Release Notes for Cisco Cyber Vision Knowledge DB

Release 202106

Compatible device list 2
Links 2
Software Download 2
Related Documentation 2
Database download 3
How to update the database 3
Release contents 4
20210625 4
20210618 5
20210611 5
20210604 10

Compatible device list

Center	Description
All version 3 centers	All Cisco Cyber Vision center version 3 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-3.2.4.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-3.2.4.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-3.2.4.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-3.2.4.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-3.2.4.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-3.2.4.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.2.4.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-3.2.4.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-3.2.4.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates/3/3.2.4	**Description**
CiscoCyberVision-sysupgrade-3.2.4.dat	System Upgrade file for Center and Sensors 3.1.x to 3.2.4
CiscoCyberVision-sysupgrade-sensor-3.2.4.dat	Cisco Cyber Vision System Upgrade file for IC3000 Sensors or other non IOx Sensors 3.x to 3.2.4
CiscoCyberVision-Embedded-KDB-3.2.4.dat	Knowledge DB embedded in Cisco Cyber Vision 3.2.4
Updates/KDB/KDB.202106	**Description**
CiscoCyberVision_knowledgedb_20210604.db	Knowledge DB version 20210604
CiscoCyberVision_knowledgedb_20210611.db	Knowledge DB version 20210611
CiscoCyberVision_knowledgedb_20210618.db	Knowledge DB version 20210618
CiscoCyberVision_knowledgedb_20210625.db	Knowledge DB version 20210625

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_3_2_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

20210625

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

- **Talos Rules 2021-06-24 (https://www.snort.org/advisories/talos-rules-2021-06-24)**
  - 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 2021-06-22 (https://www.snort.org/advisories/talos-rules-2021-06-22)**
  - Talos has added and modified multiple rules in the browser-chrome, file-pdf, malware-cnc, malware-other, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-06-17 (https://www.snort.org/advisories/talos-rules-2021-06-17)**
  - Talos has added and modified multiple rules in the indicator-obfuscation, malware-other, server-apache 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-2020-25860: (Time-of-Check-Time-of-Use Vulnerability in Phoenix Contact PLCNext, SMARTRTU AXC, CHARX control modular and EEM-SB37x)
  - The vulnerability is a Time-of-Check-Time-of-Use (CWE-367) issue which allows an attacker with access to the firmware update file to overwrite it after it has been verified (but before installation is completed), which consequently allows installing an arbitrary firmware update, bypassing the cryptographic signature check mechanism.
- CVE-2021-33540: (Use of Hard-coded Credentials in Phoenix Contact AXL F BK and IL BK products)
  - An undocumented password protected FTP access to the root directory exists in certain devices of the AXL F BK and IL BK product families (CWE-798). An attacker who was able to obtain the hard-coded password to FTP access could access the FTP area and read the scrambled monitoring information of the device.
- CVE-2021- 20004: (Cross-site Scripting in Phoenix Contact FL SWITCH SMCS series)
  - An attacker may insert malicious code via LLDP frames into the web-based management which could then be executed by the client. An attacker may use the vulnerability to provoke a denial of service to defeat certain management functions of the device or use the XSS vulnerability to attack the client PC.
- CVE-2021- 20005: (Race Condition in Phoenix Contact FL SWITCH SMCS series)
  - If an attacker sends a hand-crafted TCP-Packet with the Urgent-Flag set and the Urgent-Pointer set to 0, the network stack will crash. The device needs to be rebooted afterwards. An attacker may use the vulnerability to provoke a denial of service to defeat certain management functions of the device or use the XSS vulnerability to attack the client PC.
- CVE-2021-33541: (Allocation of Resources Without Limits or Throttling in Phoenix Contact ILC1x1 Industrial controllers)

- Phoenix Contact Classic Line industrial controllers are developed and designed for the use in closed industrial networks. The communication protocols and device access do not feature authentication measures. Remote attackers can use specially crafted IP packets to cause a denial of service on the PLC's network communication module (CWE-770). A successful attack stops all network communication. To restore the network connectivity the device needs to be restarted. The automation task is not affected.

- CVE-2021-3449: (Improper Certificate Validation Vulnerability in multiple Phoenix Contact products)
  - An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation Client Hello message from a client (CWE-476)
- CVE-2021-21002: (Denial of Service Vulnerability in Phoenix Contact FL COMSERVER UNI products)
  - When the communication partner sends an invalid Modbus exception response to the FL COMSERVER UNI as a query, the Modbus communication stops, and the device will be unresponsive for some minutes before the functionality is fully restored (CWE-772).
- CVE-2021-20003: (Improper Resource Shutdown or Release in Phoenix Contact FL SWITCH SMCS series)
  - Fragmented TCP-Packets may cause a Denial of Service of Web-, SNMP-, and ICMP Echo- service. The switching functionality of the device is not affected. An attacker may use the vulnerability to provoke a denial of service to defeat certain management functions of the device or use the XSS vulnerability to attack the client PC.

