Release Notes for Cisco Cyber Vision Knowledge DB

Release 202110

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-4.0.2.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.0.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.0.2.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.0.2.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.0.2.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.0.2.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.0.2.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.0.2.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.2.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates/4/4.0.2	**Description**
CiscoCyberVision-Embedded-KDB-4.0.2.dat	Knowledge DB embedded in Cisco Cyber Vision 4.0.2
Updates/KDB/KDB.202110	**Description**
CiscoCyberVision_knowledgedb_20211001.db	Knowledge DB version 20211001
CiscoCyberVision_knowledgedb_20211008.db	Knowledge DB version 20211008
CiscoCyberVision_knowledgedb_20211015.db	Knowledge DB version 20211015
CiscoCyberVision_knowledgedb_20211022.db	Knowledge DB version 20211022
CiscoCyberVision_knowledgedb_20211029.db	Knowledge DB version 20211029

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_4_0_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

20211029

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

- **Talos Rules 2021-10-28 (https://www.snort.org/advisories/talos-rules-2021-10-28)**
  - Talos has added and modified multiple rules in the file-multimedia, indicator-scan, malware-cnc, malware-other, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-10-26 (https://www.snort.org/advisories/talos-rules-2021-10-26)**
  - Talos has added and modified multiple rules in the malware-cnc, pua-adware and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-10-21 (https://www.snort.org/advisories/talos-rules-2021-10-21)**
  - Talos has added and modified multiple rules in the indicator-compromise, indicator-obfuscation, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20211022

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

- **Talos Rules 2021-10-19 (https://www.snort.org/advisories/talos-rules-2021-10-19)**
  - Talos has added and modified multiple rules in the file-office, file-pdf, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20211015

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

- **Talos Rules 2021-10-14 (https://www.snort.org/advisories/talos-rules-2021-10-14)**
  - Talos has added and modified multiple rules in the browser-chrome and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-10-12 (https://www.snort.org/advisories/talos-rules-2021-10-12)**
  - Microsoft Vulnerability CVE-2021-40443: 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 58303 through 58304.
  - Microsoft Vulnerability CVE-2021-40449: 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 58288 through 58289.
  - Microsoft Vulnerability CVE-2021-40450: 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 58310 through 58313.
- Microsoft Vulnerability CVE-2021-40466: 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 58308 through 58309.
- Microsoft Vulnerability CVE-2021-40467: 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 58305 through 58306.
- Microsoft Vulnerability CVE-2021-40470: A coding deficiency exists in DirectX Graphics Kernel 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 58294 through 58295.
- Microsoft Vulnerability CVE-2021-40487: A coding deficiency exists in Microsoft SharePoint 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 58314 through 58319.
- Microsoft Vulnerability CVE-2021-41357: 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 58286 through 58287.
- Talos also has added and modified multiple rules in the malware-other, os-windows, policy-other 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:

- CVE-2020-17438: (Out-of-bounds Write Vulnerability in embedded TCP/IP Stack (Amnesia:33))
  An issue was discovered in uIP 1.0, as used in Contiki 3.0 and other products. The code that reassembles fragmented packets fails to properly validate the total length of an incoming packet specified in its IP header, as well as the fragmentation offset value specified in the IP header. By crafting a packet with specific values of the IP header length and the fragmentation offset, attackers can write into the .bss section of the program (past the statically allocated buffer that is used for storing the fragmented data) and cause a denial of service in uip_reass() in uip.c, or possibly execute arbitrary code on some target architectures.
- CVE-2021-22806: (Incorrect Resource Transfer Between Spheres vulnerability in Shneider SpaceLYnk, Wiser For KNX and FellerLYnk)
  A CWE-669: Incorrect Resource Transfer Between Spheres vulnerability exists that could cause data exfiltration and unauthorized access when accessing a malicious website.
- CVE-2021-22800: (Improper Input Validation vulnerability in Schneider Modicon M218 Logic Controller)
  A CWE-20: Improper Input Validation vulnerability exists that could cause a Denial of Service when a crafted packet is sent to the controller over network port 1105/TCP.

