Release Notes for Cisco Cyber Vision Knowledge DB

Release 202207

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.202207	**Description**
CiscoCyberVision_knowledgedb_20220701.db	Knowledge DB version 20220701
CiscoCyberVision_knowledgedb_20220708.db	Knowledge DB version 20220708
CiscoCyberVision_knowledgedb_20220715.db	Knowledge DB version 20220715
CiscoCyberVision_knowledgedb_20220722.db	Knowledge DB version 20220722
CiscoCyberVision_knowledgedb_20220729.db	Knowledge DB version 20220729

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

20220729

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

- **Talos Rules 2022-07-28 (https://www.snort.org/advisories/talos-rules-2022-07-28)**
  - Talos has added and modified multiple rules in the malware-cnc, os-other, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-07-26 (https://www.snort.org/advisories/talos-rules-2022-07-26)**
  - Talos has added and modified multiple rules in the browser-chrome, file-other, malware-cnc, malware-other, os-mobile 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 vulnerability:

- CVE-2022-2043: (Buffer Overflow Vulnerability in Moxa NPort 5110)
  - The affected product is vulnerable to an out-of-bounds write that can cause the device to become unresponsive.
- CVE-2022-2044: (Buffer Overflow Vulnerability in Moxa NPort 5110)
  - The affected product is vulnerable to an out-of-bounds write that may allow an attacker to overwrite values in memory, causing a denial-of-service condition or potentially bricking the device

20220722

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

- **Talos Rules 2022-07-21 (https://www.snort.org/advisories/talos-rules-2022-07-21)**
  - Talos has added and modified multiple rules in the malware-cnc, malware-other, os-other, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-07-19 (https://www.snort.org/advisories/talos-rules-2022-07-19)**
  - Talos has added and modified multiple rules in the browser-chrome, file-office, file-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20220715

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

- **Talos Rules 2022-07-14 (https://www.snort.org/advisories/talos-rules-2022-07-14)**
  - Talos has added and modified multiple rules in the malware-other, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-07-12 (https://www.snort.org/advisories/talos-rules-2022-07-12)**
  - Microsoft Vulnerability CVE-2022-22034: A coding deficiency exists in Microsoft Graphics Component that may lead to an escalation of privilege.

        - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 60206 through 60207, Snort3: GID 1, SID 300215.
    - Microsoft Vulnerability CVE-2022-22047: A coding deficiency exists in Microsoft Windows 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: Snort2: GID 1, SIDs 60213 through 60214, Snort3: GID 1, SID 300216.
    - Microsoft Vulnerability CVE-2022-30202: A coding deficiency exists in Microsoft Windows Advanced Local Procedure Call that may lead to an escalation of privilege.
        - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 60198 through 60199, Snort3: GID 1, SIDs 60198 through 60199.
    - Microsoft Vulnerability CVE-2022-30216: A coding deficiency exists in Microsoft Windows Server Service that may lead to tampering.
        - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 60201 through 60202, Snort3: GID 1, SIDs 60201 through 60202.
    - Microsoft Vulnerability CVE-2022-30220: A coding deficiency exists in Microsoft Windows Common Log File System 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: Snort2: GID 1, SIDs 60191 through 60192, Snort3: GID 1, SIDs 60191 through 60192.
    - Talos also has added and modified multiple rules in the browser-chrome, file-image, file-other, malware-cnc, os-windows, policy-other 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 vulnerability:

- CVE-2022-25622: (Denial of Service Vulnerability in PROFINET Stack Integrated on Interniche Stack)
    - The PROFINET (PNIO) stack, when integrated with the Interniche IP stack, contains a vulnerability that could allow an attacker to cause a denial of service condition on affected industrial products.
- CVE-2022-34753: (OS Command Injection Vulnerability in Schneider SpaceLogic C-Bus Home Controller)
    - An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that could cause remote root exploit when the command is compromised.
- CVE-2022-34820: (Command Injection Vulnerability in the SRCS VPN Feature in Siemens SIMATIC CP Devices)
    - The application does not correctly escape some user provided fields during the authentication process. This could allow an attacker to inject custom commands and execute arbitrary code with elevated privileges.
- CVE-2022-33137: (Insufficient Session Expiration Vulnerability in Siemens SIMATIC MV500 Devices)
    - SIMATIC MV500 devices before V3.3 are affected by a vulnerability that could allow attackers to hijack other users' web based management sessions
- CVE-2022-30938: (Memory Corruption Vulnerability in Siemens EN100 Ethernet Module)
    - Siemens EN100 Ethernet module is affected by a memory corruption vulnerability. Affected applications contains a memory corruption vulnerability while parsing specially crafted HTTP packets to /txtrace

endpoint manipulating a specific argument. This could allow an attacker to crash the affected application leading to a denial of service condition.

