Release Notes for Cisco Cyber Vision Knowledge DB

Release 202410

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-5.0.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.0.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.0.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.0.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.0.1.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.0.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.0.1.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.0.1.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.0.1.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.0.1.dat	Knowledge DB embedded in Cisco Cyber Vision 5.0.1
Updates/KDB/KDB.202410	**Description**
CiscoCyberVision_knowledgedb_20241004.db	Knowledge DB version 20241004
CiscoCyberVision_knowledgedb_20241011.db	Knowledge DB version 20241011
CiscoCyberVision_knowledgedb_20241018.db	Knowledge DB version 20241018
CiscoCyberVision_knowledgedb_20241025.db	Knowledge DB version 20241025
CiscoCyberVision_knowledgedb_20241031.db	Knowledge DB version 20241031

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

20241031

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

- **Talos Rules 2024-10-31 (https://www.snort.org/advisories/talos-rules-2024-10-31)**
- **Talos Rules 2024-10-29 (https://www.snort.org/advisories/talos-rules-2024-10-29)**

The new and updated Snort rules span the following categories:

- 1 browser-firefox rule with SID 301053
- 1 file-multimedia rule with SID 301051
- 5 malware-cnc rules with SIDs 64180, 64179, 64168, 64167, 64169
- 1 malware-other rule with SID 64178
- 1 os-linux rule with SID 301052
- 1 protocol-snmp rule with SID 60839
- 3 server-other rules with SIDs 64177, 16514, 5316
- 9 server-webapp rules with SIDs 63856, 64164, 64165, 64163, 56579, 64166, 64172, 64174, 64173

20241025

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

- **Talos Rules 2024-10-22 (https://www.snort.org/advisories/talos-rules-2024-10-22)**

The new and updated Snort rules span the following categories:

- 17 malware-cnc rules with SIDs 64158, 64162, 64160, 64159, 64154, 64155, 64157, 64161, 64156, 301046, 301049, 301044, 301047, 301048, 64153, 301050, 301045
- 1 policy-other rule with SID 63460
- 3 server-webapp rules with SIDs 64136, 64137, 64138

20241018

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

- **Talos Rules 2024-10-17 (https://www.snort.org/advisories/talos-rules-2024-10-17)**
- **Talos Rules 2024-10-15 (https://www.snort.org/advisories/talos-rules-2024-10-15)**

The new and updated Snort rules span the following categories:

- 2 file-image rules with SIDs 64130, 64129
- 1 malware-cnc rule with SID 64127

- 1 malware-other rule with SID 64128
- 1 os-windows rule with SID 64125
- 4 policy-other rules with SIDs 64123, 64124, 64135, 64134
- 1 server-mail rule with SID 64126
- 12 server-other rules with SIDs 27771, 27122, 27571, 27773, 27125, 27769, 27770, 27539, 27170, 27772, 28227, 27124
- 4 server-webapp rules with SIDs 63856, 64131, 64132, 64133

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

- CVE-2024-41798: (Improper Authentication Vulnerability in Siemens SENTRON PAC3200)
    - Affected devices only provide a 4-digit PIN to protect from administrative access via Modbus TCP interface. Attackers with access to the Modbus TCP interface could easily bypass this protection by brute-force attacks or by sniffing the Modbus clear text communication.
- CVE-2024-46887: (Unauthenticated Information Disclosure in Web Server of Siemens SIMATIC S7-1500 CPUs)
    - The web server of affected devices do not properly authenticate user request to the '/ClientArea/Run-timeInfoData.mwsl' endpoint. This could allow an unauthenticated remote attacker to gain knowledge about current actual and configured maximum cycle times as well as about configured maximum communication load.
- CVE-2024-9137: (Missing Authentication for Critical Function Vulnerability in Moxa Cellular Routers, Secure Routers, and Network Security Appliances)
    - The affected product lacks an authentication check when sending commands to the server via the Moxa service. This vulnerability allows an attacker to execute specified commands, potentially leading to unauthorized downloads or uploads of configuration files and system compromise.
- CVE-2024-9139: (OS Command Injection Vulnerability in Moxa Cellular Routers, Secure Routers, and Network Security Appliances)
    - The affected product permits OS command injection through improperly restricted commands, potentially allowing attackers to execute arbitrary code.
- CVE-2024-6207: (Improper Input Validation in Rockwell ControlLogix devices)
    - A denial-of-service vulnerability exists in the affected products that will cause the device to result in a major nonrecoverable fault (MNRF) when it receives an invalid CIP request. To exploit this vulnerability a malicious user must chain this exploits with CVE-2021-2268 and send a specially crafted CIP message to the device. If exploited, a threat actor could help prevent access to the legitimate user and end connections to connected devices including the workstation. To recover the controllers, a download is required which ends any process that the controller is running.
- CVE-2024-9124: (Improper Check for Unusual or Exceptional Conditions in Rockwell PowerFlex 6000T)

- A denial-of-service vulnerability exists in the PowerFlex® 6000T. If the device is overloaded with requests, it will become unavailable. The device may require a power cycle to recover it if it does not re-establish a connection after it stops receiving requests.

20241011

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

- **Talos Rules 2024-10-10 (https://www.snort.org/advisories/talos-rules-2024-10-10)**
- **Talos Rules 2024-10-08 (https://www.snort.org/advisories/talos-rules-2024-10-08)**

The new and updated Snort rules span the following categories:

- 1 malware-cnc rules with SIDs 64116
- 15 malware-other rules with SIDs 301043, 301042, 64104, 301039, 301040, 64109, 64108, 64106, 64105, 301037, 64107, 301038, 64110, 64122, 64121
- 2 os-other rules with SIDs 64088, 64087
- 4 os-windows rules with SIDs 301034, 301035, 301041, 301036
- 1 policy-other rules with SIDs 64082
- 10 server-webapp rules with SIDs 64119, 64080, 64100, 64115, 64103, 64081, 64101, 64091, 64120, 64102

20241004

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

- **Talos Rules 2024-10-03 (https://www.snort.org/advisories/talos-rules-2024-10-03)**
- **Talos Rules 2024-10-01 (https://www.snort.org/advisories/talos-rules-2024-10-01)**

The new and updated Snort rules span the following categories:

- 6 file-pdf rules with SIDs 64067, 64068, 64066, 64063, 64064, 64065
- 3 malware-cnc rules with SIDs 64056, 64054, 64072
- 8 malware-other rules with SIDs 301030, 64074, 301029, 301031, 64073, 64075, 64076, 301032
- 1 os-windows rules with SIDs 301033
- 5 server-webapp rules with SIDs 64071, 64078, 64055, 64079, 64077