Release Notes for Cisco Cyber Vision Knowledge DB

Release 202203

Compatible device list 2
Links 2
  Software Download 2
  Related Documentation 2
Database download 3
How to update the database 3
Release contents 4
  20220325 4
  20220318 4
  20220311 5
  20220304 8

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.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates/4/4	**Description**
CiscoCyberVision-Embedded-KDB-4.dat	Knowledge DB embedded in Cisco Cyber Vision 4
Updates/KDB/KDB.202203	**Description**
CiscoCyberVision_knowledgedb_20220304.db	Knowledge DB version 20220304
CiscoCyberVision_knowledgedb_20220311.db	Knowledge DB version 20220311
CiscoCyberVision_knowledgedb_20220318.db	Knowledge DB version 20220318
CiscoCyberVision_knowledgedb_20220325.db	Knowledge DB version 20220325

Related Documentation

- Cisco Cyber Vision GUI User Guide:

  https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_GUI_User_Guide_4_0_0.pdf

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

20220325

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

- **Talos Rules 2022-03-24 (https://www.snort.org/advisories/talos-rules-2022-03-24)**
  - Talos has added and modified multiple rules in the file-image and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-03-22 (https://www.snort.org/advisories/talos-rules-2022-03-22)**
  - Talos has added and modified multiple rules in the policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20220318

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

- **Talos Rules 2022-03-17 (https://www.snort.org/advisories/talos-rules-2022-03-17)**
  - Talos has added and modified multiple rules in the malware-other, policy-other, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-03-15 (https://www.snort.org/advisories/talos-rules-2022-03-15)**
  - Talos has added and modified multiple rules in the malware-cnc, malware-other, malware-tools, os-linux and server-other 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-2022-22148: (OS Command Injection Vulnerability in Yokogawa CENTUM and Exaopc)

  If an attacker is somehow able to intrude into a computer that installed the product, the named pipe created by Root Service function may have inappropriate access privileges, which may allow arbitrary programs to be executed with the system privileges running the process.

- CVE-2022-22729: (Authentication Bypass by Assumed-Immutable Data Vulnerability in Yokogawa CENTUM and Exaopc)

  If CAMS for HIS server receives a malformed packet, the following incidents may occur with user permissions running the service: (i) Any file on CAMS for HIS server will be read, (ii) Arbitrary files are created/overwritten in any location on CAMS for HIS server, (iii) Arbitrary commands will be executed on CAMS for HIS server.

- CVE-2022-23402: (Use of Hard-coded Credentials in Yokogawa CENTUM and Exaopc)

  If the hard-coded credentials for CAMS server application are used to send a malformed packet to CAMS server, all functions of CAMS server can be abused, including suppressing alarms.

- CVE-2022-21808: (Relative Path Traversal Vulnerability in Yokogawa CENTUM and Exaopc)

  If CAMS for HIS server receives a malformed packet, the following incidents may occur with user permissions running the service: (i) Any file on CAMS for HIS server will be read, (ii) Arbitrary files are created/overwritten in any location on CAMS for HIS server, (iii) Arbitrary commands will be executed on CAMS for HIS server.

- CVE-2022-23401: (DLL Planting Vulnerability in Yokogawa CENTUM and Exaopc)

  CENTUM and Exaopc have a DLL injection vulnerability using the vulnerability 1 and a DLL planting vulnerability using the DLL search order vulnerability.

- CVE-2022-22145: (Uncontrolled Resource Consumption Vulnerability in Yokogawa CENTUM and Exaopc)

  If CAMS for HIS log server receives a malformed packet, the following incidents may occur with user privileges running the service: (i) CAMS for HIS log server crashes, (ii) Arbitrary log files are created/overwritten in any location in CAMS for HIS log server, (iii) Creating invalid logs on CAMS for HIS log server makes it difficult to analyze the logs when problems occur.

- CVE-2022-21177: (Relative Path Traversal Vulnerability in Yokogawa CENTUM and Exaopc)

  If CAMS for HIS log server receives a malformed packet, the following incidents may occur with user privileges running the service: (i) CAMS for HIS log server crashes, (ii) Arbitrary log files are created/overwritten in any location in CAMS for HIS log server, (iii) Creating invalid logs on CAMS for HIS log server makes it difficult to analyze the logs when problems occur.