- CVE-2021-41546: (Uncontrolled Resource Consumption Vulnerability in Siemens RUGGEDCOM ROX)
  Affected devices write crash-dumps without checking if enough space is available on the file system. Once the crash-dump fills the entire root file system, affected devices fail to boot. An attacker can leverage this vulnerability to cause a permanent denial-of-service condition.
- CVE-2021-37199: (Heap-based Buffer Overflow Vulnerability in Siemens SINUMERIK Controllers)
  Affected devices do not correctly process certain special crafted packets sent to Port 102/TCP, which could allow an attacker to cause a denial-of-service condition on the device.
- CVE-2021-37718: (Command Injection Vulnerability in Siemens SCALANCE)
  An authenticated command injection vulnerability exists in the ArubaOS web-based management user interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.
- CVE-2021-37716: (Classic Buffer Overflow Vulnerability in Siemens SCALANCE)
  There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP Port (8211) of devices running ArubaOS. This may allow for denial-of-service attacks and/or remote code execution in the underlying operating system.
- CVE-2021-37720: (Command Injection Vulnerability in Siemens SCALANCE)
  An authenticated command injection vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.
- CVE-2021-37724: (Command Injection Vulnerability in Siemens SCALANCE)
  An authenticated command injection vulnerability exists in the ArubaOS command line interface. This vulnerability is only present in instances of the Mobility Conductor. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the Mobility Conductor running ArubaOS.
- CVE-2020-37719: (OS Command Injection Vulnerability in Siemens SCALANCE)
  An authenticated command injection vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.
- CVE-2021-37717: (Command Injection Vulnerability in Siemens SCALANCE)
  An authenticated command injection vulnerability exists in the ArubaOS web-based management user interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.
- CVE-2021-37722: (Command Injection Vulnerability in Siemens SCALANCE)
  An authenticated command injection vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.
- CVE-2021-37731: (Missing Encryption of Sensitive Data Vulnerability in Siemens SCALANCE)
  An authenticated local path traversal vulnerability exists in the ArubaOS web-based management interface and CLI. This vulnerability only affects physical hardware controllers such as the 9000 series and 7x00

series. Successful exploitation of this vulnerability requires physical access to the controller and results in the ability to impact the integrity and confidentiality of critical files on the underlying operating system. This allows an attacker to impact the availability of the ArubaOS instance and may allow for modification or disclosure of sensitive data.

- CVE-2021-37723: (Command Injection Vulnerability in Siemens SCALANCE)
  An authenticated command injection vulnerability exists in the ArubaOS command line interface. This vulnerability is only present in instances of the Mobility Conductor. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the Mobility Conductor running ArubaOS.
- CVE-2019-5318: (Cross-site Request Forgery Vulnerability in Siemens SCALANCE)
  The web interface for RAPConsole lacks Anti-CSRF protections in place for state-changing operations. This can be exploited by an attacker to reboot the affected device if the attacker can convince a user to visit a specially crafted webpage.
- CVE-2021-37729: (Path Traversal Vulnerability in Siemens SCALANCE)
  An authenticated path traversal vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to impact the integrity of critical files on the underlying operating system. This allows an attacker to impact the availability of the ArubaOS instance and may allow for modification of sensitive data.
- CVE-2021-37721: (Command Injection Vulnerability in Siemens SCALANCE)
  An authenticated command injection vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.
- CVE-2021-37733: (Path Traversal Vulnerability in Siemens SCALANCE)
  An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files.
- CVE-2021-37725: (Cross-site Request Forgery Vulnerability in Siemens SCALANCE)
  A vulnerability in the web-based management interface of ArubaOS could allow an unauthenticated remote attacker to conduct a Cross-Site Request Forgery (CSRF) attack against a vulnerable system. Successful exploitation of this vulnerability would consist of an attacker persuading an authorized user to follow a malicious link, resulting in the deletion of arbitrary files with the privilege level of the targeted user.
- CVE-2021-37728: (Path Traversal Vulnerability in Siemens SCALANCE)
  An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to impact the integrity of critical files on the underlying operating system. This allows an attacker to impact the availability of the ArubaOS instance and may allow for modification of sensitive data.

20211008

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

- **Talos Rules 2021-10-07 (https://www.snort.org/advisories/talos-rules-2021-10-07)**
  - Talos is releasing SID 58276 (SID 300053 for Snort3) as coverage for CVE-2021-41773, an Apache HTTP

server directory traversal vulnerability which can lead to remote code execution.

- 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.

- **Talos Rules 2021-10-05 (https://www.snort.org/advisories/talos-rules-2021-10-05)**
  - Talos has added and modified multiple rules in the file-other, malware-other, malware-tools, protocol-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20211001

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

- **Talos Rules 2021-09-30 (https://www.snort.org/advisories/talos-rules-2021-09-30)**
  - Talos has added and modified multiple rules in the file-image, file-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-09-28 (https://www.snort.org/advisories/talos-rules-2021-09-28)**
  - Talos has added and modified multiple rules in the deleted, file-image, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.