Release Notes for Cisco Cyber Vision Knowledge DB

Release 202212

Compatible device list

Center	Description
All version 4 centers	All Cisco Cyber Vision center version 4 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-4.1.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.1.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.1.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.1.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.1.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.1.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.1.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.1.0.dat	Knowledge DB embedded in Cisco Cyber Vision 4.1.0
Updates/KDB/KDB.202212	**Description**
CiscoCyberVision_knowledgedb_20221202.db	Knowledge DB version 20221202
CiscoCyberVision_knowledgedb_20221209.db	Knowledge DB version 20221209
CiscoCyberVision_knowledgedb_20221216.db	Knowledge DB version 20221216
CiscoCyberVision_knowledgedb_20221223.db	Knowledge DB version 20221223

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

20221223

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

- **Talos Rules 2022-12-22 (https://www.snort.org/advisories/talos-rules-2022-12-22)**
  - Talos has added and modified multiple rules in the browser-chrome, file-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-12-20 (https://www.snort.org/advisories/talos-rules-2022-12-20)**
  - Talos has added and modified multiple rules in the file-identify, file-other, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.

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

- CVE-2022-3157: (Improper Input Validation Vulnerability in Rockwell GuardLogix and ControlLogix controllers)
  - An improper input validation vulnerability exists in affected versions of Rockwell Automation controllers that could allow a malformed CIP request to cause a major nonrecoverable fault and a denial-of-service condition.
- CVE-2022-3166: (Insufficient Verification of Data Authenticity in Rockwell Micrologix 1100 and 1400)
  - The affected products have a clickjacking vulnerability where an attacker with network access to the affected systems could send TCP packets to the webserver, closing it abruptly. This could cause a denial-of-service condition for the web server application on the device.
- CVE-2022-46670: (Cross-site Scripting Vulnerability in Rockwell Micrologix 1100 and 1400)
  - The affected products have an unauthenticated stored cross-site scripting vulnerability in the embedded webserver. The payload is transferred to the controller over simple network management protocol (SNMP) and is rendered on the homepage of the embedded website. Exploitation of this vulnerability could result in unauthenticated remote code execution.

20221216

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

- **Talos Rules 2022-12-15 (https://www.snort.org/advisories/talos-rules-2022-12-15)**
  - Talos has added and modified multiple rules in the file-office, file-other, file-pdf and policy-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-12-13 (https://www.snort.org/advisories/talos-rules-2022-12-13)**
  - Talos has added and modified multiple rules in the browser-chrome, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.

- Microsoft Vulnerability CVE-2022-44673: A coding deficiency exists in Microsoft Windows Client Server Run-time Subsystem (CSRSS) that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort 2: GID 1, SIDs 60972 through 60973, Snort 3: GID 1, SID 300339.
- Microsoft Vulnerability CVE-2022-44675: A coding deficiency exists in Microsoft Windows Bluetooth Driver that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort 2: GID 1, SIDs 60977 through 60978, Snort 3: GID 1, SID 300341.
- Microsoft Vulnerability CVE-2022-44683: A coding deficiency exists in Microsoft Windows Kernel that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort 2: GID 1, SIDs 60974 through 60975, Snort 3: GID 1, SID 300340.
- Talos also has added and modified multiple rules in the indicator-compromise, malware-cnc and protocol-scada rule sets to provide coverage for emerging threats from these technologies.

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

- CVE-2020-28388: (Random Number Issues in Siemens APOGEE/TALON Field Panels)
    - A TCP sequence vulnerability in the APOGEE PXC and TALON TC series of products could allow an attacker to execute a denial of service attack by sending specially crafted packets to the device.
- CVE-2021-40365: (Improper Input Validation Vulnerability in Siemens industrial products)
    - Affected devices don’t process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial-of-service in the device.
- CVE-2022-32206: (Uncontrolled Resource Consumption Vulnerability in Siemens SCALANCE SC-600 Family)
    - curl < 7.84.0 supports "chained" HTTP compression algorithms, meaning that a serverresponse can be compressed multiple times and potentially with different algorithms. The number of acceptable "links" in this "decompression chain" was unbounded, allowing a malicious server to insert a virtually unlimited number of compression steps.The use of such a decompression chain could result in a "malloc bomb", making curl end up spending enormous amounts of allocated heap memory, or trying toand returning out of memory
- CVE-2021-44694: (Improper Input Validation Vulnerability in Siemens industrial products)
    - Affected devices don’t process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial-of-service in the device.
- CVE-2018-25032: (Buffer Overflow Vulnerability in Siemens SCALANCE SC-600 Family)

    - zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches

- CVE-2022-46353: (Insufficient Random Values Vulnerability in Siemens SCALANCE X-200RNA Switch Devices)
    - The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions.
- CVE-2022-46354: (Sensitive Information Exposure Vulnerability in Siemens SCALANCE X-200RNA Switch Devices)
    - The affected products are vulnerable to an "Exposure of Sensitive Information to an Unauthorized Actor" vulnerability by leaking sensitive data in the HTTP Referer.
- CVE-2022-32205: (Uncontrolled Resource Consumption Vulnerability in Siemens SCALANCE SC-600 Family)
    - A malicious server can serve excessive amounts of "Set-Cookie:" headers in a HTTP response to curl and curl < 7.84.0 stores all of them. A sufficiently large amount of (big) cookies make subsequent HTTP requests to this, or other servers to which the cookies match, create requests that become larger than the threshold that curl uses internally to avoid sending crazy large requests (1048576 bytes) and instead returns an error.This denial state might remain for as long as the same cookies are kept, match and haven't expired. Due to cookie matching rules, a server on "foo.example.com" can set cookies that also would match for "bar.example.com", making it it possible for a "sister server" to effectively cause a denial of service for a sibling site on the same second level domain using this method.
- CVE-2020-6996: (Buffer Overflow Vulnerability in Schneider Saitel DR RTU)
    - An Out-of-bounds write vulnerability exists that could cause a denial of service when an attacker gains access to the RTU communication network.
- CVE-2015-6574: (Resource Management Errors in Siemens SIPROTEC 5 Devices)
    - The SNAP Lite component in certain SISCO MMS-EASE and AX-S4 ICCP products allows remote attackers to cause a denial of service (CPU consumption) via a crafted packet.
- CVE-2021-44695: (Improper Input Validation Vulnerability in Siemens industrial products)
    - Affected devices don’t process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial-of-service in the device.
- CVE-2022-46350: (Basic XSS Vulnerability in Siemens SCALANCE X-200RNA Switch Devices)
    - The integrated web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. This can be used by an attacker to trigger a malicious request on the affected device.
- CVE-2021-44693: (Improper Input Validation Vulnerability in Siemens industrial products)
    - Affected devices don’t process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial-of-service in the device.

- CVE-2022-46352: (Uncontrolled Resource Consumption Vulnerability in Siemens SCALANCE X-200RNA Switch Devices)
    - Specially crafted PROFINET DCP packets could cause a denial of service condition of affected products.
- CVE-2022-30065: (Use After Free Vulnerability in Siemens SCALANCE SC-600 Family)
    - A use-after-free in Busybox 1.35-x's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the copyvar function.

20221209

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

- **Talos Rules 2022-12-08 (https://www.snort.org/advisories/talos-rules-2022-12-08)**
    - Talos has added and modified multiple rules in the browser-chrome, deleted, malware-other and server-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-12-06 (https://www.snort.org/advisories/talos-rules-2022-12-06)**
    - Talos has added and modified multiple rules in the browser-chrome, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.

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

- CVE-2022-3752: (Denial-of-Service Vulnerability in Rockwell Logix Controllers)
    - An unauthorized user could use a specially crafted sequence of Ethernet/IP messages, combined with heavy traffic loading to cause a denial-of-service condition resulting in a major non-recoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online and continue normal operation.

20221202

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

- **Talos Rules 2022-12-01 (https://www.snort.org/advisories/talos-rules-2022-12-01)**
    - Talos has added and modified multiple rules in the and file-image rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-11-29 (https://www.snort.org/advisories/talos-rules-2022-11-29)**
    - Talos has added and modified multiple rules in the browser-chrome, browser-ie and server-webapp rule sets to provide coverage for emerging threats from these technologies.

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

- CVE-2022-3086: (Improper Physical Access Control in Moxa UC Series)

- An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system.