- CVE-2022-29560: (Command Injection Vulnerability in Siemens RUGGEDCOM ROX)
  - RUGGEDCOM ROX devices are affected by a command injection vulnerability that could allow an attacker with administrative privileges to gain root access.
- CVE-2022-34757: (Use of a Broken or Risky Cryptographic Algorithm Vulnerability in Schneider Easergy P5)
  - A Use of a Broken or Risky Cryptographic Algorithm vulnerability exists where weak cipher suites can be used for the SSH connection between Easergy Pro software and the device, which may allow an attacker to observe protected communication details.
- CVE-2022-34758: (Improper Input Validation Vulnerability in Schneider Easergy P5)
  - An Improper Input Validation vulnerability exists that could cause the device watchdog function to be disabled if the attacker had access to privileged user credentials.
- CVE-2022-26647: (Use of Insufficiently Random Values in Siemens SCALANCE X Switch Devices)
  - Several SCALANCE X switches contain multiple vulnerabilities. An unauthenticated attacker could reboot, cause denial-of-service conditions and potentially impact the system by other means through heap and buffer overflow vulnerabilities.
- CVE-2022-34819: (Heap-based Buffer Overflow Vulnerability in the SRCS VPN Feature in Siemens SIMATIC CP Devices)
  - The application lacks proper validation of user-supplied data when parsing specific messages. This could result in a heap-based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of device.
- CVE-2022-34754: (Improper Privilege Management Vulnerability in Schneider Acti9 PowerTag Link C)
  - An Improper Privilege Management vulnerability exists that could allow elevated functionality when guessing credentials.
- CVE-2022-26648: (Classic Buffer Overflow Vulnerability in Siemens SCALANCE X Switch Devices)
  - Several SCALANCE X switches contain multiple vulnerabilities. An unauthenticated attacker could reboot, cause denial-of-service conditions and potentially impact the system by other means through heap and buffer overflow vulnerabilities.
- CVE-2022-34764: (Buffer Overflow Vulnerability in Schneider OPC UA and X80 Advanced RTU Modicon Communication Modules)
  - An Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause denial of service when parsing the URL.
- CVE-2022-26649: (Classic Buffer Overflow Vulnerability in Siemens SCALANCE X Switch Devices)
  - Several SCALANCE X switches contain multiple vulnerabilities. An unauthenticated attacker could reboot, cause denial-of-service conditions and potentially impact the system by other means through heap and buffer overflow vulnerabilities.
- CVE-2022-34759: (Out-of-bounds Write Vulnerability in Schneider OPC UA and X80 Advanced RTU Modicon Communication Modules)
  - An Out-of-bounds Write vulnerability exists that could cause a denial of service of the webserver due to

improper parsing of the HTTP Headers.

- CVE-2022-34765: (External Control of File Name or Path Vulnerability in Schneider OPC UA and X80 Advanced RTU Modicon Communication Modules)
  - An External Control of File Name or Path vulnerability exists that could cause loading of unauthorized firmware images when user-controlled data is written to the file path.
- CVE-2022-33138: (Missing Authentication for Critical Function Vulnerability in Siemens SIMATIC MV500 Devices)
  - SIMATIC MV500 devices before V3.3 are affected by a vulnerability that could allow attackers to access data on the device without prior authentication
- CVE-2022-34762: (Path Traversal Vulnerability in Schneider OPC UA and X80 Advanced RTU Modicon Communication Modules)
  - An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause unauthorized firmware image loading when unsigned images are added to the firmware image path
- CVE-2022-34663: (Code Injection Vulnerability in Siemens RUGGEDCOM ROS)
  - RUGGEDCOM ROS-based devices are vulnerable to a web-based code injection attack. To execute this attack, it is necessary to access the system via the console.
- CVE-2022-34821: (Code Injection Vulnerability in the SRCS VPN Feature in Siemens SIMATIC CP Devices)
  - By injecting code to specific configuration options for OpenVPN, an attacker could execute arbitrary code with elevated privileges.
- CVE-2022-34763: (Insufficient Verification of Data Authenticity Vulnerability in Schneider OPC UA and X80 Advanced RTU Modicon Communication Modules)
  - An Insufficient Verification of Data Authenticity vulnerability exists that could cause loading of unauthorized firmware images due to improper verification of the firmware signature.
- CVE-2022-34761: (NULL Pointer Dereference Vulnerability in Schneider OPC UA and X80 Advanced RTU Modicon Communication Modules)
  - A NULL Pointer Dereference vulnerability exists that could cause a denial of service of the webserver when parsing JSON content type.
- CVE-2022-34760: (Infinite Loop Vulnerability in Schneider OPC UA and X80 Advanced RTU Modicon Communication Modules)
  - A Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability exists that could cause a denial of service of the webserver due to improper handling of the cookies
- CVE-2022-29884: (Denial of Service Vulnerability in CPC80 Firmware of SICAM A8000 Devices)
  - A vulnerability was identified in the CPC80 firmware of SICAM A8000 devices. It could allow an unauthenticated remote attacker to cause a permanent denial of service condition.
- CVE-2022-34756: (Buffer Overflow Vulnerability in Schneider Easergy P5)
  - A Buffer Copy without Checking Size of Input vulnerability exists that could result in remote code execution or the crash of HTTPs stack which is used for the device Web HMI.

