Release Notes for Cisco Cyber Vision Knowledge DB

Release 202101

Compatible device list 2
Links 2
  Software Download 2
  Related Documentation 2
Database download 3
How to update the database 3
Release contents 4
  20210129 4
  20210122 4

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-3.2.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-3.2.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-3.2.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-3.2.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-3.2.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-3.2.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.2.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-3.2.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
Updates/3/3.2.0	**Description**
CiscoCyberVision-sysupgrade-3.2.0.dat	System Upgrade file for Center and Sensors 3.1.x to 3.2.0
CiscoCyberVision-sysupgrade-sensor-3.2.0.dat	Cisco Cyber Vision System Upgrade file for IC3000 Sensors or other non IOx Sensors 3.x to 3.2.0
CiscoCyberVision-Embedded-KDB-3.2.0.dat	Knowledge DB embedded in Cisco Cyber Vision 3.2.0
Updates/KDB/KDB.202101	**Description**
CiscoCyberVision_knowledgedb_20210122.db	Knowledge DB version 20210122
CiscoCyberVision_knowledgedb_20210129.db	Knowledge DB version 20210129

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 below. 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 and update network data.

Release contents

20210129

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

- **Talos Rules 2020-12-26 (https://www.snort.org/advisories/talos-rules-2021-01-26)**
  - Talos has added and modified multiple rules in the file-image, file-other, indicator-compromise, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-12-26 (https://www.snort.org/advisories/talos-rules-2021-01-28)**
  - Talos has added and modified multiple rules in the browser-webkit, exploit-kit, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20210122

Up to now, the Cisco Cyber Vision Knowledge DB included the Snort Registered ruleset and the Snort Subscriber ruleset. Starting from this release, the Cisco Cyber Vision Knowledge DB introduces the Snort Community ruleset instead of the Snort Registered ruleset. As such, the following policy will be applied :

- *Users with a paid license will receive the Subscriber ruleset which contains the latest rules made available to Cisco customers as they are released by the Talos Security Intelligence and Research Team.*
- *Users with a free license will receive the Community ruleset which is a subset of the Subscriber ruleset. The Community ruleset is freely available to all Snort users and contains rules that have been submitted by members of the open-source community or by Snort Integrators.*

Unless otherwise specified, all updates reported in the subsequent Knowledge DB release notes will be specific to the Subscriber ruleset.
The Subscriber ruleset is not accessible for users with a Cisco Cyber Vision version prior to 3.2.0. Users running the 3.2.0 version and above can switch between the Community and the Subscriber ruleset through the dedicated Snort page on the Cisco Cyber Vision Center webapp.

Please note that, in order to keep consistency between the Community and the Subscriber ruleset, Snort rules with the same sid are assigned the same category by taking as a baseline the categories within the Subscriber ruleset. Please note also that, when exporting Snort rules, users might notice the presence of empty non-triggering rules. These are used internally to cover the missing sids between the community and the subscriber rulesets and should not trigger any alert. If you observe an alert on one of these rules, please notify the Cisco Cyber Vision team.

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

- **Talos Rules 2020-12-30 (https://www.snort.org/advisories/talos-rules-2020-12-30)**
  - Talos has added and modified multiple rules in the malware-cnc, malware-other, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-01-05 (https://www.snort.org/advisories/talos-rules-2021-01-05)**
  - 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.

- **Talos Rules 2021-01-07 (https://www.snort.org/advisories/talos-rules-2021-01-07)**
  - Talos has added and modified multiple rules in the content-replace and malware-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-01-12 (https://www.snort.org/advisories/talos-rules-2021-01-12)**
  - Talos Microsoft Vulnerability CVE-2021-1647: A coding deficiency exists in Microsoft Defender that may lead to remote code execution.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 56857 through 56860.
  - Microsoft Vulnerability CVE-2021-1707: A coding deficiency exists in Microsoft SharePoint 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 56865.
  - Microsoft Vulnerability CVE-2021-1709: A coding deficiency exists in Microsoft 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 GID 1, SIDs 56849 through 56856.
  - Talos also has added and modified multiple rules in the browser-other, content-replace, file-executable, file-other, malware-cnc, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-01-14 (https://www.snort.org/advisories/talos-rules-2021-01-14)**
  - Talos has added and modified multiple rules in the exploit-kit, file-other, malware-backdoor, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-01-19 (https://www.snort.org/advisories/talos-rules-2021-01-19)**
  - Talos has added and modified multiple rules in the malware-other, malware-tools, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-01-21 (https://www.snort.org/advisories/talos-rules-2021-01-21)**
  - Talos has added and modified multiple rules in the file-other, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

