Release Notes for Cisco Cyber Vision Knowledge DB

Release 202508

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-5.2.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.2.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.2.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.2.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.2.1.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.2.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.2.1.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.2.1.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.2.1.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.2.1.dat	Knowledge DB embedded in Cisco Cyber Vision 5.2.1
Updates/KDB/KDB.202508	**Description**
CiscoCyberVision_knowledgedb_20250801.db	Knowledge DB version 20250801
CiscoCyberVision_knowledgedb_20250808.db	Knowledge DB version 20250808
CiscoCyberVision_knowledgedb_20250822.db	Knowledge DB version 20250822
CiscoCyberVision_knowledgedb_20250829.db	Knowledge DB version 20250829

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

20250829

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

- **Talos Rules 2025-08-28 (https://www.snort.org/advisories/talos-rules-2025-08-28)**
- **Talos Rules 2025-08-26 (https://www.snort.org/advisories/talos-rules-2025-08-26)**

The new and updated Snort rules span the following categories:

- 10 file-other rules with SIDs 301308, 301208, 65279, 65267, 65278, 65266, 65268, 65271, 65269, 65270
- 3 malware-backdoor rules with SIDs 65273, 65275, 65274
- 2 malware-cnc rules with SIDs 65248, 65276
- 1 malware-other rule with SID 65233
- 8 os-windows rules with SIDs 301300, 65241, 61303, 65240, 301301, 301304, 301305, 301306
- 6 policy-other rules with SIDs 65260, 60599, 65286, 65284, 65283, 65285
- 1 protocol-dns rule with SID 65256
- 6 server-other rules with SIDs 65280, 54575, 54518, 54576, 54577, 65272
- 21 server-webapp rules with SIDs 65252, 65238, 62383, 65230, 65277, 65250, 65253, 65282, 301307, 301303, 65281, 301302, 65251, 64941, 65249, 65257, 65264, 65263, 65262, 65261, 65265

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

- CVE-2025-20224: Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerabilities
  - Multiple vulnerabilities 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 denial of service (DoS) condition.
- CVE-2025-20225: Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerabilities
  - Multiple vulnerabilities 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 denial of service (DoS) condition.
- CVE-2025-20239: Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerabilities

    - Multiple vulnerabilities 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 denial of service (DoS) condition.
- CVE-2025-20252: Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerabilities
    - Multiple vulnerabilities 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 denial of service (DoS) condition.
- CVE-2025-20253: Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerabilities
    - Multiple vulnerabilities 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 denial of service (DoS) condition.
- CVE-2025-20254: Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software IKEv2 Denial of Service Vulnerabilities
    - Multiple vulnerabilities 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 denial of service (DoS) condition.

20250822

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

- **Talos Rules 2025-08-21 (https://www.snort.org/advisories/talos-rules-2025-08-21)**
- **Talos Rules 2025-08-19 (https://www.snort.org/advisories/talos-rules-2025-08-19)**
- **Talos Rules 2025-08-14 (https://www.snort.org/advisories/talos-rules-2025-08-14)**
- **Talos Rules 2025-08-12 (https://www.snort.org/advisories/talos-rules-2025-08-12)**

The new and updated Snort rules span the following categories:

- 10 file-other rules with SIDs 301308, 301208, 65279, 65267, 65278, 65266, 65268, 65271, 65269, 65270
- 3 malware-backdoor rules with SIDs 65273, 65275, 65274
- 2 malware-cnc rules with SIDs 65248, 65276
- 1 malware-other rule with SID 65233
- 8 os-windows rules with SIDs 301300, 65241, 61303, 65240, 301301, 301304, 301305, 301306
- 6 policy-other rules with SIDs 65260, 60599, 65286, 65284, 65283, 65285

