Release Notes for Cisco Cyber Vision Knowledge DB

Release 202308

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-4.2.2.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.2.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.2.2.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.2.2.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.2.2.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.2.2.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.2.2.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.2.2.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.2.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.2.2.dat	Knowledge DB embedded in Cisco Cyber Vision 4.2.1
Updates/KDB/KDB.202308	**Description**
CiscoCyberVision_knowledgedb_20230804.db	Knowledge DB version 20230804
CiscoCyberVision_knowledgedb_20230811.db	Knowledge DB version 20230811

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

20230811

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

- **Talos Rules 2023-08-08 (https://www.snort.org/advisories/talos-rules-2023-08-08)**

The new and updated Snort rules span the following categories:

- 2 file-identify rules with SIDs 300656, 61894
- 3 file-other rules with SIDs 40690, 300647, 40689
- 1 indicator-compromise rules with SIDs 61893
- 5 malware-other rules with SIDs 300654, 300646, 300655, 300657, 300653
- 4 os-windows rules with SIDs 300648, 300652, 300650, 300649
- 14 server-webapp rules with SIDs 61356, 62217, 62206, 62102, 62199, 62201, 62219, 62207, 62205, 300651, 62218, 62212, 62204, 62200

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

- CVE-2023-0286: (Type Confusion Vulnerability in OpenSSL X.400 Address Processing in Siemens SIMATIC Products)
  - There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.
- CVE-2022-4304: (Timing Based Side Channel Vulnerability in the OpenSSL RSA Decryption in Siemens SIMATIC Products)
  - A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an

encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre master secret used for the original connection and thus be able to decrypt the application data sent over that connection.

- CVE-2023-24845: (Mirror Port Isolation Vulnerability in Siemens RUGGEDCOM ROS Devices)
  - The affected products insufficiently block data from being forwarded over the mirror port into the mirrored network. An attacker could use this behavior to transmit malicious packets to systems in the mirrored network, possibly influencing their configuration and runtime behavior.
- CVE-2023-39269: (Denial of Service Vulnerability in the Web Server of Siemens RUGGEDCOM ROS Devices)
  - The web server of the affected devices contains a vulnerability that may lead to a denial of service condition. An attacker may cause total loss of availability of the web server, which might recover after the attack is over.
- CVE-2023-3526: (Cross-site Scripting Vulnerability in Phoenix Contact TC ROUTER, TC CLOUD CLIENT and CLOUD CLIENT devices)
  - In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an unauthenticated remote attacker could use a reflective XSS within the license viewer page of the devices in order to execute code in the context of the user's browser.
- CVE-2023-3569: (Denial of Service Vulnerability in Phoenix Contact TC ROUTER, TC CLOUD CLIENT and CLOUD CLIENT devices)
  - In PHOENIX CONTACTs TC ROUTER and TC CLOUD CLIENT in versions prior to 2.07.2 as well as CLOUD CLIENT 1101T-TX/TX prior to 2.06.10 an authenticated remote attacker with admin privileges could upload a crafted XML file which causes a denial-of-service.
- CVE-2023-37855: (Access Control Vulnerability in Phoenix Contact WP 6xxx Web panels)
  - In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem within the embedded Qt browser.
- CVE-2023-37863: (OS Command Injection Vulnerability in Phoenix Contact WP 6xxx Web panels)
  - In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with SNMPv2 write privileges may use an a special SNMP request to gain full access to the device.
- CVE-2023-37861: (OS Command Injection in Phoenix Contact WP 6xxx Web panels)
  - In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated remote attacker can execute code with root permissions with a specially crafted HTTP POST when uploading a certificate to the device.
- CVE-2023-37862: (Missing Authorization Vulnerability in Phoenix Contact WP 6xxx Web panels)

    - In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an unauthenticated remote attacker can access upload-functions of the HTTP API. This might cause certificate errors for SSL-connections and might result in a partial denial-of-service.
- CVE-2023-37856: (Access Control Vulnerability in Phoenix Contact WP 6xxx Web panels)
    - In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges is able to gain limited read-access to the device-filesystem through a configuration dialog within the embedded Qt browser .
- CVE-2023-37860: (Missing Authorization Vulnerability in Phoenix Contact WP 6xxx Web panels)
    - In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote unauthenticated attacker can obtain the r/w community string of the SNMPv2 daemon.
- CVE-2023-37857: (Use of Hard-coded Credentials in Phoenix Contact WP 6xxx Web panels)
    - In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing the attacker to create valid session cookies. This issue cannot be exploited to bypass the web service authentication of the affected device(s).
- CVE-2023-37859: (Improper Privilege Management Vulnerability in Phoenix Contact WP 6xxx Web panels)
    - In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 the SNMP daemon is running with root privileges allowing a remote attacker with knowledge of the SNMPv2 r/w community string to execute system commands as root.
- CVE-2023-3572: (OS Command Injection in Phoenix Contact WP 6xxx Web panels)
    - In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use an attribute of a specific HTTP POST request releated to date/time operations to gain full access to the device.
- CVE-2023-3573: (OS Command Injection in Phoenix Contact WP 6xxx Web panels)
    - In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a command injection in a HTTP POST request related to font configuration operations to gain full access to the device
- CVE-2023-37858: (Use of Hard-coded Credentials in Phoenix Contact WP 6xxx Web panels)
    - In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 an authenticated, remote attacker with admin privileges is able to read hardcoded cryptographic keys allowing to decrypt an encrypted web application login password.
- CVE-2023-3571: (OS Command Injection in Phoenix Contact WP 6xxx Web panels)
    - In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attacker with low privileges may use a specific HTTP POST releated to certificate operations to gain full access to the device.
- CVE-2023-37864: (Download of Code Without Integrity Check in Phoenix Contact WP 6xxx Web panels)

- In PHOENIX CONTACTs WP 6xxx series web panels in versions prior to 4.0.10 a remote attackerwith SNMPv2 write privileges may use an a special SNMP request to gain full access to the device.

20230804

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

- **Talos Rules 2023-08-03 (https://www.snort.org/advisories/talos-rules-2023-08-03)**
- **Talos Rules 2023-08-01 (https://www.snort.org/advisories/talos-rules-2023-08-01)**

The new and updated Snort rules span the following categories:

- 5 malware-cnc rules with SIDs 300633, 300634, 300635, 300636, 300637
- 8 malware-other rules with SIDs 300626, 300638, 300639, 300640, 300641, 300642, 300643, 300644, 300645
- 1 policy-other rule with SID 62172
- 4 server-webapp rules with SIDs 62158, 62159, 62160, 62171