This release also contains additions and modifications following the publication of several vulnerabilities:

- CVE-2020-7568: (Information Disclosure Vulnerability on Modicon M221 Programmable Logic Controller)
  - A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists that could allow non sensitive information disclosure when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M221 controller
- CVE-2020-7567: (Missing Encryption of Sensitive Data Vulnerability on Modicon M221 Programmable Logic Controller)

- A CWE-311: Missing Encryption of Sensitive Data vulnerability exists that could allow the attacker to find the password hash when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M221 controller and broke the encryption keys

- CVE-2020-7566: (Small Space of Random Values Vulnerability on Modicon M221 Programmable Logic Controller)
  - A CWE-334: Small Space of Random Values vulnerability exists that could allow the attacker to break the encryption keys when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M221 controller

- CVE-2020-7565: (Inadequate Encryption Strength Vulnerability on Modicon M221 Programmable Logic Controller)
  - A CWE-326: Inadequate Encryption Strength vulnerability exists that could allow the attacker to break the encryption key when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M221 controller

- CVE-2020-28395: (Use of Hard-coded Cryptographic Key in Siemens SCALANCE family)
  - Devices do not create a new unique private key after factory reset. An attacker could leverage this situation to a man-in-the-middle situation and decrypt previously captured traffic.

- CVE-2020-28391: (Use of Hard-coded Cryptographic Key in Siemens SCALANCE X200)
  - Devices create a new unique key upon factory reset, except when used with C-PLUG. When used with C-PLUG the devices use the hardcoded private RSA-key shipped with the firmware-image. An attacker could leverage this situation to a man-in-the-middle situation and decrypt previously captured traffic.

- CVE-2020-28214: (Use of a One-Way Hash with a Predictable Salt vulnerability in Modicon M221)
  - A CWE-760: Use of a One-Way Hash with a Predictable Salt vulnerability exists that could allow an attacker to pre-compute the hash value using dictionary attack technique such as rainbow tables, effectively disabling the protection that an unpredictable salt would provide

- CVE-2020-27338: (Improper Input Validation in Treck's IPv6 stack)
  - A CWE-125: Out-of-bounds Read vulnerability exists that could cause improper input validation in the DHCPv6 component when handling a packet sent by a remote attacker.

- CVE-2020-27337: (Improper Input Validation in Treck's IPv6 stack)
  - A CWE-787: Out-of-bounds Write vulnerability exists that could cause improper input validation in the ICMPv6 component when handling a packet sent by a remote attacker.

- CVE-2020-27336: (Improper Input Validation in Treck's IPv6 stack)
  - A CWE-125: Out-of-bounds Read vulnerability exists that could cause improper input validation in the IPv6 component when handling a packet sent by a remote attacker

- CVE-2020-25226: (Heap-based Buffer Overflow in Siemens SCALANCE X Products)
  - Successful exploitation of these vulnerabilities could cause denial-of-service conditions and further impact the system through heap and buffer overflows.

- CVE-2020-25066: (Heap-based buffer overflow in Treck HTTP Server)
  - A heap-based buffer overflow in the Treck HTTP Server component before 6.0.1.68 allows remote attackers to cause a denial of service (crash/reset) or to possibly execute arbitrary code.

- CVE-2020-15800: (Heap-based Buffer Overflow in Siemens SCALANCE X Products)
  - The web server of the affected devices contains a vulnerability that may lead to a buffer overflow condition. An attacker could cause this condition on the webserver by sending a specially crafted request. The webserver could stop and not recover anymore.

- CVE-2020-15799: (Missing Authentication for Critical Function in Siemens SCALANCE X Products)
  - The vulnerability could allow an unauthenticated attacker to reboot the device over the network by using special urls from integrated web server of the affected products.

- CVE-2020-12524: (BTP Touch Panels uncontrolled resource consumption)
  - Uncontrolled Resource Consumption can be exploited to cause the HMI to become unresponsive and not accurately update the display content (Denial of Service).

