Release Notes for Cisco Cyber Vision Knowledge DB

Release 202009

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.202009	**Description**
CiscoCyberVision_knowledgedb_20200904.db	Knowledge DB version 20200904
CiscoCyberVision_knowledgedb_20200911.db	Knowledge DB version 20200911
CiscoCyberVision_knowledgedb_20200918.db	Knowledge DB version 20200918
CiscoCyberVision_knowledgedb_20200925.db	Knowledge DB version 20200925

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

20200925

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

- **Talos Rules 2020-09-22 (https://www.snort.org/advisories/talos-rules-2020-09-22)**
  - Talos has added and modified multiple rules in the file-other, malware-other, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-09-24 (https://www.snort.org/advisories/talos-rules-2020-09-24)**
  - Talos has added and modified multiple rules in the app-detect, browser-chrome, browser-other, file-multimedia, file-other, indicator-compromise, indicator-shellcode, malware-backdoor, malware-cnc, malware-other, malware-tools, os-linux, policy-other, protocol-dns, protocol-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20200918

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

- **Talos Rules 2020-09-15 (https://www.snort.org/advisories/talos-rules-2020-09-15)**
  - Talos has added and modified multiple rules in the file-other, indicator-scan, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-09-15 (https://www.snort.org/advisories/talos-rules-2020-09-15-9-15-2020)**
  - Talos has added and modified multiple rules in the and os-windows rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-09-17 (https://www.snort.org/advisories/talos-rules-2020-09-17)**
  - Talos has added and modified multiple rules in the browser-ie, file-image, file-office, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20200911

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

- **Talos Rules 2020-09-08 (https://www.snort.org/advisories/talos-rules-2020-09-08)**
  - Microsoft Vulnerability CVE-2020-0664: A coding deficiency exists in Active Directory 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 55139 through 55140.

- Microsoft Vulnerability CVE-2020-0856: A coding deficiency exists in Active Directory that may lead to information disclosure.
- A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 1, SID 55206.
- Microsoft Vulnerability CVE-2020-0941: A coding deficiency exists in Microsoft Win32k 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 55187 through 55188.
- Microsoft Vulnerability CVE-2020-1115: 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 55141 through 55142.
- Microsoft Vulnerability CVE-2020-1152: 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 55161 through 55162.
- Microsoft Vulnerability CVE-2020-1245: 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 55143 through 55144.
- Microsoft Vulnerability CVE-2020-1308: A coding deficiency exists in DirectX 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 55145 through 55146.
- Talos also has added and modified multiple rules in the browser-chrome, file-other, malware-cnc, malware-other, os-windows, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

- **Talos Rules 2020-09-10 (https://www.snort.org/advisories/talos-rules-2020-09-10)**
  - Talos has added and modified multiple rules in the malware-other 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-2020-15791: (Insufficiently Protected Credentials Vulnerability in Siemens SIMATIC S7-300 and S7-400 CPUs)**
   - The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials.
2. **CVE-2020-15787: (Authentication Bypass by Primary Weakness Vulnerability in Siemens SIMATIC HMI**

Products)

- Affected devices insufficiently validate authentication attempts as the information given can be truncated to match only a set number of characters versus the whole provided string. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack.

3. **CVE-2020-15786: (Improper Restriction of Excessive Authentication Attempts Vulnerability in Siemens SIMATIC HMI Products)**
   - Affected devices insufficiently block excessive authentication attempts. This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack.
4. **CVE-2020-0543: (Exposure of Sensitive Information to an Unauthorized Actor Vulnerability in Siemens Industrial Products (Special Register Buffer Data Sampling aka Crosstalk))**
   - Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access

20200904

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

- **Talos Rules 2020-08-27 (https://www.snort.org/advisories/talos-rules-2020-08-27)**
  - Talos has added and modified multiple rules in the indicator-compromise, malware-cnc, malware-other, protocol-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-08-28 (https://www.snort.org/advisories/talos-rules-2020-08-28)**
  - Talos is releasing SID 54902 to address anomalous DVMRP traffic. This traffic has been associated with DOS incidents.
  - Talos has added and modified multiple rules in the file-identify and protocol-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-09-01 (https://www.snort.org/advisories/talos-rules-2020-09-01)**
  - Talos has added and modified multiple rules in the file-other, malware-other, malware-tools and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-09-03 (https://www.snort.org/advisories/talos-rules-2020-09-03)**
  - Talos has added and modified multiple rules in the browser-chrome, browser-webkit, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.