Release Notes for Cisco Cyber Vision Knowledge DB

Release 202208

Compatible device list

Center	Description
All version 4 centers	All Cisco Cyber Vision center version 4 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-4.1.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.1.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.1.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.1.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.1.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.1.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.1.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.1.0.dat	Knowledge DB embedded in Cisco Cyber Vision 4.1.0
Updates/KDB/KDB.202208	**Description**
CiscoCyberVision_knowledgedb_20220805.db	Knowledge DB version 20220805
CiscoCyberVision_knowledgedb_20220816.db	Knowledge DB version 20220816
CiscoCyberVision_knowledgedb_20220823.db	Knowledge DB version 20220823
CiscoCyberVision_knowledgedb_20220826.db	Knowledge DB version 20220826

Related Documentation

- Cisco Cyber Vision GUI User Guide:

  https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/GUI/b_Cisco_Cyber_Vision_GUI_User_Guide.html

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

20220826

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

- **Talos Rules 2022-08-25 (https://www.snort.org/advisories/talos-rules-2022-08-25)**
  - Talos has added and modified multiple rules in the browser-chrome, malware-cnc, malware-other, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-08-23 (https://www.snort.org/advisories/talos-rules-2022-08-23)**
  - Talos has added and modified multiple rules in the file-other, malware-cnc, malware-other, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20220823

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

- **Talos Rules 2022-08-18 (https://www.snort.org/advisories/talos-rules-2022-08-18)**
  - Talos has added and modified multiple rules in the malware-cnc, os-linux, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-08-16 (https://www.snort.org/advisories/talos-rules-2022-08-16)**
  - Talos has added and modified multiple rules in the browser-webkit, os-mobile 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 vulnerability:

- CVE-2022-33939: (Resource Management Errors in Yokogawa CENTUM Controller FCS
  - CENTUM VP / CS 3000 controller FCS (CP31, CP33, CP345, CP401, and CP451) contains an issue in processing communication packets, which may lead to resource consumption. If this vulnerability is exploited, an attacker may cause a denial of service (DoS) condition in ADL communication by sending a specially crafted packet to the affected product.

20220816

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

- **Talos Rules 2022-08-10 (https://www.snort.org/advisories/talos-rules-2022-08-10)**
  - Talos is withdrawing rule 60381 from the release due to FP concerns, a replacement signature will be released to cover CVE 2022-35748 in an upcoming release.

- Talos also has added and modified multiple rules in the browser-chrome, malware-cnc and os-windows rule sets to provide coverage for emerging threats from these technologies.

- **Talos Rules 2022-08-09 (https://www.snort.org/advisories/talos-rules-2022-08-09)**
  - Microsoft Vulnerability CVE-2022-34699: 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: Snort2: GID 1, SIDs 60379 through 60380. Snort3: GID 1, SID 300237.
  - Microsoft Vulnerability CVE-2022-34713: A coding deficiency exists in Microsoft Windows Support Diagnostic Tool (MSDT) that may lead to remote code execution.
    - A rule to detect attacks targeting this vulnerability is included in this release and is identified with: Snort2: GID 1, SID 60384. Snort3: GID 1, SID 60384.
  - Microsoft Vulnerability CVE-2022-35748: A coding deficiency exists in HTTP.sys that may lead to a Denial of Service (DoS).
    - A rule to detect attacks targeting this vulnerability is included in this release and is identified with: Snort2: GID 1, SID 60381. Snort3: GID 1, SID 60381.
  - Microsoft Vulnerability CVE-2022-35750: 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: Snort2: GID 1, SIDs 60382 through 60383. Snort3: GID 1, SID 300238.
  - Microsoft Vulnerability CVE-2022-35751: A coding deficiency exists in Microsoft Hyper-V that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 60386 through 60387. Snort3: GID 1, SID 300239.
  - Microsoft Vulnerability CVE-2022-35755: A coding deficiency exists in Microsoft Windows Print Spooler that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 60371 through 60372. Snort3: GID 1, SID 300233.
  - Microsoft Vulnerability CVE-2022-35756: A coding deficiency exists in Microsoft Windows Kerberos that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 60377 through 60378. Snort3: GID 1, SID 300236.
  - Microsoft Vulnerability CVE-2022-35761: 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: Snort2: GID 1, SIDs 60373 through 60374. Snort3: GID 1, SID 300234.