- 1 protocol-dns rule with SID 65256
- 6 server-other rules with SIDs 65280, 54575, 54518, 54576, 54577, 65272
- 21 server-webapp rules with SIDs 65252, 65238, 62383, 65230, 65277, 65250, 65253, 65282, 301307, 301303, 65281, 301302, 65251, 64941, 65249, 65257, 65264, 65263, 65262, 65261, 65265

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

- CVE-2023-48691: Out-of-bounds Write Vulnerability in Rockwell Micro800
    - Azure RTOS NetX Duo is a TCP/IP network stack designed specifically for deeply embedded real-time and IoT applications. An attacker can cause an out-of-bounds write in Azure RTOS NETX Duo, that could lead to remote code execution. The affected components include a process related to IGMP protocol in RTOS v6.2.1 and below. The fix has been included in NetX Duo release 6.3.0. Users are advised to upgrade.
- CVE-2023-48692: Out-of-bounds Write Vulnerability in Rockwell Micro800
    - Azure RTOS NetX Duo is a TCP/IP network stack designed specifically for deeply embedded real-time and IoT applications. An attacker can cause remote code execution due to memory overflow vulnerabilities in Azure RTOS NETX Duo. The affected components include processes/functions related to icmp, tcp, snmp, dhcp, nat and ftp in RTOS v6.2.1 and below. The fixes have been included in NetX Duo release 6.3.0. Users are advised to upgrade.
- CVE-2023-48693: Improper Input Validation Vulnerability in Rockwell Micro800
    - Azure RTOS ThreadX is an advanced real-time operating system (RTOS) designed specifically for deeply embedded applications. An attacker can cause arbitrary read and write due to vulnerability in parameter checking mechanism in Azure RTOS ThreadX, which may lead to privilege escalation. The affected components include RTOS ThreadX v6.2.1 and below. The fixes have been included in ThreadX release 6.3.0. Users are advised to upgrade.
- CVE-2024-52504: Denial of Service Vulnerability in Siemens SIPROTEC 4 and SIPROTEC 4 Compact
    - Affected devices do not properly handle interrupted operations of file transfer. This could allow an unauthenticated remote attacker to cause a denial of service condition. To restore normal operations, the devices need to be restarted.
- CVE-2025-33023: Arbitrary File Upload Vulnerability in Siemens RUGGEDCOM ROX II
    - RUGGEDCOM ROX II devices does not properly enforce limitations on type and size of files that can be uploaded through their web interface. This could allow an attacker with a legitimate, highly privileged account on the web interface to upload arbitrary files onto the filesystem of the devices.
- CVE-2025-40570: Improper Bandwidth Limitation of Network Packets Over Local USB Port Vulnerability in Siemens SIPROTEC 5
    - Affected devices do not properly limit the bandwidth for incoming network packets over their local USB port. This could allow an attacker with physical access to send specially crafted packets with high bandwidth to the affected devices thus forcing them to exhaust their memory and stop

responding to any network traffic via the local USB port. Affected devices reset themselves automatically after a successful attack. The protection function is not affected of this vulnerability.

