder.)
- CVE-2025-40574: (Incorrect Permission Assignment for Critical Resource Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices do not properly assign permissions to critical ressources. This could allow a non-privileged local attacker to interact with the backupmanager service.)
- CVE-2025-40575: (Use of Uninitialized Variable Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices do not properly validate incoming Profinet packets. An unauthenticated remote attacker can exploit this flaw by sending a specially crafted malicious packet, which leads to a crash of the dcpd process.)

- CVE-2025-40576: (NULL Pointer Dereference Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices do not properly validate incoming Profinet packets. An unauthenticated remote attacker can exploit this flaw by sending a specially crafted malicious packet, which leads to a crash of the dcpd process.)
- CVE-2025-40577: (Out-of-bounds Read Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices do not properly validate incoming Profinet packets. An unauthenticated remote attacker can exploit this flaw by sending a specially crafted malicious packet, which leads to a crash of the dcpd process.)
- CVE-2025-40578: (Out-of-bounds Read Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices do not properly handle multiple incoming Profinet packets received in rapid succession. An unauthenticated remote attacker can exploit this flaw by sending multiple packets in a very short time frame, which leads to a crash of the dcpd process.)
- CVE-2025-40579: (Stack-based Buffer Overflow Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices are vulnerable to a stack-based buffer overflow. This could allow a non-privileged local attacker to execute arbitrary code on the device or to cause a denial of service condition.)
- CVE-2025-40580: (Stack-based Buffer Overflow Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices are vulnerable to a stack-based buffer overflow. This could allow a non-privileged local attacker to execute arbitrary code on the device or to cause a denial of service condition.)
- CVE-2025-40581: (Authentication Bypass Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices are vulnerable to an authentication bypass. This could allow a non-privileged local attacker to bypass the authentication of the SINEMA Remote Connect Edge Client, and to read and modify the configuration parameters.)
- CVE-2025-40582: (OS Command Injection Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices do not properly sanitize configuration parameters. This could allow a non-privileged local attacker to execute root commands on the device.)
- CVE-2025-40583: (Cleartext Transmission of Sensitive Information Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices do transmit sensitive information in cleartext. This could allow a privileged local attacker to retrieve this sensitive information.)
- CVE-2024-54085: (Authentication Bypass Vulnerability in Siemens SIMATIC IPC RS-828A)
    - AMI’s SPx contains a vulnerability in the BMC where an Attacker may bypass authentication remotely through the Redfish Host Interface. A successful exploitation of this vulnerability may lead to a loss of confidentiality, integrity, and/or availability.)
- CVE-2025-40556: (Improper Input Validation Vulnerability in Siemens BACnet ATEC Devices)
    - Affected devices improperly handle specific incoming BACnet MSTP messages. This could allow an attacker residing in the same BACnet network to send a specially crafted MSTP message that results

in a denial of service condition of the targeted device. A power cycle is required to restore the device's normal operation.)

- CVE-2025-31929: (Missing Immutable Root of Trust Vulnerability in Siemens VersiCharge AC Series EV Chargers)
    - Affected devices do not contain an Immutable Root of Trust in M0 Hardware. An attacker with physical access to the device could use this to execute arbitrary code.)
- CVE-2025-31930: (Improper Initialization Vulnerability in Siemens VersiCharge AC Series EV Chargers)
    - Affected devices contain Modbus service enabled by default. This could allow an attacker connected to the same network to remotely control the EV charger.)
- CVE-2025-2875: (Externally Resource Reference Vulnerability in Schneider Modicon Controllers M241/M251/M258/LMC058)
    - An Externally Controlled Reference to a Resource in Another Sphere vulnerability (CWE-610) exists that could cause a loss of confidentiality when an unauthenticated attacker manipulates controller's webserver URL to access resources)

20250509

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

- **Talos Rules 2025-05-08 (https://www.snort.org/advisories/talos-rules-2025-05-08)**
- **Talos Rules 2025-05-06 (https://www.snort.org/advisories/talos-rules-2025-05-06)**
- **Talos Rules 2025-05-01 (https://www.snort.org/advisories/talos-rules-2025-05-01)**
- **Talos Rules 2025-04-29 (https://www.snort.org/advisories/talos-rules-2025-04-29)**

The new and updated Snort rules span the following categories:

- 1 app-detect rule with SID 301190
- 1 indicator-scan rule with SID 64815
- 1 malware-cnc rule with SID 64816
- 3 os-other rules with SIDs 31976, 64846, 64847
- 4 os-windows rules with SIDs 300133, 301035, 301191, 301188
- 7 policy-other rules with SIDs 301189, 64830, 64825, 64840, 64826, 64845, 64839
- 2 protocol-other rules with SIDs 64836, 64837
- 3 server-other rules with SIDs 64788, 52287, 64844
- 16 server-webapp rules with SIDs 64828, 64813, 64832, 64726, 64833, 64834, 64829, 64831, 64827, 64843, 64814, 64821, 64822, 64823, 64838, 64824