- Microsoft Vulnerability CVE-2022-35793: A coding deficiency exists in Microsoft Windows Print Spooler that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 60375 through 60376. Snort3: GID 1, SID 300235.
- Talos also has added and modified multiple rules in the browser-chrome, 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 vulnerability:

- CVE-2020-26147: (FragAttack Vulnerability on Hirschmann BAT devices)
  - An issue was discovered in the Linux kernel 5.8.9. The WEP, WPA, WPA2, and WPA3 implementations reassemble fragments even though some of them were sent in plaintext. This vulnerability can be abused to inject packets and/or exfiltrate selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used.
- CVE-2020-26146: (FragAttack Vulnerability on Hirschmann BAT devices)
  - An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WPA, WPA2, and WPA3 implementations reassemble fragments with non-consecutive packet numbers. An adversary can abuse this to exfiltrate selected fragments. This vulnerability is exploitable when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used. Note that WEP is vulnerable to this attack by design.
- CVE-2020-26145: (FragAttack Vulnerability on Hirschmann BAT devices)
  - An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WEP, WPA, WPA2, and WPA3 implementations accept second (or subsequent) broadcast fragments even when sent in plaintext and process them as full unfragmented frames. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.
- CVE-2020-26144: (FragAttack Vulnerability on Hirschmann BAT devices)
  - An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WEP, WPA, WPA2, and WPA3 implementations accept plaintext A-MSDU frames as long as the first 8 bytes correspond to a valid RFC1042 (i.e., LLC/SNAP) header for EAPOL. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.
- CVE-2020-26142: (FragAttack Vulnerability on Hirschmann BAT devices)
  - An issue was discovered in the kernel in OpenBSD 6.6. The WEP, WPA, WPA2, and WPA3 implementations treat fragmented frames as full frames. An adversary can abuse this to inject arbitrary network packets, independent of the network configuration.
- CVE-2020-24588 : (FragAttack Vulnerability on Hirschmann BAT devices)
  - The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that the A-MSDU flag in the plaintext QoS header field is authenticated. Against devices that support receiving non-SSP A-MSDU frames (which is mandatory

as part of 802.11n), an adversary can abuse this to inject arbitrary network packets.

- CVE-2020-24587 : (FragAttack Vulnerability on Hirschmann BAT devices)
  - The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that all fragments of a frame are encrypted under the same key. An adversary can abuse this to decrypt selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP encryption key is periodically renewed.
- CVE-2020-24586 : (FragAttack Vulnerability on Hirschmann BAT devices)
  - The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that received fragments be cleared from memory after (re)connecting to a network. Under the right circumstances, when another device sends fragmented frames encrypted using WEP, CCMP, or GCMP, this can be abused to inject arbitrary network packets and/or exfiltrate user data.
- CVE-2021-22786 : (Information Exposure Vulnerability in Schneider Modicon PAC Controllers)
  - A CWE-200: Information Exposure vulnerability exists that could cause the exposure of sensitive information stored on the memory of the controller when communicating over the Modbus TCP protocol.
- CVE-2022-37301: (Underflow Vulnerability in Schneider Modicon PAC Controllers)
  - A CWE-191: Integer Underflow (Wrap or Wraparound) vulnerability exists that could cause a denial of service of the controller due to memory access violations when using the Modbus TCP protocol
- CVE-2022-37300 : (Weak Password Recovery Mechanism in Schneider Modicon Controllers M580 and M340)
  - A CWE-640: Weak Password Recovery Mechanism for Forgotten Password vulnerability exists that could cause unauthorized access in read and write mode to the controller when communicating over Modbus.
- CVE-2022-36325: (Basic XSS Vulnerability in Siemens Scalance Products)
  - Affected devices do not properly sanitize data introduced by an user when rendering the web interface. This could allow an authenticated remote attacker with administrative privileges to inject code and lead to a DOM-based XSS.
- CVE-2022-36324: (Underflow Vulnerability in Schneider Modicon PAC Controllers)
  - Affected devices do not properly handle the renegotiation of SSL/TLS parameters. This could allow an unauthenticated remote attacker to bypass the TCP brute force prevention and lead to a denial of service condition for the duration of the attack.
- CVE-2022-36323: (Data Injection Vulnerability in Siemens Scalance Products)
  - Affected devices do not properly sanitize an input field. This could allow an authenticated remote attacker with administrative privileges to inject code or spawn a system root shell.

20220805

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

- **Talos Rules 2022-08-04 (https://www.snort.org/advisories/talos-rules-2022-08-04)**
  - Talos has added and modified multiple rules in the browser-chrome, os-mobile and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-08-02 (https://www.snort.org/advisories/talos-rules-2022-08-02)**
  - Talos has added and modified multiple rules in the malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.