20220708

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

- **Talos Rules 2022-07-07 (https://www.snort.org/advisories/talos-rules-2022-07-07)**
  - Talos has added and modified multiple rules in the malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-07-05 (https://www.snort.org/advisories/talos-rules-2022-07-05)**
  - Talos has added and modified multiple rules in the browser-webkit 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 vulnerability:

- CVE-2022-2179: (Clickjacking Vulnerability in Rockwell Automation MicroLogix)
  - The X-Frame-Options header is not configured in the HTTP response, which could allow clickjacking attacks.

20220701

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

- **Talos Rules 2022-06-30 (https://www.snort.org/advisories/talos-rules-2022-06-30)**
  - Talos has added and modified multiple rules in the and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-06-28 (https://www.snort.org/advisories/talos-rules-2022-06-28)**
  - Talos has added and modified multiple rules in the 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-2022-31205: (Compromise of credentials vulnerability in Omron SYSMAC CP series)
  - The password to access the Web UI can be read from memory using the Omron FINS protocol without any further authentication.
- CVE-2022-31207: (Logic manipulation vulnerability in Omron SYSMAC CS/CJ/CP series)
  - The logic that is downloaded to the PLC is not cryptographically authenticated, allowing an attacker to manipulate transmitted object code to the PLC and execute arbitrary object code commands on the defined software logic.
- CVE-2022-31206: (Remote Code Execution Vulnerability in Omron SYSMAC NJ/NX)
  - The logic that is downloaded to the PLC is not cryptographically authenticated, allowing an attacker to manipulate transmitted object code to the PLC and execute arbitrary machine code on the processor of the PLC's CPU module.
- CVE-2022-31204: (Compromise of credentials vulnerability in Omron SYSMAC CS1/CJ1/CP1/CP2 series)
  - The password used to restrict engineering operations is transmitted in plaintext.
- CVE-2022-29957: (Missing Authentication for Critical Function Vulnerability in Emerson DeltaV Distributed

Control System)

- Several protocols, including Firmware upgrade, Plug-and-Play, Hawk services, Management, SIS communications, and multi-cast have no authentication. This could allow an attacker who has reverse-engineered communications to invoke desired functionality or cause a denial-of-service condition.

- CVE-2022-29965: (Use of Broken or Risky Cryptographic Algorithm Vulnerability in Emerson DeltaV Distributed Control System)
  - Access to privileged operations in the maintenance interface is controlled by a challenge-response authentication that uses a deterministic insecure algorithm.
- CVE-2022-29964: (Use of Hard-coded Credentials Vulnerability in Emerson DeltaV Distributed Control System)
  - The affected product is vulnerable to hard-coded credential use within the SSH service, which is disabled by default.
- CVE-2022-29963: (Use of Hard-coded Credentials Vulnerability in Emerson DeltaV Distributed Control System)
  - The affected product is vulnerable to hard-coded credential use within the read-only Telnet service.
- CVE-2022-29962: (Use of Hard-coded Credentials Vulnerability in Emerson DeltaV Distributed Control System)
  - The affected product is vulnerable by using hard-coded credentials in the FTP service, which is disabled by default.
- CVE-2022-30260: (Insufficient Verification of Data Authenticity Vulnerability in Emerson DeltaV Distributed Control System)
  - Firmware images are not signed and rely on insecure checksums for regular integrity checks. This could allow an attacker to push malicious firmware images, execute code, or cause a denial-of-service condition.