Release Notes for Cisco Cyber Vision Knowledge DB

Release 202107

Compatible device list 2
Links 2
Software Download 2
Related Documentation 2
Database download 3
How to update the database 3
Release contents 4
20210730 4
20210723 4
20210716 4
20210709 6
20210702 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-center-3.2.4.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-3.2.4.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-3.2.4.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-3.2.4.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-3.2.4.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-3.2.4.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.2.4.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-3.2.4.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-3.2.4.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates/3/3.2.4	**Description**
CiscoCyberVision-sysupgrade-3.2.4.dat	System Upgrade file for Center and Sensors 3.1.x to 3.2.4
CiscoCyberVision-sysupgrade-sensor-3.2.4.dat	Cisco Cyber Vision System Upgrade file for IC3000 Sensors or other non IOx Sensors 3.x to 3.2.4
CiscoCyberVision-Embedded-KDB-3.2.4.dat	Knowledge DB embedded in Cisco Cyber Vision 3.2.4
Updates/KDB/KDB.202107	**Description**
CiscoCyberVision_knowledgedb_20210702.db	Knowledge DB version 20210702
CiscoCyberVision_knowledgedb_20210709.db	Knowledge DB version 20210709
CiscoCyberVision_knowledgedb_20210716.db	Knowledge DB version 20210716
CiscoCyberVision_knowledgedb_20210723.db	Knowledge DB version 20210723
CiscoCyberVision_knowledgedb_20210730.db	Knowledge DB version 20210730

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

20210730

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

- **Talos Rules 2021-07-29 (https://www.snort.org/advisories/talos-rules-2021-07-29)**
  - Talos has added and modified multiple rules in the browser-other and malware-cnc rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-07-26 (https://www.snort.org/advisories/talos-rules-2021-07-26)**
  - Today Talos is releasing coverage to detect exploitation attempts of NTLM Relay Attacks on Active Directory Certificate Services AKA SeriousSAM. Coverage is being released as SIDs 57965-57966. Talos has added and modified multiple rules in the exploit-kit, malware-cnc, os-other, os-windows, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20210723

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

- **Talos Rules 2021-07-22 (https://www.snort.org/advisories/talos-rules-2021-07-22)**
  - Talos has added and modified multiple rules in the browser-chrome, file-other, file-pdf, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-07-20 (https://www.snort.org/advisories/talos-rules-2021-07-20)**
  - Talos has added and modified multiple rules in the malware-backdoor, os-other, server-apache, server-other and sql rule sets to provide coverage for emerging threats from these technologies.

20210716

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

- **Talos Rules 2021-07-15 (https://www.snort.org/advisories/talos-rules-2021-07-15)**
  - Talos has added and modified multiple rules in the browser-ie and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-07-13 (https://www.snort.org/advisories/talos-rules-2021-07-13)**
  - Talos Microsoft Vulnerability CVE-2021-31979: A coding deficiency exists in Microsoft Windows Kernel that may lead to elevation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 57894 through 57895.
  - Microsoft Vulnerability CVE-2021-33771: A coding deficiency exists in Microsoft Windows Kernel that may lead to elevation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 57896 through 57897.

- Microsoft Vulnerability CVE-2021-34448: A coding deficiency exists in Microsoft Scripting Engine 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 42749 through 42750.
- Microsoft Vulnerability CVE-2021-34449: 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 57890 through 57891.
- Microsoft Vulnerability CVE-2021-34467: A coding deficiency exists in Microsoft SharePoint 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 57910.
- Microsoft Vulnerability CVE-2021-34473: 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 57906 through 57909.
- Microsoft Vulnerability CVE-2021-34527: A coding deficiency exists in Microsoft Windows Print Spooler 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 57876 through 57877.
- Talos also has added and modified multiple rules in the browser-ie, malware-cnc, os-other, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.

This release also adds support and modifications for the detection of the following vulnerabilities:

1. CVE-2021-25671: (Allocation of Resources Without Limits or Throttling in Siemens RWG Universal Controllers)
   Successful exploitation of this vulnerability could allow an attacker to cause a denial-of-service condition.
2. CVE-2021-22771: (Improper Neutralization of Formula Elements in a CSV File Vulnerability in Schneider Easergy T300)
   Information Exposure vulnerability exists that exposes sensitive information to an actor not explicitly authorized to have access to that information.
3. CVE-2015-8011: (Uncontrolled Resource Consumption in Siemens Industrial Products LLDP)
   Successful exploitation of these vulnerabilities could allow an attacker to cause a denial-of-service condition or execute arbitrary code.
4. CVE-2021-22770: (Information Exposure Vulnerability in Schneider Easergy T300)
   Information Exposure vulnerability exists that exposes sensitive information to an actor not explicitly authorized to have access to that information.
5. CVE-2020-27827: (Uncontrolled Resource Consumption in Siemens Industrial Products LLDP)
   Successful exploitation of these vulnerabilities could allow an attacker to cause a denial-of-service condition or execute arbitrary code.
6. CVE-2021-29998: (Heap-based Buffer Overflow in Siemens Wind River VxWorks-based Industrial Products)

Successful exploitation of this vulnerability could allow an attacker to cause a heap-based buffer overflow.

7. CVE-2020-28400: (Allocation of Resources Without Limits or Throttling in Siemens PROFINET Devices)
   Successful exploitation of this vulnerability could allow an attacker to perform a denial-of-service attack if a large amount of PROFINET Discovery and Configuration Protocol (DCP) reset packets is sent to the affected devices.
8. CVE-2021-31895: (Classic Buffer Overflow in Siemens RUGGEDCOM ROS)
   Successful exploitation of this vulnerability could allow an attacker with network access to an affected device to cause a remote code execution condition.
9. CVE-2021-22772: (Missing Authentication for Critical Function Vulnerability in Schneider Easergy T200)
   A Missing Authentication for Critical Function vulnerability exists that could cause unauthorized operation when authentication is bypassed.
10. CVE-2021-22779: (Authentication Bypass by Spoofing Vulnerability in Schneider Modicon Controllers M580 and M340)
    An Authentication Bypass by Spoofing vulnerability exists that could cause unauthorized access in read and write mode to the controller by spoofing the Modbus communication between the engineering software and the controller

20210709

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

- **Talos Rules 2021-07-08 (https://www.snort.org/advisories/talos-rules-2021-07-08)**
  - Talos has added and modified multiple rules in the os-other, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-07-06 (https://www.snort.org/advisories/talos-rules-2021-07-06)**
  - Talos has added and modified multiple rules in the indicator-compromise, malware-cnc, os-windows and server-other rule sets to provide coverage for emerging threats from these technologies.

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

1. CVE-2021-33012: (Improper Input Validation Vulnerability in Rockwell Automation MicroLogix 1100)
   A remote, unauthenticated attacker sending specially crafted commands could cause the PLC to fault when the controller is switched to RUN mode, which results in a denial-of-service condition. If successfully exploited, this vulnerability will cause the controller to fault when the controller is switched to RUN mode.

20210702

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

- **Talos Rules 2021-06-30 (https://www.snort.org/advisories/talos-rules-2021-06-30)**
  - Talos has added and modified multiple rules in the malware-other, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-06-29 (https://www.snort.org/advisories/talos-rules-2021-06-29)**
  - Talos has added and modified multiple rules in the browser-chrome, exploit-kit, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.