Release Notes for Cisco Cyber Vision Knowledge DB

Release 202008

Compatible device list 2
Links 2
  Software Download 2
  Related Documentation 2
Database download 3
How to update the database 3
Release contents 4
  20200827 4
  20200821 4
  20200814 4
  20200807 6

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	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-3.1.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.1.0.tar	Cisco Catalyst 9300 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/KDB.202008	**Description**
CiscoCyberVision_knowledgedb_20200807.db	Knowledge DB version 20200807
CiscoCyberVision_knowledgedb_20200814.db	Knowledge DB version 20200814
CiscoCyberVision_knowledgedb_20200821.db	Knowledge DB version 20200821
CiscoCyberVision_knowledgedb_20200827.db	Knowledge DB version 20200827

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

20200827

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

- **Talos Rules 2020-08-25 (https://www.snort.org/advisories/talos-rules-2020-08-25)**
  - Talos has added and modified multiple rules in the file-office, file-pdf, malware-other, os-other, os-windows and server-other rule sets to provide coverage for emerging threats from these technologies.

20200821

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

- **Talos Rules 2020-08-18 (https://www.snort.org/advisories/talos-rules-2020-08-18)**
  - Talos has added and modified multiple rules in the file-executable, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-08-20 (https://www.snort.org/advisories/talos-rules-2020-08-20)**
  - Talos has added and modified multiple rules in the file-flash, file-multimedia, malware-cnc, malware-other, malware-tools, os-other, os-windows, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20200814

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

- **Talos Rules 2020-08-11 (https://www.snort.org/advisories/talos-rules-2020-08-11)**
  - Microsoft Vulnerability CVE-2020-1380: A coding deficiency exists in Microsoft Windows Scripting Engine 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 54743 through 54744.
  - Microsoft Vulnerability CVE-2020-1480: A coding deficiency exists in Microsoft Windows GDI 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 54745 through 54746.
  - Microsoft Vulnerability CVE-2020-1529: A coding deficiency exists in Microsoft Windows GDI 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 54737 through 54738.
  - Microsoft Vulnerability CVE-2020-1566: A coding deficiency exists in Microsoft Windows Kernel 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 54765 through 54766.
  - Microsoft Vulnerability CVE-2020-1567: A coding deficiency exists in Microsoft Windows MSHTML Engine 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 54741 through 54742.
  - Microsoft Vulnerability CVE-2020-1570: A coding deficiency exists in Microsoft Windows Scripting Engine 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 54739 through 54740.
  - Microsoft Vulnerability CVE-2020-1578: 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 54753 through 54754.
  - Microsoft Vulnerability CVE-2020-1584: A coding deficiency exists in Microsoft Windows dnsrslvr.dll 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 54735 through 54736.
  - Microsoft Vulnerability CVE-2020-1587: A coding deficiency exists in Microsoft Windows Ancillary Function Driver for WinSock 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 54733 through 54734.
  - Talos also has added and modified multiple rules in the browser-ie, file-flash, file-image, file-office, file-other, file-pdf, indicator-compromise, malware-backdoor, malware-cnc, malware-other, os-other, os-windows, policy-other, protocol-scada, server-oracle and server-webapp rule sets to provide coverage for emerging threats from these technologies.

- **Talos Rules 2020-08-13 (https://www.snort.org/advisories/talos-rules-2020-08-13)**
  - Talos has added and modified multiple rules in the 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:

1. CVE-2020-8597: (Buffer Overflow Vulnerability in Siemens SCALANCE, RUGGEDCOM)
   The version of pppd shipped with this product has a vulnerability that may allow an unauthenticated remote attacker to cause a stack buffer overflow, which may allow arbitrary code execution on the target system.

2. CVE-2020-7525: (Improper Restriction of Excessive Authentication Attempts vulnerability in spaceLYnk & Wiser for KNX)
   A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists which could allow an attacker to guess a password when brute force is used

3. CVE-2020-7524: (Out-of-bounds Write vulnerability in Modicon M218 Logic Controller)
   A CWE-787:Out-of-bounds Write vulnerability exists which could cause Denial of Service when sending specific crafted IPV4 packet to the controller: Sending a specific IPv4 protocol package to Schneider Electric Modicon M218 Logic Controller can cause IPv4 devices to go down. The device does not work properly and must be powered back on to return to normal.

4. CVE-2020-5609: (Path Traversal Vulnerability in Yokogawa CENTUM)
   Successful exploitation of these vulnerabilities could allow a remote unauthenticated attacker to send tampered communication packets or create/overwrite any file and run any commands.

5. CVE-2020-5608: (Improper Authentication Vulnerability in Yokogawa CENTUM)
   Successful exploitation of these vulnerabilities could allow a remote unauthenticated attacker to send tampered communication packets or create/overwrite any file and run any commands.

6. CVE-2020-15781: (Cross-Site Scripting Vulnerability in Siemens SICAM A8000 RTUs)
   The login screen does not sufficiently sanitize input, which enables an attacker to generate specially crafted log messages. If an unsuspecting victim views the log messages via the web browser, these log messages might be interpreted and executed as code by the web application. This Cross-Site-Scripting (XSS) vulnerability might compromize the confidentiality, integrity and availability of the web application

7. CVE-2019-19301: (SegmentSmack 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

8. CVE-2019-19193: (SweynTooth vulnerability)
   The Bluetooth Low Energy peripheral implementation on Texas Instruments SIMPLELINK-CC2640R2-SDK through 3.30.00.20 and BLE-STACK through 1.5.0 before Q4 2019 for CC2640R2 and CC2540/1 devices does not properly restrict the advertisement connection request packet on reception, allowing attackers in radio range to cause a denial of service (crash) via a crafted packet.

9. CVE-2019-15126: (Information Disclosure Vulnerability (Kr00k) in Industrial Wi-Fi Products)
   Successful exploitation of this vulnerability could allow an attacker to read a discrete set of traffic over the air after a Wi-Fi device state change.

10. 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 are sent to the device.

11. CVE-2018-7857: (Multiple vulnerabilities in Modicon controllers)
    Schneider Electric is aware of multiple vulnerabilities in its Modicon Controller products.

20200807

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

- **Talos Rules 2020-08-04 (https://www.snort.org/advisories/talos-rules-2020-08-04)**
- **Talos Rules 2020-08-06 (https://www.snort.org/advisories/talos-rules-2020-08-06)**

In this release we also enabled some specific OT-related rules from Talos that were disabled by default.

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