Release Notes for Cisco Cyber Vision Knowledge DB

Release 20200624

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-3.1.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-3.1.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-3.1.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-3.1.0.tar	IE3400, IR1101 sensor installation and update file
CiscoCyberVision-IOx-IC3K-3.1.0.tar	IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.1.0.tar	Cat9k sensor installation and update file
Updates/3/3.1.0	**Description**
CiscoCyberVision-update-center-3.1.0.dat	Center update file
CiscoCyberVision-update-sensor-3.1.0.dat	Sentryo Sensor3, 5, 7 update file
CiscoCyberVision-update-combined-3.1.0.dat	Center and Legacy Sensor update file from GUI
CiscoCyberVision-Embedded-KDB-3.1.0.dat	Knowledge DB embedded in Cisco Cyber Vision 3.1.0
Updates/KDB	**Description**
CiscoCyberVision_knowledgedb_20200618.db	Knowledge DB version 20200618

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_Release_3_1_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.

Please note that the product may not show the CVSS score for some of these vulnerabilities due to ongoing work on the integration of CVSSv3 scores.

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

The new version is available following the publication and the update of several vulnerabilities. These new additions are a subset of the Ripple20 (https://www.jsof-tech.com/ripple20/) vulnerabilities targeting Rockwell products:

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

There is an improper input validation issue in the ARP component. An unauthenticated, local attacker can send a malicious Layer-2 ARP packet that could lead to unintended exposure of some sensitive information on the target device.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

Cisco Cyber Vision detects the presence of these vulnerabilities using this new Knowledge DB.

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

- Talos Rules 2020-06-09 (https://www.snort.org/advisories/talos-rules-2020-06-09)
- Talos Rules 2020-06-11 (https://www.snort.org/advisories/talos-rules-2020-06-11)
- Talos Rules 2020-06-12 (https://www.snort.org/advisories/talos-rules-2020-06-12)
- Talos Rules 2020-06-16 (https://www.snort.org/advisories/talos-rules-2020-06-16)
- Talos Rules 2020-06-18 (https://www.snort.org/advisories/talos-rules-2020-06-18)
- Talos Rules 2020-06-23 (https://www.snort.org/advisories/talos-rules-2020-06-23)

If needed, the Cisco Cyber Vision security team is willing to help you analyze and patch your network.