20210618

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

- **Talos Rules 2021-06-15 (https://www.snort.org/advisories/talos-rules-2021-06-15)**
  - Talos has added and modified multiple rules in the browser-ie, deleted, file-flash, file-image, file-multimedia, file-other, indicator-compromise, malware-cnc, os-linux, os-other, os-windows, protocol-dns, protocol-icmp, protocol-other, server-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20210611

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

- **Talos Rules 2021-06-10 (https://www.snort.org/advisories/talos-rules-2021-06-10)**
  - 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 2021-06-08 (https://www.snort.org/advisories/talos-rules-2021-06-08)**
  - Microsoft Vulnerability CVE-2021-31199: A coding deficiency exists in Microsoft Enhanced Cryptographic Provider that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included I n this release and are identified with GID 1, SIDs 57724 through 57725.
  - Microsoft Vulnerability CVE-2021-31201: A coding deficiency exists in Microsoft Enhanced Cryptographic Provider 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 57730 through 57731.

- Microsoft Vulnerability CVE-2021-31952: A coding deficiency exists in Microsoft Windows Kernel-Mode 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 57722 through 57723.
- Microsoft Vulnerability CVE-2021-31954: 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 GID 1, SIDs 57734 through 57735.
- Microsoft Vulnerability CVE-2021-31955: A coding deficiency exists in Microsoft Windows Kernel that may lead to information disclosure.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 57726 through 57727.
- Microsoft Vulnerability CVE-2021-31956: A coding deficiency exists in Microsoft Windows NTFS 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 57732 through 57733.
- Microsoft Vulnerability CVE-2021-31959: A coding deficiency exists in Scripting Engine 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 49388 through 49389.
- Microsoft Vulnerability CVE-2021-33739: 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 GID 1, SIDs 57736 through 57737.
- Talos also has added and modified multiple rules in the browser-ie, file-other, malware-backdoor and os-windows rule sets to provide coverage for emerging threats from these technologies.

- **Talos Rules 2021-06-04 (https://www.snort.org/advisories/talos-rules-2021-06-04)**
    - This release provides coverage via SID 57720 for CVE-2021-21985, a remote code execution vulnerability in the vSphere Client's Virtual SAN Health Check plug-in, which is enabled by default in vCenter Server. An attacker with network access to this service can exploit this vulnerability to gain remote code execution on the affected vCenter Server. Talos has added a rule in the 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-2019-6821: (Use of Insufficiently Random Values in Modicon Controllers)
    - Schneider Electric is aware of a vulnerability affecting some of its Modicon line of process controllers.
- CVE-2020-7503: (Security Notification - Easergy T300 (V1.1) | Schneider Electric)
    - A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists which could allow an attacker to execute malicious commands on behalf of a legitimate user when xsrf-token data is intercepted

- CVE-2021-22768: (Improper Input Validation vulnerability in PowerLogic EGX100 and PowerLogicEGX300)
    - A CWE-20: Improper Input Validation vulnerability exists that could cause denial of service or remote code execution via a specially crafted HTTP packet.
- CVE-2021-22766: (Improper Input Validation vulnerability in PowerLogic EGX100 and PowerLogicEGX300)
    - A CWE-20: Improper Input Validation vulnerability exists that could cause denial of service via a specially crafted HTTP packet.
- CVE-2016-4956: (Improper Input Validation in Siemens SIMATIC NET CP 443-1 OPC UA)
    - Successful exploitation of these vulnerabilities could create a denial-of-service condition as well as other specified and unspecified impacts.
- CVE-2020-7505: (Security Notification - Easergy T300 (V1.1) | Schneider Electric)
    - A CWE-494 Download of Code Without Integrity Check vulnerability exists which could allow an attacker to inject data with dangerous content into the firmware and execute arbitrary code on the system
- CVE-2015-7853: (Classic Buffer Overflow in Siemens SIMATIC NET CP 443-1 OPC UA)
    - Successful exploitation of these vulnerabilities could create a denial-of-service condition as well as other specified and unspecified impacts.
- CVE-2021-32926: (Channel Accessible by Non-endpoint in Rockwell Automation Micro800 and MicroLogix 1400)
    - A vulnerability exists in how the Micro800 and MicroLogix 1400 controllers authenticate password change requests. If successfully exploited, this vulnerability may allow a remote, unauthenticated attacker to perform a man-in-the-middle attack in which the attacker intercepts the message that includes the legitimate, new password hash and replaces the legitimate password hash with an illegitimate hash. The user would no longer be able to authenticate to the controller causing a denial-of-service condition.
- CVE-2020-7506: (Security Notification - Easergy T300 (V1.1) | Schneider Electric)
    - A CWE-200: Information Exposure vulnerability exists which could allow an attacker to pack or unpack the archive with the firmware for the controller and modules using the usual tar archiver resulting in an information exposure
- CVE-2016-4955: (Race Condition in Siemens SIMATIC NET CP 443-1 OPC UA)
    - Successful exploitation of these vulnerabilities could create a denial-of-service condition as well as other specified and unspecified impacts.
- CVE-2021-22765: (Improper Input Validation vulnerability in PowerLogic EGX100 and PowerLogicEGX300)
    - A CWE-20: Improper Input Validation vulnerability exists that could cause denial of service or remote code execution via a specially crafted HTTP packet.
- CVE-2017-6458: (Improper Restriction of Operations within the Bounds of a Memory Buffer in Siemens SIMATIC NET CP 443-1 OPC UA)
    - Successful exploitation of these vulnerabilities could create a denial-of-service condition as well as other specified and unspecified impacts.
- CVE-2021-22749: (Exposure of Sensitive Information to an Unauthorized Actor in Modicon X80 BMXNOR0200H RTU Module)