- CVE-2025-40752: Cleartext Storage of Sensitive Information Vulnerability in Siemens SICAM Q100/Q200
  - Affected devices store the password for the SMTP account as plain text. This could allow an authenticated local attacker to extract it and use the configured SMTP service for arbitrary purposes.
- CVE-2025-40753: Cleartext Storage of Sensitive Information Vulnerability in Siemens SICAM Q100/Q200
  - Affected devices export the password for the SMTP account as plain text in the Configuration File. This could allow an authenticated local attacker to extract it and use the configured SMTP service for arbitrary purposes.
- CVE-2025-6625: Improper Input Validation Vulnerability in Schneider Modicon M340 Controller and Communication Modules
  - An Improper Input Validation vulnerability exists that could cause a Denial Of Service when specific crafted FTP command is sent to the device
- CVE-2025-7353: Remote Code Execution Vulnerability in Rockwell ControlLogix Ethernet
  - A security issue exists due to the web-based debugger agent enabled on released devices. If a specific IP address is used to connect to the WDB agent, it can allow remote attackers to perform memory dumps, modify memory, and control execution flow.
- CVE-2025-7693: Improper Input Validation Vulnerability in Rockwell Micro800
  - A security issue exists due to improper handling of malformed CIP Forward Close packets during fuzzing. The controller enters a solid red Fault LED state and becomes unresponsive. Upon power cycle, the controller will enter recoverable fault where the MS LED and Fault LED become flashing red and reports fault code 0xF015. To recover, clear the fault.
- CVE-2025-7773: Incorrect Authorization Vulnerability in Rockwell ArmorBlock 5000 I/O
  - A security issue exists within the 5032 16pt Digital Configurable module’s web server. The web server’s session number increments at an interval that correlates to the last two consecutive sign in session interval, making it predictable.
- CVE-2025-7774: Missing Authentication for Critical Function Vulnerability in Rockwell ArmorBlock 5000 I/O
  - A security issue exists within the 5032 16pt Digital Configurable module’s web server. Intercepted session credentials can be used within a 3-minute timeout window, allowing unauthorized users to perform privileged actions.
- CVE-2025-8453: Improper Privilege Management Vulnerability in Schneider Saitel DR & Saitel DP Remote Terminal Unit
  - An Improper Privilege Management vulnerability exists that could cause privilege escalation and arbitrary code execution when a privileged engineer user with console access modifies a configuration file used by a root-level daemon to execute custom scripts.

- CVE-2025-9041: Improper Input Validation in Rockwell FLEX 5000 I/O
    - A security issue exists due to improper handling of CIP Class 32's request when a module is inhibited on the 5094-IF8 device. It causes the module to enter a fault state with the Module LED flashing red. Upon un-inhibiting, the module returns a connection fault (Code 16#0010), and the module cannot recover without a power cycle.
- CVE-2025-9042: Improper Input Validation in Rockwell FLEX 5000 I/O
    - A security issue exists due to improper handling of CIP Class 32's request when a module is inhibited on the 5094-IY8 device. It causes the module to enter a fault state with the Module LED flashing red. Upon un-inhibiting, the module returns a connection fault (Code 16#0010), and the module cannot recover without a power cycle.

20250808

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

- **Talos Rules 2025-08-07 (https://www.snort.org/advisories/talos-rules-2025-08-07)**
- **Talos Rules 2025-08-05 (https://www.snort.org/advisories/talos-rules-2025-08-05)**

The new and updated Snort rules span the following categories:

- 8 file-image rules with SIDs 65219, 65221, 65217, 65224, 65220, 65218, 65223, 65222
- 2 file-other rules with SIDs 65225, 65226
- 3 malware-cnc rules with SIDs 65215, 301299, 301298
- 1 policy-other rule with SID 65228
- 1 server-other rule with SID 65062
- 3 server-webapp rules with SIDs 65229, 65214, 65227

20250801

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

- **Talos Rules 2025-07-31 (https://www.snort.org/advisories/talos-rules-2025-07-31)**
- **Talos Rules 2025-07-29 (https://www.snort.org/advisories/talos-rules-2025-07-29)**

The new and updated Snort rules span the following categories:

- 1 malware-backdoor rule with SID 65183
- 14 malware-cnc rules with SIDs 65187, 65146, 65182, 65145, 65143, 65142, 65147, 65144, 65148, 65151, 65152, 65150, 65149, 65177
- 14 malware-other rules with SIDs 301290, 301291, 301286, 301287, 301281, 301284, 301283, 301280, 301288, 301278, 301282, 301289, 301285, 301279
- 1 os-solaris rule with SID 10136

- 1 policy-other rule with SID 51377
- 1 server-mail rule with SID 65064
- 1 server-other rule with SID 59881
- 8 server-webapp rules with SIDs 65060, 65092, 65184, 65179, 65178, 65066, 58549, 58550