- CVE-2022-22151: (Improper Output Neutralization for Logs Vulnerability in Yokogawa CENTUM and Exaopc)

  If CAMS for HIS log server receives a malformed packet, the following incidents may occur with user privileges running the service: (i) CAMS for HIS log server crashes, (ii) Arbitrary log files are created/overwritten in any location in CAMS for HIS log server, (iii) Creating invalid logs on CAMS for HIS log server makes it difficult to analyze the logs when problems occur.

- CVE-2022-22141: (Inappropriate Access Privilege Vulnerability in Yokogawa CENTUM and Exaopc)

  If an attacker is somehow able to intrude into a computer that installed the product, the named pipe created by Long-term Data Archive Package may have inappropriate access privileges, arbitrary files may be deleted with the system privileges running the process.

- CVE-2020-24588: (Missing Authentication for Critical Function Vulnerability in Wifi devices)

  The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that the A-MSDU flag in the plaintext QoS header field is authenticated. Against devices that support receiving non-SSP A-MSDU frames (which is mandatory as part of 802.11n), an adversary can abuse this to inject arbitrary network packets.

- CVE-2019-18232: (Improper Link Resolution Before File Access Vulnerability in License Function in Yokogawa Products)

  A vulnerability has been found in a module that is used in license function of Yokogawa products. SafeNet Sentinel LDK License Manager, all versions prior to 7.101, is vulnerable when configured as a service. This vulnerability may allow an attacker with local access to create, write, and/or delete files in system folder using symbolic links, leading to a privilege escalation. This vulnerability could also be used by an attacker to execute a malicious DLL, which could impact the integrity and availability of the system.

- CVE-2022-21194: (Use of Hard-coded Credentials in Yokogawa CENTUM and Exaopc)

  If the password for the OS account created when installing the product has not been changed from the default password, and the hard-coded credentials (default password) for the account are used to unauthorized login to the computer that installed the product, there is a possibility that files and shared

20220311

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

- **Talos Rules 2022-03-10 (https://www.snort.org/advisories/talos-rules-2022-03-10)**
  - Talos has added and modified multiple rules in the file-pdf, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-03-08 (https://www.snort.org/advisories/talos-rules-2022-03-08)**
  - Microsoft Vulnerability CVE-2022-21990: A coding deficiency exists in Remote Desktop Client that may lead to remote code execution.
    - Previously released rules will detect attacks targeting these vulnerabilities and have been updated with the appropriate reference information. They are also included in this release and are identified with GID 1, SIDs 59107 through 59108.
  - Microsoft Vulnerability CVE-2022-23253: A coding deficiency exists in Point-to-Point Tunneling Protocol that may lead to denial of service.
    - A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 1, SID 59212.
  - Microsoft Vulnerability CVE-2022-23285: A coding deficiency exists in Remote Desktop Client that may lead to remote code execution.
    - A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 1, SID 59215.
  - Microsoft Vulnerability CVE-2022-23286: A coding deficiency exists in Microsoft Windows Cloud Files Mini Filter 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 GID 1, SIDs 59213 through 59214.
  - Microsoft Vulnerability CVE-2022-23299: A coding deficiency exists in Microsoft Windows PDEV that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 59210 through 59211.
  - Microsoft Vulnerability CVE-2022-24502: A coding deficiency exists in Microsoft Windows HTML Platforms that may lead to security feature bypass.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 59216 through 59217.
  - Microsoft Vulnerability CVE-2022-24507: A coding deficiency exists in Microsoft Windows Ancillary Function 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 GID 1, SIDs 59220 through 59221.
  - Talos also has added and modified multiple rules in the browser-ie, malware-cnc, malware-other, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-03-04 (https://www.snort.org/advisories/talos-rules-2022-03-04)**
  - Talos is releasing Snort coverage to protect against ongoing cyber operations against Ukraine. These new Snort rules provide protection against the following malware families: Redline (SID 59160), IsaacWiper (SIDs 59163-59164), SunSeed Lua (SIDs 59165-59173), HermeticRansom (SIDs 59154-59159), Vidar (SIDs 59200-59203), and WhiteBlackCrypt (SIDs 59161-59162).
  - Talos has added and modified multiple rules in the deleted, malware-cnc, malware-other 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 vulnerabilities:

- CVE-2022-22806: (Authentication Bypass by Capture-replay Vulnerability in APC Smart-UPS SMT, SMC, SMX, SCL, SMTL and SRT Series)

  Improper Authentication vulnerability exists that could cause an attacker to arbitrarily change the behavior of the UPS if a key is leaked and used to upload malicious firmware.