- CVE-2020-12523: (Missing Initialization of Resource in mGuard products)
  - For mGuard devices with integrated switch on the LAN side, single switch ports can be disabled by device configuration. After a reboot these ports get functional independent from their configuration setting: Missing Initialization of Resource (CWE-909). After a reboot, affected mGuard devices may unexpectedly receive or send data on disabled switch ports. This includes the unexpected provision of administrative interfaces. Attackers may try to access confidential data or compromise the availability of mGuard services by flooding or resource exhaustion.

- CVE-2020-12521: (Improper Input Validation in PLCnext Control devices)
  - A specially crafted LLDP packet may lead to a high system load in the PROFINET stack. An attacker can cause failure of system services or a complete reboot.

- CVE-2020-12519: (Improper Privilege Management in PLCnext Control devices)
  - An attacker can use this vulnerability i.e., to open a reverse shell with root privileges.

- CVE-2020-12518: (Exposure of Sensitive Information in PLCnext Control devices)
  - An attacker can use the knowledge gained by reading the insufficiently protected sensitive information to plan further attacks.

- CVE-2020-12517: (Improper Neutralization of Input in PLCnext Control devices)
  - An authenticated low privileged user could embed malicious Javascript code to gain admin rights when the admin user visits the vulnerable website (local privilege escalation).

- CVE-2020-11914: (Improper input validation in Treck TCP/IP Stack)

- Improper input validation in ARP component when handling a packet sent by an unauthorized network attacker. This vulnerability may allow out-of-bounds Read.

- CVE-2020-11913: (Improper input validation in Treck TCP/IP Stack)
  - Improper input validation in IPv6 component when handling a packet sent by an unauthorized network attacker. This vulnerability may allow out-of-bounds Read.

- CVE-2020-11912: (Improper input validation issue in Treck TCP/IP Stack)
  - There is an improper input validation issue in the IPv6 component. A remote, unauthenticated attacker can send a malicious packet that may expose some data that is present outside the bounds of allocated memory.

- CVE-2020-11911: (Improper access control issue in Treck TCP/IP Stack)
  - There is an improper access control issue in the ICPMv4 component. A remote, unauthenticated attacker can send a malicious packet that can lead to higher privileges in permissions assignments for some critical resources on the destination device.

- CVE-2020-11910: (Improper input validation issue in Treck TCP/IP Stack)
  - There is an improper input validation issue in the ICMPv4 component. A remote, unauthenticated attacker can send a malicious packet that may expose data present outside the bounds of allocated memory.

- CVE-2020-11909: (Possible integer underflow in Treck TCP/IP Stack)
  - The Treck TCP/IP stack before 6.0.1.66 has an IPv4 Integer Underflow

- CVE-2020-11908: (Improper null termination in Treck TCP/IP Stack)
  - Improper null termination in DHCP component when handling a packet sent by an unauthorized network attacker. This vulnerability may allow exposure of sensitive information.

- CVE-2020-11907: (Improper handling of length parameter consistency issue in Treck TCP/IP Stack)
  - There is an improper handling of length parameter consistency issue in the TCP component. A remote, unauthenticated, attacker can send a malformed TCP packet that can trigger an integer underflow event leading to a crash or segmentation fault on the device.

- CVE-2020-11906: (Improper input validation issue in the Ethernet Link Layer in Treck TCP/IP Stack)
  - There is an improper input validation issue in the Ethernet Link Layer component. An adjacent, unauthenticated attacker can send a malicious Ethernet packet that can trigger an integer underflow event leading to a crash or segment fault on the target device.

- CVE-2020-11905: (Possible out-of-bounds read in Treck TCP/IP Stack)
  - Possible out-of-bounds read in DHCPv6 component when handling a packet sent by an unauthorized network attacker. This vulnerability may allow exposure of sensitive information.

- CVE-2020-11904: (Possible integer overflow in Treck TCP/IP Stack)

- Possible integer overflow or wraparound in memory allocation component when handling a packet sent by an unauthorized network attacker may result in out-of-bounds write.

- CVE-2020-11903: (Possible out-of-bounds read in Treck TCP/IP Stack)
  - Possible out-of-bounds read in DHCP component when handling a packet sent by an unauthorized network attacker. This vulnerability may allow exposure of sensitive information.

