Release Notes for Cisco Cyber Vision Knowledge DB

Release 202007

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	**Description**
CiscoCyberVision_knowledgedb_20200702.db	Knowledge DB version 20200702
CiscoCyberVision_knowledgedb_20200709.db	Knowledge DB version 20200709
CiscoCyberVision_knowledgedb_20200716.db	Knowledge DB version 20200716
CiscoCyberVision_knowledgedb_20200723.db	Knowledge DB version 20200723

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

20200731

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

- Talos Rules 2020-07-28 (https://www.snort.org/advisories/talos-rules-2020-07-28)
- Talos Rules 2020-07-30 (https://www.snort.org/advisories/talos-rules-2020-07-30)

20200723

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

- **Talos Rules 2020-07-16 (https://www.snort.org/advisories/talos-rules-2020-07-16)**
  - 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 2020-07-16 (https://www.snort.org/advisories/talos-rules-2020-07-16-7-16-2020)**
  - Talos has added and modified multiple rules in the server-other rule sets to provide coverage for emerging threats from these technologies.

- **Talos Rules 2020-07-21 (https://www.snort.org/advisories/talos-rules-2020-07-21)**
  - Talos has added and modified multiple rules in the browser-chrome, browser-webkit, file-other, os-windows, policy-other, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.

- **Talos Rules 2020-07-23 (https://www.snort.org/advisories/talos-rules-2020-07-23)**
  - Talos has added and modified multiple rules in the browser-chrome, file-office, file-other, malware-cnc, malware-other, protocol-dns, server-mail 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-2020-11914: (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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20200716

This release includes additions and modifications to the Snort ruleset covering the following Talos advisories. In particular, these new rules detect vulnerabilities affecting products from Microsoft Corporation such as CVE-2020-1350 which enables remote code execution on Microsoft Windows DNS servers:

- **Talos Rules 2020-07-14 (https://www.snort.org/advisories/talos-rules-2020-07-14)**
    - Microsoft Vulnerability CVE-2020-1147: A coding deficiency exists in .NET Framework, SharePoint Server, and Visual Studio 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 54511.
    - Microsoft Vulnerability CVE-2020-1350: A coding deficiency exists in Microsoft Windows DNS server 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 54518.
    - Microsoft Vulnerability CVE-2020-1374: A coding deficiency exists in Remote Desktop Client 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 54523.

- Microsoft Vulnerability CVE-2020-1381: A coding deficiency exists in Microsoft Windows Graphics Component 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 54521 through 54522.
- Microsoft Vulnerability CVE-2020-1382: A coding deficiency exists in Microsoft Windows Graphics Component 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 54512 through 54515.
- Microsoft Vulnerability CVE-2020-1399: A coding deficiency exists in Microsoft Windows Runtime 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 54534 through 54535.
- Microsoft Vulnerability CVE-2020-1403: A coding deficiency exists in Microsoft Windows VBScript 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 54509 through 54510.
- Microsoft Vulnerability CVE-2020-1410: A coding deficiency exists in Microsoft Windows Address Book 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 54528 through 54533.
- Microsoft Vulnerability CVE-2020-1426: 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 54516 through 54517.
- Talos also has added and modified multiple rules in the browser-chrome, browser-ie, file-executable, file-other, malware-cnc, malware-other, os-other, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.

- **Talos Rules 2020-07-09 (https://www.snort.org/advisories/talos-rules-2020-07-09)**
  - Talos has added and modified multiple rules in the deleted, 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:

1. CVE-2020-7593: (Classic Buffer Overflow Vulnerability in Siemens LOGO! Web Server)

A buffer overflow vulnerability exists in the Web Server functionality of the device. A remote unauthenticated attacker could send a specially crafted HTTP request to cause a memory corruption, potentially resulting in remote code execution

2. CVE-2020-7592: (Cleartext Transmission of Sensitive Information Vulnerability in Siemens SIMATIC HMI Panels)

Unencrypted communication between the configuration software and the respective device could allow an attacker to capture potential plain text communication and have access to sensitive information.

3. CVE-2020-7584: (Uncontrolled Resource Consumption Vulnerability in Siemens SIMATIC S7-200 SMART CPU Family)

Affected devices do not properly handle large numbers of new incoming connections and could crash under certain circumstances. An attacker may leverage this to cause a Denial-of-Service situation.

4. CVE-2020-10045: (Authentication Bypass by Capture-replay Vulnerability in Siemens SICAM MMU, SICAM T, and SICAM SGU)

An error in the challenge-response procedure could allow an attacker to replay authentication traffic and gain access to protected areas of the web application

5. CVE-2020-10044: (Missing Authentication for Critical Function in Siemens SICAM MMU, SICAM T, and SICAM SGU)

An attacker with access to the network could be able to install specially crafted firmware to the device.

6. CVE-2020-10043: (Basic XSS Vulnerability in Siemens SICAM MMU, SICAM T, and SICAM SGU)

The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link

7. CVE-2020-10042: (Classic Buffer Overflow Vulnerability in Siemens SICAM MMU, SICAM T, and SICAM SGU)

A buffer overflow in various positions of the web application might enable an attacker with access to the web application to execute arbitrary code over the network.

8. CVE-2020-10041: (Cross-site Scripting Vulnerability in Siemens SICAM MMU, SICAM T, and SICAM SGU)

A stored Cross-Site-Scripting (XSS) vulnerability is present in different locations of the web application. An attacker might be able to take over a session of a legitimate user

9. CVE-2020-10040: (Use of Password Hash with Insufficient Computational Effort Vulnerability in Siemens SICAM MMU, SICAM T, and SICAM SGU)

An attacker with local access to the device might be able to retrieve some passwords in clear text.

10. CVE-2020-10039: (Missing Encryption of Sensitive Data in Siemens SICAM MMU, SICAM T, and SICAM SGU)

    An attacker in a privileged network position between a legitimate user and the web server might be able to conduct a Man-in-the-middle attack and gain read and write access to the transmitted data.

11. CVE-2020-10038: (Missing Authentication for Critical Function Vulnerability in Siemens SICAM MMU, SICAM T, and SICAM SGU)

    An attacker with access to the device's web server might be able to execute administrative commands without authentication.

12. CVE-2020-10037: (Out-of-bounds Read Vulnerability in Siemens SICAM MMU, SICAM T, and SICAM SGU)

    By performing a flooding attack against the web server, an attacker might be able to gain read access to the device's memory, possibly revealing confidential information.

20200709

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

- Talos Rules 2020-07-02 (https://www.snort.org/advisories/talos-rules-2020-07-02)
- Talos Rules 2020-07-06 (https://www.snort.org/advisories/talos-rules-2020-07-06)

20200702

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

- Talos Rules 2020-06-25 (https://www.snort.org/advisories/talos-rules-2020-06-25)
- Talos Rules 2020-06-30 (https://www.snort.org/advisories/talos-rules-2020-06-30)

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