Release Notes for Cisco Cyber Vision Knowledge DB

Release 202503

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-5.1.2.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.1.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.1.2.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.1.2.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.1.2.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.1.2.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.1.2.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.1.2.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.1.2.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.1.2.dat	Knowledge DB embedded in Cisco Cyber Vision 5.1.2
Updates/KDB/KDB.202503	**Description**
CiscoCyberVision_knowledgedb_20250307.db	Knowledge DB version 20250307
CiscoCyberVision_knowledgedb_20250314.db	Knowledge DB version 20250314
CiscoCyberVision_knowledgedb_20250321.db	Knowledge DB version 20250321

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

20250321

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

- **Talos Rules 2025-03-20 (https://www.snort.org/advisories/talos-rules-2025-03-20)**
- **Talos Rules 2025-03-18 (https://www.snort.org/advisories/talos-rules-2025-03-18)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 64675
- 3 browser-plugins rules with SIDs 33070, 33071, 64680
- 1 file-multimedia rule with SID 38124
- 2 file-other rules with SIDs 300814, 301167
- 2 malware-cnc rules with SIDs 64677, 64683
- 4 os-windows rules with SIDs 300612, 64676, 61303, 59212
- 2 server-webapp rules with SIDs 64679, 6467

20250314

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

- **Talos Rules 2025-03-13 (https://www.snort.org/advisories/talos-rules-2025-03-13)**
- **Talos Rules 2025-03-11 (https://www.snort.org/advisories/talos-rules-2025-03-11)**

The new and updated Snort rules span the following categories:

- 2 file-image rules with SIDs 55742, 55741
- 1 file-pdf rules with SIDs 16343
- 4 malware-cnc rules with SIDs 64667, 64669, 64674, 64668
- 5 os-windows rules with SIDs 301166, 301163, 301165, 64432, 301164
- 1 policy-other rules with SIDs 301162
- 9 server-webapp rules with SIDs 64131, 64666, 64665, 64671, 64672, 64664, 64670, 64673, 64655

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

- CVE-2024-56336: (Improper Authentication Vulnerability in Siemens SINAMICS S200)
    - The affected device contains an unlocked bootloader. This security oversight enables attackers to inject malicious code, or install untrusted firmware. The intrinsic security features designed to

protect against data manipulation and unauthorized access are compromised when the bootloader is not secured.)

- CVE-2025-23384: (Partial String Comparison Vulnerability in Siemens SCALANCE M-800 and SC-600 Families)
    - Affected devices improperly validate usernames during OpenVPN authentication. This could allow an attacker to get partial invalid usernames accepted by the server.)
- CVE-2024-56181: (Protection Mechanism Failure Vulnerability in Siemens SIMATIC IPCs, SIMATIC Tablet PCs, and SIMATIC Field PGs)
    - The affected devices have insufficient protection mechanism for the EFI(Extensible Firmware Interface) variables stored on the device. This could allow an authenticated attacker to alter the secure boot configuration without proper authorization by directly communicate with the flash controller.)
- CVE-2024-56182: (Protection Mechanism Failure Vulnerability in Siemens SIMATIC IPCs, SIMATIC Tablet PCs, and SIMATIC Field PGs)
    - The affected devices have insufficient protection mechanism for the EFI(Extensible Firmware Interface) variables stored on the device. This could allow an authenticated attacker to disable the BIOS password without proper authorization by directly communicate with the flash controller.)
- CVE-2025-27392: (OS Command Injection Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices do not properly sanitize user input when creating new VXLAN configurations. This could allow an authenticated highly-privileged remote attacker to execute arbitrary code on the device.)
- CVE-2025-27393: (OS Command Injection Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices do not properly sanitize user input when creating new users. This could allow an authenticated highly-privileged remote attacker to execute arbitrary code on the device.)
- CVE-2025-27394: (OS Command Injection Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices do not properly sanitize user input when creating new SNMP users. This could allow an authenticated highly-privileged remote attacker to execute arbitrary code on the device.)
- CVE-2025-27395: (Path Traversal Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices do not properly limit the scope of files accessible through and the privileges of the SFTP functionality. This could allow an authenticated highly-privileged remote attacker to read and write arbitrary files.)
- CVE-2025-27396: (Improper Check for Dropped Privileges Vulnerability in Siemens SCALANCE LPE9403)
    - Affected devices do not properly limit the elevation of privileges required to perform certain valid functionality. This could allow an authenticated lowly-privileged remote attacker to escalate their privileges)
- CVE-2025-27397: (Improper Check for Dropped Privileges Vulnerability in Siemens SCALANCE LPE9403)