- CVE-2020-11902: (Improper input validation in Treck TCP/IP Stack)
  - Improper input validation in IPv6 over IPv4 tunneling component when handling a packet sent by an unauthorized network attacker. This vulnerability may allow out-of-bounds Read.

- CVE-2020-11901: (Improper input validation in DNS resolver in Treck TCP/IP Stack)
  - There is an improper input validation issue in the DNS resolver component when handling a sent packet. A remote, unauthenticated attacker may be able to inject arbitrary code on the target system using a maliciously crafted packet.

- CVE-2020-11900: (Possible double free in Treck TCP/IP Stack)
  - Possible double free in IPv4 tunneling component when handling a packet sent by a network attacker. This vulnerability may result in use after free.

- CVE-2020-11899: (Improper input validation in Treck TCP/IP Stack)
  - Improper input validation in IPv6 component when handling a packet sent by an unauthorized network attacker. This vulnerability may allow out-of-bounds Read and a possible Denial of Service.

- CVE-2020-11898: (Improper handling of length parameter inconsistency in Treck TCP/IP Stack)
  - Improper handling of length parameter inconsistency in IPv4/ICMPv4 component when handling a packet sent by an unauthorized network attacker. This vulnerability may result in out-of-bounds Read.

- CVE-2020-11897: (Improper handling of length parameter inconsistency in Treck TCP/IP Stack)
  - Improper handling of length parameter inconsistency in IPv6 component when handling a packet sent by an unauthorized network attacker. This vulnerability may result in possible out-of-bounds write.

- CVE-2020-11896: (Improper handling of length parameter inconsistency in Treck TCP/IP Stack)
  - Improper handling of length parameter inconsistency in IPv4/UDP component when handling a packet sent by an unauthorized network attacker. This vulnerability may result in remote code execution.

- CVE-2019-19301: (Segment Smack in VxWorks-based Industrial Devices)
  - The VxWorks-based Profinet TCP Stack can be forced to make very expensive calls for every incoming packet which can lead to a denial of service

- CVE-2019-13939: (DHCP Client Vulnerability in SIMOTICS CONNECT 400, Desigo PXC/PXM, APOGEE MEC/MBC/PXC, APOGEE PXC Series, and TALON TC Series)

- SIMOTICS CONNECT 400, Desigo (Power PC-based), APOGEE MEC/MBC/PXC and TALON TC products are affected by a DHCP Client vulnerability as initially reported in SSA-434032 for the MentorNucleus Networking Module. By sending specially crafted DHCP packets to a device where the DHCP client is enabled, an attacker could change the IP address of the device to an invalid value.

- CVE-2019-10998: (Physical access to SD card enables authentication bypass opportunity in Phoenix Contact PLCNext AXC F 2152)
  - State of the art PLC devices offer SD cards to store the PLC's data. In case of hardware failure easy and fast hardware replacement is required in industrial applications. Replacement of the SD card without any additional tools and knowledge about the PLC or PLCs toolchain as well as automatic startup is a must. To support this handling the physical access to the PLC device must be restricted by organizational measurements (e.g.: locked cabinets or other limited accesses)In special use cases it might be not possible to effectively restrict access to authorized personal. In such application scenarios, manipulation of the SD card is possible.

- CVE-2019-10997: (Man-in-the-Middle Vulnerability in Phoenix Contact PLCNext AXC F 2152)
  - Protocol Fuzzing on PC WORX Engineer by a man in the middle attacks stops the PLC service. The device must be rebooted, or the PLC service must be restarted manually via Linux shell.

- CVE-2019-10936: (Denial-of-Service Vulnerability in Profinet Devices)
  - A vulnerability in affected devices could allow an attacker to perform a denial-of-service attack if a large amount of specially crafted UDP packets is sent to the device.

- CVE-2018-7559: (User Authentication Token Exploit in Phoenix Contact PLCNext AXC F 2152)
  - The OPC Foundation has published CVE-2018-7559 with a Security Bulletin on April 12, 2018.This vulnerability affects the handling of User Identity Tokens when used with the Basic128Rsa15 security policy. The vulnerability allows an attacker to decrypt a previously captured password or to sign arbitrary data. The Basic128Rsa15 security policy is deprecated by the UA Specification since July 2015,therefore it is recommended not to use this policy any longer.