    - A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists that could cause information leak concerning the current RTU configuration including communication parameters dedicated to telemetry, when a specially crafted HTTP request is sent to the web server of the module.
- CVE-2016-7431: (Improper Input Validation in Siemens SIMATIC NET CP 443-1 OPC UA)
    - Successful exploitation of these vulnerabilities could create a denial-of-service condition as well as other specified and unspecified impacts.
- CVE-2020-7507: (Security Notification - Easergy T300 (V1.1) | Schneider Electric)
    - A CWE-400: Uncontrolled Resource Consumption vulnerability exists which could allow an attacker to login multiple times resulting in a denial of service
- CVE-2020-7513: (Security Notification - Easergy T300 (V1.1) | Schneider Electric)
    - A CWE-312: Cleartext Storage of Sensitive Information vulnerability exists which could allow an attacker to intercept traffic and read configuration data
- CVE-2020-7508: (Security Notification - Easergy T300 (V1.1) | Schneider Electric)
    - A CWE-307 Improper Restriction of Excessive Authentication Attempts vulnerability exists which could allow an attacker to gain full access by brute force
- CVE-2020-25180: (Information Disclosure due to Hard-coded Cryptographic Key in ISaGRAF Runtime)
    - ISaGRAF Runtime includes the functionality of setting a password which is required to execute privileged commands. The password value passed to ISaGRAF Runtime is the result of encryption performed with a fixed key value using the Tiny Encryption Algorithm (TEA) on a password that has been entered or saved. A remote, unauthenticated attacker could pass his own encrypted password to the ISaGRAF 5 Runtime, which may result in information disclosure on the device.
- CVE-2020-7511: (Security Notification - Easergy T300 (V1.1) | Schneider Electric)
    - A CWE-327: Use of a Broken or Risky Cryptographic Algorithm vulnerability exists which could allow an attacker to acquire a password by brute force
- CVE-2016-9042: (Improper Input Validation in Siemens SIMATIC NET CP 443-1 OPC UA)
    - Successful exploitation of these vulnerabilities could create a denial-of-service condition as well as other specified and unspecified impacts.
- CVE-2020-8286: (Improper Certificate Validation in Siemens SIMATIC TIM libcurl)
    - Successful exploitation of these third-party vulnerabilities could allow an attacker to extract sensitive information and pass a revoked certificate as valid.
- CVE-2016-2518: (Out-of-bounds Read in Siemens SIMATIC NET CP 443-1 OPC UA)
    - Successful exploitation of these vulnerabilities could create a denial-of-service condition as well as other specified and unspecified impacts.
- CVE-2021-22705: (Improper Restriction ofOperations within the Bounds of a Memory Buffer vulnerability in several Schneider Harmony HMI products)
    - Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause denial of service or unauthorized access to system information when interacting directly with a driver installed by Vijeo Designer or EcoStruxure Machine Expert

