Release Notes for Cisco Cyber Vision Knowledge DB

Release 202103

Compatible device list 2
Links 2
Software Download 2
Related Documentation 2
Database download 3
How to update the database 3
Release contents 4
20210326 4
20210319 4
20210312 4
20210305 7

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-3.2.2.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-3.2.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-3.2.2.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-3.2.2.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-3.2.2.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-3.2.2.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.2.2.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-3.2.2.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-3.2.2.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates/3/3.2.2	**Description**
CiscoCyberVision-sysupgrade-3.2.2.dat	System Upgrade file for Center and Sensors 3.1.x to 3.2.2
CiscoCyberVision-sysupgrade-sensor-3.2.2.dat	Cisco Cyber Vision System Upgrade file for IC3000 Sensors or other non IOx Sensors 3.x to 3.2.2
CiscoCyberVision-Embedded-KDB-3.2.2.dat	Knowledge DB embedded in Cisco Cyber Vision 3.2.2
Updates/KDB/KDB.202102	**Description**
CiscoCyberVision_knowledgedb_20210305.db	Knowledge DB version 20210305
CiscoCyberVision_knowledgedb_20210312.db	Knowledge DB version 20210312
CiscoCyberVision_knowledgedb_20210319.db	Knowledge DB version 20210319
CiscoCyberVision_knowledgedb_20210326.db	Knowledge DB version 20210326

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 above.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.

Release contents

20210326

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

- **Talos Rules 2021-03-23 (https://www.snort.org/advisories/talos-rules-2021-03-23)**
  - Talos has added and modified multiple rules in the malware-other, netbios and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-03-25 (https://www.snort.org/advisories/talos-rules-2021-03-25)**
  - Talos has added and modified multiple rules in the browser-other, malware-cnc, os-windows, protocol-tftp and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20210319

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

- **Talos Rules 2021-03-16 (https://www.snort.org/advisories/talos-rules-2021-03-16)**
  - Talos has added and modified multiple rules in the file-pdf and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-03-18 (https://www.snort.org/advisories/talos-rules-2021-03-18)**
  - Talos has added and modified multiple rules in the file-image, file-pdf, malware-backdoor, malware-cnc, netbios, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20210312

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

- **Talos Rules 2021-03-09 (https://www.snort.org/advisories/talos-rules-2021-03-09)**
  - This release adds and modifies rules in several categories
    - Microsoft Vulnerability CVE-2021-24095: 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 57259 through 57260.
    - Microsoft Vulnerability CVE-2021-26411: A coding deficiency exists in Microsoft Internet Explorer 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 57268 through 57269.
    - Microsoft Vulnerability CVE-2021-26855: A coding deficiency exists in Microsoft Exchange Server that may lead to remote code execution.

- Previously released rules will detect attacks targeting these vulnerabilities and have been updated with the appropriate reference information. They are also included in this release and are identified with GID 1, SIDs 57241 through 57244.
- Microsoft Vulnerability CVE-2021-26857: A coding deficiency exists in Microsoft Exchange Server that may lead to remote code execution.
- Previously released rules will detect attacks targeting these vulnerabilities and have been updated with the appropriate reference information. They are also included in this release and are identified with GID 1, SIDs 57233 through 57234.
- Microsoft Vulnerability CVE-2021-26858: A coding deficiency exists in Microsoft Exchange Server that may lead to remote code execution.
- Previously released rules will detect attacks targeting these vulnerabilities and have been updated with the appropriate reference information. They are also included in this release and are identified with GID 1, SIDs 57245 through 57246.
- Microsoft Vulnerability CVE-2021-26863: 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 57263 through 57264.
- Microsoft Vulnerability CVE-2021-26868: A coding deficiency exists in Microsoft 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 57261 through 57262.
- Microsoft Vulnerability CVE-2021-26877: 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 57274.
- Microsoft Vulnerability CVE-2021-26897: A coding deficiency exists in Microsoft Windows DNS server that may lead to remote code execution.
- A previously released rule will detect attacks targeting these vulnerabilities and has been updated with the appropriate reference information. It is included in this release and is identified with GID 1, SID 54518.
- Microsoft Vulnerability CVE-2021-27065: A coding deficiency exists in Microsoft Exchange Server that may lead to remote code execution.
- Previously released rules will detect attacks targeting these vulnerabilities and have been updated with the appropriate reference information. They are also included in this release and are identified with GID 1, SIDs 57245 through 57246 and 57252 through 57253.
- Microsoft Vulnerability CVE-2021-27076: A coding deficiency exists in Microsoft SharePoint Server 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 57275 through 57276.

- Talos also has added and modified multiple rules in the browser-firefox, browser-ie, file-image, file-pdf, indicator-compromise, netbios, os-other, os-windows, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

- **Talos Rules 2021-03-11 (https://www.snort.org/advisories/talos-rules-2021-03-11)**
  - Talos has added and modified multiple rules in the file-other, malware-backdoor, netbios, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.