  - Affected devices do not properly limit user controlled paths to which logs are written and from where they are read. This could allow an authenticated highly-privileged remote attacker to read and write arbitrary files in the filesystem, if and only if the malicious path ends with 'log')

- CVE-2025-27398: (OS Command Injection Vulnerability in Siemens SCALANCE LPE9403)
  - Affected devices do not properly neutralize special characters when interpreting user controlled log paths. This could allow an authenticated highly-privileged remote attacker to execute a limited set of binaries that are already present on the filesystem.)
- CVE-2025-20177: (Cisco IOS XR Software Image Verification Bypass Vulnerability)
  - A vulnerability in the boot process of Cisco IOS XR Software could allow an authenticated, local attacker to bypass Cisco IOS XR image signature verification and load unverified 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 in the boot verification process. An attacker could exploit this vulnerability by manipulating the system configuration options to bypass some of the integrity checks that are performed during the boot process. A successful exploit could allow the attacker to control the boot configuration, which could enable them to bypass the requirement to run Cisco-signed images or alter the security properties of the running system.
- CVE-2025-20144: (Cisco IOS XR Software Hybrid Access Control List Bypass Vulnerability)
  - A vulnerability in the hybrid access control list (ACL) processing of IPv4 packets in Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to incorrect handling of packets when a specific configuration of the hybrid ACL exists. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to bypass a configured ACL on the affected device.
- CVE-2025-20138: (Cisco IOS XR Software CLI Privilege Escalation Vulnerability)
  - A vulnerability in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker 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 with a low-privileged account could exploit this vulnerability by using crafted commands at the prompt. A successful exploit could allow the attacker to elevate privileges to root and execute arbitrary commands.
- CVE-2025-20209: (Cisco IOS XR Software Internet Key Exchange Version 2 Denial of Service Vulnerability)
  - A vulnerability in the Internet Key Exchange version 2 (IKEv2) function of Cisco IOS XR Software could allow an unauthenticated, remote attacker to prevent an affected device from processing any control plane UDP packets. This vulnerability is due to improper handling of malformed IKEv2 packets. An attacker could exploit this vulnerability by sending malformed IKEv2 packets to an affected device. A successful exploit could allow the attacker to prevent the affected device from processing any control plane UDP packets, resulting in a denial of service (DoS) condition.
- CVE-2025-20141: (Cisco IOS XR Software Release 7.9.2 Denial of Service Vulnerability)

  - A vulnerability in the handling of specific packets that are punted from a line card to a route processor in Cisco IOS XR Software Release 7.9.2 could allow an unauthenticated, adjacent attacker to cause control plane traffic to stop working on multiple Cisco IOS XR platforms. This vulnerability is due to incorrect handling of packets that are punted to the route processor. An attacker could exploit this vulnerability by sending traffic, which must be handled by the Linux stack on the route processor, to an affected device. A successful exploit could allow the attacker to cause control plane traffic to stop working, resulting in a denial of service (DoS) condition.

- CVE-2025-20143: (Cisco IOS XR Software Secure Boot Bypass Vulnerability)

  - A vulnerability in the boot process of Cisco IOS XR Software could allow an authenticated, local attacker with high privileges to bypass the Secure Boot functionality and load unverified 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 insufficient verification of modules in the software load process. An attacker could exploit this vulnerability by manipulating the loaded binaries to bypass some of the integrity checks that are performed during the booting process. A successful exploit could allow the attacker to control the boot configuration, which could enable them to bypass the requirement to run Cisco-signed images or alter the security properties of the running system.