- CVE-2020-25176: (Information Disclosure due to cleartext storage of passwords in a file and memory in ISaGRAF Runtime)
    - ISaGRAF Runtime stores the password in plaintext in a file which is located in the same directory with the executable file. ISaGRAF Runtime reads the file and saves the data in a variable without any additional modification. A local, unauthenticated attacker could compromise the user passwords resulting in information disclosure.
- CVE-2020-25178: (Information Disclosure due to Cleartext Transmission of Information in ISaGRAF Runtime)
    - ISaGRAF Workbench communicates with ISaGRAF Runtime using TCP/IP. The communication protocol provides various file system operations as well as uploading applications. Data is transferred over this protocol unencrypted, which could allow a remote, unauthenticated attacker to upload, read and delete files.
- CVE-2021-22767: (Improper Input Validation vulnerability in PowerLogic EGX100 and PowerLogicEGX300)
    - A CWE-20: Improper Input Validation vulnerability exists that could cause denial of service or remote code execution via a specially crafted HTTP packet.
- CVE-2016-7433: (Incorrect Calculation in Siemens SIMATIC NET CP 443-1 OPC UA)
    - Successful exploitation of these vulnerabilities could create a denial-of-service condition as well as other specified and unspecified impacts.
- CVE-2021-22763: (Weak Password Recovery Mechanism for Forgotten Password vulnerability in PowerLogic EGX100, PowerLogicEGX300, PowerLogic PM55xx and PowerLogic PM8ECC)
    - A CWE-640: Weak Password Recovery Mechanism for Forgotten Password vulnerability exists that could allow an attacker administrator level access to a device.
- CVE-2020-8169: (Exposure of Sensitive Information to an Unauthorized Actor in Siemens SIMATIC TIM libcurl)
    - Successful exploitation of these third-party vulnerabilities could allow an attacker to extract sensitive information and pass a revoked certificate as valid.
- CVE-2020-7509: (Security Notification - Easergy T300 (V1.1) | Schneider Electric)
    - A CWE-269: Improper privilege management (write) vulnerability exists which could allow an attacker to elevate their privileges and delete files
- CVE-2021-22764: (Improper Authentication vulnerability in PowerLogic EGX100, PowerLogicEGX300, PowerLogic PM55xx and PowerLogic PM8ECC)
    - A CWE-287: Improper Authentication vulnerability exists that could cause loss of connectivity to the device via Modbus TCP protocol when an attacker sends a specially crafted HTTP request.
- CVE-2020-25182: (Code Execution due to Uncontrolled Search Path Element in ISaGRAF Runtime)
    - ISaGRAF Runtime searches and loads DLLs as dynamic libraries. Uncontrolled loading of dynamic libraries could allow a local, unauthenticated attacker to execute arbitrary code. This vulnerability only affects Microsoft Windows systems running ISaGRAF Runtime.
- CVE-2021-22769: (Improper Privilege Management in Enerlin'X Com'X 510)
    - A CWE-269: Improper Privilege Management vulnerability exists that could cause disclosure of device configuration information to any authenticated user when a specially crafted request is sent to the device.

- CVE-2020-25184: (Information Disclosure due to cleartext storage of passwords in a file and memory in ISaGRAF Runtime)
    - ISaGRAF Runtime stores the password in plaintext in a file which is located in the same directory with the executable file. ISaGRAF Runtime reads the file and saves the data in a variable without any additional modification. A local, unauthenticated attacker could compromise the user passwords resulting in information disclosure.
- CVE-2020-7510: (Security Notification - Easergy T300 (V1.1) | Schneider Electric)
    - A CWE-200: Information Exposure vulnerability exists which could allow attacker to obtain private keys
- CVE-2021-31340: (Uncontrolled Resource Consumption in Siemens SIMATIC RF Products)
    - Successful exploitation of this vulnerability could allow an unauthorized attacker to crash the OPC UA service of the affected devices.
- CVE-2020-7512: (Security Notification - Easergy T300 (V1.1) | Schneider Electric)
    - A CWE-1103: Use of Platform-Dependent Third Party Components with vulnerabilities vulnerability exists which could allow an attacker to exploit the component
- CVE-2020-7504: (Security Notification - Easergy T300 (V1.1) | Schneider Electric)
    - A CWE-20: Improper Input Validation vulnerability exists which could allow an attacker to disable the webserver service on the device when specially crafted network packets are sent
- CVE-2018-0732: (Uncontrolled Resource Consumption in Siemens TIM 1531 IRC)
    - Successful exploitation of this vulnerability could allow a remote attacker to cause a denial-of-service condition.

20210604

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

- **Talos Rules 2021-06-03 (https://www.snort.org/advisories/talos-rules-2021-06-03)**
    - Talos has added and modified multiple rules in the deleted, malware-cnc, malware-other and server-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-06-01 (https://www.snort.org/advisories/talos-rules-2021-06-01)**
    - Talos has added and modified multiple rules in the deleted, indicator-compromise, malware-other, protocol-voip 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-2020-15782: (Improper Restriction of Operations within the Bounds of a Memory Buffer in Siemens SIMATIC S7-1200 and S7-1500 CPU Families)
    - Affected devices are vulnerable to a memory protection bypass through a specific operation. A remote unauthenticated attacker with network access to port 102/tcp could potentially write arbitrary data and code to protected memory areas or read sensitive data to launch further attacks.