Release Notes for Cisco Cyber Vision Knowledge DB

Release 202211

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.202211	**Description**
CiscoCyberVision_knowledgedb_20221104.db	Knowledge DB version 20221104
CiscoCyberVision_knowledgedb_20221110.db	Knowledge DB version 20221110
CiscoCyberVision_knowledgedb_20221118.db	Knowledge DB version 20221118
CiscoCyberVision_knowledgedb_20221125.db	Knowledge DB version 20221125

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

20221125

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

- **Talos Rules 2022-11-23 (https://www.snort.org/advisories/talos-rules-2022-11-23)**
  - Talos has added and modified multiple rules in the file-other, malware-cnc, malware-other, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20221118

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

- **Talos Rules 2022-11-17 (https://www.snort.org/advisories/talos-rules-2022-11-17)**
  - Talos has added and modified multiple rules in the indicator-compromise and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-11-15 (https://www.snort.org/advisories/talos-rules-2022-11-15)**
  - Talos has added and modified multiple rules in the file-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20221110

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

- **Talos Rules 2022-11-10 (https://www.snort.org/advisories/talos-rules-2022-11-10)**
  - Talos has added and modified multiple rules in the file-pdf, indicator-scan, malware-cnc and protocol-snmp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-11-08 (https://www.snort.org/advisories/talos-rules-2022-11-08)**
  - Microsoft Vulnerability CVE-2022-41057: A coding deficiency exists in Microsoft Windows HTTP.sys 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 60822 through 60823, Snort 3: GID 1, SID 300312
  - Microsoft Vulnerability CVE-2022-41096: A coding deficiency exists in Microsoft DWM Core Library 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 60820 through 60821, Snort 3: GID 1, SID 300311.

- Microsoft Vulnerability CVE-2022-41109: A coding deficiency exists in Microsoft Windows Win32k 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 60815 through 60816, Snort 3: GID 1, SID 300309.
- Microsoft Vulnerability CVE-2022-41113: A coding deficiency exists in Microsoft Windows Win32k Kernel Subsystem 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 60818 through 60819, Snort 3: GID 1, SID 300310.
- Microsoft Vulnerability CVE-2022-41118: A coding deficiency exists in Microsoft Windows Scripting Languages that may lead to remote code execution.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort 2: GID 1, SIDs 60833 through 60834, Snort 3: GID 1, SID 300316.
- Microsoft Vulnerability CVE-2022-41125: A coding deficiency exists in Microsoft Windows CNG Key Isolation Service 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 60831 through 60832, Snort 3: GID 1, SID 300315.
- Talos also has added and modified multiple rules in the browser-ie, file-other, malware-cnc and os-windows rule sets to provide coverage for emerging threats from these technologies.

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

- CVE-2022-39158: (Uncontrolled Resource Consumption Vulnerability in Siemens RUGGEDCOM ROS V4)
    - RUGGEDCOM ROS-based V4 devices are vulnerable to a denial of service attack (Slowloris). By sending partial HTTP requests nonstop, with none completed, the affected web servers will be waiting for the completion of each request, occupying all available HTTP connections. The web server recovers by itself once the attack ends
- CVE-2022-31765: (Privilege Escalation Vulnerability in the Web Interface of Siemens SCALANCE and RUGGEDCOM Products)
    - Affected devices do not properly authorize the change password function of the web interface. This could allow low privileged users to escalate their privileges
- CVE-2022-37894: (Improper Input Validation Vulnerability in Siemens SCALANCE W1750D)
    - An unauthenticated denial of service (DoS) vulnerability exists in the handling of certain SSID strings. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected Access Point

- CVE-2022-37891: (Buffer Overflow Vulnerability in Siemens SCALANCE W1750D)
    - An unauthenticated buffer overflow vulnerability exists within the web management interface. Successful exploitation results in the execution of arbitrary commands on the underlying operating system
- CVE-2022-40631: (Cross-site Scripting Vulnerability in Siemens SCALANCE X-200 and X-200IRT Families)
    - There is a cross-site scripting vulnerability on the affected devices, that if used by a threat actor, it could result in session hijacking
- CVE-2022-37892: (Cross-site Scripting Vulnerability in Siemens SCALANCE W1750D)
    - A vulnerability in the web management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface
- CVE-2002-20001: (Uncontrolled Resource Consumption in Siemens SCALANCE W1750D)
    - The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE
- CVE-2022-37895: (Improper Input Validation Vulnerability in Siemens SCALANCE W1750D)
    - An authenticated denial of service (DoS) vulnerability exists in the web management interface. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected Access Point
- CVE-2022-37890: (Buffer Overflow Vulnerability in Siemens SCALANCE W1750D)
    - An unauthenticated buffer overflow vulnerability exists within the web management interface. Successful exploitation results in the execution of arbitrary commands on the underlying operating system
- CVE-2022-43546: (Improper Input Validation Vulnerability in Siemens SICAM Q100)
    - Affected devices do not properly validate the EndTime-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device
- CVE-2022-37896: (Cross-site Scripting Vulnerability in Siemens SCALANCE W1750D)
    - A vulnerability in the web management interface could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface
- CVE-2022-30694: (Missing CSRF Protection in the Web Server Login Page of Siemens Industrial Controllers)

    - The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack

- CVE-2022-43439: (Improper Input Validation Vulnerability in Siemens SICAM Q100)
    - Affected devices do not properly validate the Language-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device
- CVE-2022-43398: (Session Fixation Vulnerability in Siemens SICAM Q100)
    - Affected devices do not renew the session cookie after login/logout and also accept user defined session cookies. An attacker could overwrite the stored session cookie of a user. After the victim logged in, the attacker is given access to the user's account through the activated session
- CVE-2022-43545: (Improper Input Validation Vulnerability in Siemens SICAM Q100)
    - Affected devices do not properly validate the RecordType-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device
- CVE-2022-37885: (Buffer Overflow Vulnerability in Siemens SCALANCE W1750D)
    - A buffer overflow vulnerability in an underlying service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI UDP port (8211)

20221104

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

- **Talos Rules 2022-11-03 (https://www.snort.org/advisories/talos-rules-2022-11-03)**
    - Talos has added and modified multiple rules in the file-image, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-11-01 (https://www.snort.org/advisories/talos-rules-2022-11-01)**
    - Talos is releasing the following SIDs to protect against a critical vulnerability in OpenSSL (CVE-2022-3602): 60790, 300306-300307. Talos has added and modified multiple rules in the file-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.