- CVE-2025-20142: (Cisco IOS XR Software for ASR 9000 Series Routers IPv4 Unicast Packets Denial of Service Vulnerability)

  - A vulnerability in the IPv4 access control list (ACL) feature and quality of service (QoS) policy feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed IPv4 packets that are received on line cards where the interface has either an IPv4 ACL or QoS policy applied. An attacker could exploit this vulnerability by sending crafted IPv4 packets through an affected device. A successful exploit could allow the attacker to cause network processor errors, resulting in a reset or shutdown of the network process. Traffic over that line card would be lost while the line card reloads. Note: This vulnerability has predominantly been observed in Layer 2 VPN (L2VPN) environments where an IPv4 ACL or QoS policy has been applied to the bridge virtual interface. Layer 3 configurations where the interface has either an IPv4 ACL or QoS policy applied are also affected, though the vulnerability has not been observed.

- CVE-2025-20145: (Cisco IOS XR Software Access Control List Bypass Vulnerability)

  - A vulnerability in the access control list (ACL) processing in the egress direction of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability exists because certain packets are handled incorrectly when they are received on an ingress interface on one line card and destined out of an egress interface on another line card where the egress ACL is configured. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to bypass an egress ACL on the affected device.

- CVE-2025-20146: (Cisco IOS XR Software for ASR 9000 Series Routers Layer 3 Multicast Denial of Service Vulnerability)
    - A vulnerability in the Layer 3 multicast feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed IPv4 multicast packets that are received on line cards where the interface has either an IPv4 access control list (ACL) or a QoS policy applied. An attacker could exploit this vulnerability by sending crafted IPv4 multicast packets through an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset. Traffic over that line card would be lost while the line card reloads.
- CVE-2025-20115: (Cisco IOS XR Software Border Gateway Protocol Confederation Denial of Service Vulnerability)
    - A vulnerability in confederation implementation for the Border Gateway Protocol (BGP) in Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to a memory corruption that occurs when a BGP update is created with an AS_CONFED_SEQUENCE attribute that has 255 autonomous system numbers (AS numbers). An attacker could exploit this vulnerability by sending a crafted BGP update message, or the network could be designed in such a manner that the AS_CONFED_SEQUENCE attribute grows to 255 AS numbers or more. A successful exploit could allow the attacker to cause memory corruption, which may cause the BGP process to restart, resulting in a DoS condition. To exploit this vulnerability, an attacker must control a BGP confederation speaker within the same autonomous system as the victim, or the network must be designed in such a manner that the AS_CONFED_SEQUENCE attribute grows to 255 AS numbers or more.
- CVE-2025-20111: (Cisco Nexus 3000 and 9000 Series Switches Health Monitoring Diagnostics Denial of Service Vulnerability)
    - A vulnerability in the health monitoring diagnostics of 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 device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of specific Ethernet frames. An attacker could exploit this vulnerability by sending a sustained rate of crafted Ethernet frames to an affected device. A successful exploit could allow the attacker to cause the device to reload.
- CVE-2025-20161: (Cisco Nexus 3000 and 9000 Series Switches Command Injection Vulnerability)
    - A vulnerability in the software upgrade process of Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an authenticated, local attacker with valid Administrator credentials to execute a command injection attack on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of specific elements within a software image. An attacker could exploit this vulnerability by installing a crafted image. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.

20250307

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

- **Talos Rules 2025-03-06 (https://www.snort.org/advisories/talos-rules-2025-03-06)**
- **Talos Rules 2025-03-04 (https://www.snort.org/advisories/talos-rules-2025-03-04)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 301160
- 3 file-image rules with SIDs 300115, 300116, 301158
- 2 file-multimedia rules with SIDs 64634, 64635
- 2 file-office rules with SIDs 301155, 64623
- 1 file-other rule with SID 301159
- 1 indicator-obfuscation rule with SID 64622
- 1 malware-cnc rule with SID 64624
- 2 malware-other rules with SIDs 301156, 301157
- 1 policy-spam rule with SID 301161
- 1 server-apache rule with SID 63187
- 3 server-other rules with SIDs 25780, 12685, 30507
- 14 server-webapp rules with SIDs 64628, 64627, 64629, 62789, 64648, 46627, 64638, 64643, 46624, 64649, 46625, 46626, 64637, 64639