- CVE-2021-37208: (Cross-site Scripting Vulnerability in third-party component of the Siemens RUGGEDCOM ROS)

  Improper neutralization of special characters on the web server configuration page could allow an attacker, in a privileged position, to retrieve sensitive information via cross-site scripting.

- CVE-2021-42019: (Integer Overflow Vulnerability in third-party component of the Siemens RUGGEDCOM ROS)

  Within a third-party component, the process to allocate partition size fails to check memory boundaries. Therefore, if a large amount is requested by an attacker, due to an integer-wrap around, it could result in a small size being allocated instead.

- CVE-2021-42017: (Improperly Implemented Security Check for Standard Vulnerability in third-party component of the Siemens RUGGEDCOM ROS)

  A new variant of the POODLE attack has left a third-party component vulnerable due to the implementation flaws of the CBC encryption mode in TLS 1.0 to 1.2. If an attacker were to exploit this, they could act as a man-in-the-middle and eavesdrop on encrypted communications.

- CVE-2021-4034: (Local Privilege Escalation Vulnerability in several Moxa devices)

  The Qualys Research Team has discovered a memory corruption vulnerability in polkit's pkexec, a SUID-root program that is installed by default on every major Linux distribution. This easily exploited vulnerability allows users without the proper access levels to gain full root privileges on a vulnerable host by exploiting this vulnerability in its default configuration.

- CVE-2022-22805: (Classic Buffer Overflow Vulnerability in APC Smart-UPS SMT, SMC, SMX, SCL, SMTL and SRT Series)

  Improper Authentication vulnerability exists that could cause an attacker to arbitrarily change the behavior of the UPS if a key is leaked and used to upload malicious firmware.

- CVE-2022-24408: (Improper Privilege Management Vulnerability in Siemens SINUMERIK MC)

  The sc SUID binary on affected devices provides several commands used to execute system commands or modify system files. A specific set of operations using sc could allow local attackers to escalate their privileges to root.

- CVE-2021-42018: (Heap-based Buffer Overflow Vulnerability in third-party component of the Siemens RUGGEDCOM ROS)

  Within a third-party component, whenever memory allocation is requested, the out of bound size is not checked. Therefore, if size exceeding the expected allocation is assigned, it could allocate a smaller buffer instead. If an attacker were to exploit this, they could cause a heap overflow.

- CVE-2022-0715: (Improper Authentication Vulnerability in APC Smart-UPS SMT, SMC, SMX, SCL, SMTL and SRT Series)

Improper Authentication vulnerability exists that could cause an attacker to arbitrarily change the behavior of the UPS if a key is leaked and used to upload malicious firmware.

- CVE-2021-42020: (Improper Check for Unusual or Exceptional Conditions Vulnerability in third-party component of the Siemens RUGGEDCOM ROS)

  The third-party component in its TFTP functionality fails to check for null terminations in file names. If an attacker were to exploit this, it could result in data corruption, and possibly a hard-fault of the application.

- CVE-2021-42016: (Observable Timing Discrepancy Vulnerability in third-party component of the Siemens RUGGEDCOM ROS)

  A timing attack in a third-party component could make the retrieval of the private key possible, used for encryption of sensitive data. If a threat actor were to exploit this, the data integrity and security could be compromised.

20220304

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

- **Talos Rules 2022-03-03 (https://www.snort.org/advisories/talos-rules-2022-03-03)**
  - Talos has added and modified multiple rules in the indicator-shellcode, malware-cnc, malware-other, malware-tools, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-03-01 (https://www.snort.org/advisories/talos-rules-2022-03-01)**
  - Talos has added and modified multiple rules in the file-pdf, malware-cnc, protocol-dns, protocol-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.