This release also adds support for the detection of the following vulnerability:

- CVE-2021-25667: (Stack-based Buffer Overflow in Siemens SCALANCE and RUGGEDCOM Devices)
  - Affected devices contain a stack-based buffer overflow vulnerability in the handling of STP BPDU frames that could allow a remote attacker to trigger a denial-of-service condition or potentially remote code execution. Successful exploitation requires the passive listening feature of the device to be active.
- CVE-2021-25676: (Improper Restriction of Excessive Authentication Attempts in Siemens SCALANCE and RUGGEDCOM Devices)
  - Multiple failed SSH authentication attempts could trigger a temporary Denial-of-Service under certain conditions. When triggered, the device will reboot automatically.
- CVE-2020-25236: (Improper Handling of Exceptional Conditions in Siemens LOGO! 8 BM)
  - The control logic (CL) the LOGO! 8 executes could be manipulated in a way that could cause the device executing the CL to improperly handle the manipulation and crash. After successful execution of the attack, the device needs to be manually reset.
- CVE-2020-17437: (Out-of-bounds Write Vulnerability in embedded TCP/IP Stack (Amnesia:33))
  - The TCP/IP stack (uIP) in affected devices is vulnerable to out-of-bounds write when processing TCP packets with urgent pointer (URG) where the location of the TCP data payload is calculated improperly.(FSCT-2020-0018)An attacker located in the same network could trigger a Denial-of-Service condition on the device by sending a specially crafted IP packet.
- CVE-2020-13987: (Out-of-bounds Read Vulnerability in embedded TCP/IP Stack (Amnesia:33))
  - The TCP/IP stack (uIP) in affected devices is vulnerable to out-of-bounds read when calculating the checksum for IP packets. (FSCT-2020-0009)An attacker located in the same network could trigger a Denial-of-Service condition on the device by sending a specially crafted IP packet.
- CVE-2020-25241: (Improper Validation of Specified Index in Siemens SIMATIC MV400)
  - The underlying TCP stack of the affected products does not correctly validate the sequence number for incoming TCP RST packages. An attacker could exploit this to terminate arbitrary TCP sessions.
- CVE-2020-27632: (Use of Insufficiently Random Values in Siemens SIMATIC MV400)
  - ISN generator is initialized with a constant value and has constant increments. An attacker could predict and hijack TCP sessions.
- CVE-2019-3823: (Out-of-bounds Read in libcurl)
  - The libcurl library versions 7.34.0 to and including 7.63.0 are vulnerable to a heap out-of-bounds

read in the code handling the end-of-response for SMTP. This vulnerability could allow an attacker to trigger a Denial-of-Service condition on the affected devices.

- CVE-2021-22713: (Buffer Overflow Vulnerability in Multiple Schneider PowerLogic ION series Power Meters)
  - A CWE-119: Improper restriction of operations within the bounds of a memory buffer vulnerability exists that could cause the meter to reboot.
- CVE-2021-22714: (Buffer Overflow Vulnerability in Siemens PowerLogic ION7400 / PM8000 / ION9000 Power Meters)
  - A CWE-119: Improper restriction of operations within the bounds of a memory buffer vulnerability exists that could cause the meter to reboot or allow for remote code execution.

20210305

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

- **Talos Rules 2021-03-02 (https://www.snort.org/advisories/talos-rules-2021-03-02)**
  - This release adds and modifies rules in several categories
    - Microsoft Vulnerability CVE-2021-26855: A coding deficiency exists in Microsoft Exchange Server 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 57241 through 57244.
    - Microsoft Vulnerability CVE-2021-26857: A coding deficiency exists in Microsoft Exchange Server 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 57233 through 57234.
    - Microsoft Vulnerability CVE-2021-26858: A coding deficiency exists in Microsoft Exchange Server 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 57245 through 57246.
    - Microsoft Vulnerability CVE-2021-27065: A coding deficiency exists in Microsoft Exchange Server 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 57245 through 57246.

- **Talos Rules 2021-03-03 (https://www.snort.org/advisories/talos-rules-2021-03-03)**
  - Talos has added and modified multiple rules in the file-image, file-office, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

This release also adds support for the detection of the following vulnerability:

- CVE-2020-14502: (Stored Cross Site Scripting in 1734-AENTR Series B and Series C)
  - The web interface of the 1734-AENTR Communications module is vulnerable to stored XSS. A remote,

unauthenticated attacker could store a malicious script within the web interface that, when executed, could modify some string values on the “Home” page of the web interface.

- CVE-2020-14504: (Unauthenticated HTTP POST Requests in 1734-AENTR Series B and Series C)
    - The web interface of the 1734-AENTR communication module mishandles authentication for HTTP POST requests. A remote, unauthenticated attacker can send a crafted request which may allow for modification of the configuration settings.
- CVE-2021-22681: (Insufficiently protected credentials in Logix controllers)
    - Studio 5000 Logix Designer uses a key to verify Logix controllers are communicating with the affected Rockwell Automation products. The product is vulnerable because an unauthenticated attacker could bypass this verification mechanism and authenticate with Logix controllers.
- CVE-2020-6998: (Improper Input Validation Causes Denial of Service Condition in CompactLogix 5370 and ControlLogix 5570 Controllers)
    - The connection establishment algorithm found in CompactLogix 5370 and ControlLogix 5570 does not sufficiently manage its control flow during execution, creating an infinite loop. This may allow an attacker to send specially crafted CIP packet requests to a controller, which may cause denial-of-service conditions in communications with other products.