Release Notes for Cisco Cyber Vision Knowledge DB

Release 202310

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-4.2.6.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.2.6.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.2.6.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.2.6.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.2.6.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.2.6.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.2.6.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.2.6.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.6.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.2.6.dat	Knowledge DB embedded in Cisco Cyber Vision 4.2.6
Updates/KDB/KDB.202310	**Description**
CiscoCyberVision_knowledgedb_20231006.db	Knowledge DB version 20231006
CiscoCyberVision_knowledgedb_20231013.db	Knowledge DB version 20231013
CiscoCyberVision_knowledgedb_20231020.db	Knowledge DB version 20231020
CiscoCyberVision_knowledgedb_20231027.db	Knowledge DB version 20231027

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

20231027

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

- **Talos Rules 2023-10-26 (https://www.snort.org/advisories/talos-rules-2023-10-26)**
- **Talos Rules 2023-10-24 (https://www.snort.org/advisories/talos-rules-2023-10-24)**

The new and updated Snort rules span the following categories:

- 1 file-image rules with SID 300740
- 1 file-pdf rules with SID 300738
- 1 malware-backdoor rules with SID 300731
- 1 malware-cnc rules with SID 47621
- 7 malware-other rules with SIDs 300739, 300733, 300737, 300736, 300734, 300732, 300735
- 1 os-windows rules with SID 62554
- 1 server-apache rules with SID 62574
- 10 server-webapp rules with SIDs 62571, 62544, 62570, 62550, 62555, 62547, 62551, 62546, 62543, 62545

20231020

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

- **Talos Rules 2023-10-17 (https://www.snort.org/advisories/talos-rules-2023-10-17-10-18-2023)**
- **Talos Rules 2023-10-17 (https://www.snort.org/advisories/talos-rules-2023-10-17)**
- **Talos Rules 2023-10-14 (https://www.snort.org/advisories/talos-rules-2023-10-14)**

The new and updated Snort rules span the following categories:

- 2 browser-chrome rules with SIDs 300728, 300729
- 1 browser-other rules with SIDs 62526
- 1 file-office rules with SIDs 300730
- 1 malware-tools rules with SIDs 300727
- 2 server-other rules with SIDs 62530, 62531
- 4 server-webapp rules with SIDs 62533, 62013, 62534, 62532

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

- CVE-2023-20198: (Cisco IOS XE Software Web UI Privilege Escalation Vulnerability)

- Cisco is aware of active exploitation of a previously unknown vulnerability in the web UI feature of Cisco IOS XE Software when exposed to the internet or to untrusted networks. This vulnerability allows a remote, unauthenticated attacker to create an account on an affected system with privilege level 15 access. The attacker can then use that account to gain control of the affected system. For steps to close the attack vector for this vulnerability, see the Recommendations section of this advisory Cisco will provide updates on the status of this investigation and when a software patch is available.

20231013

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

- **Talos Rules 2023-10-11 (https://www.snort.org/advisories/talos-rules-2023-10-11)**
- **Talos Rules 2023-10-10 (https://www.snort.org/advisories/talos-rules-2023-10-10)**

The new and updated Snort rules span the following categories:

- 1 browser-webkit rule with SID 300723
- 1 malware-cnc rule with SID 62514
- 6 os-windows rules with SIDs 300722, 300720, 300726, 300719, 300725, 300721
- 4 policy-other rules with SIDs 62501, 62497, 300724, 62500
- 1 protocol-other rule with SID 62519
- 4 server-other rules with SIDs 62518, 62517, 62515, 62516
- 9 server-webapp rules with SIDs 62506, 62496, 62507, 62512, 62513, 62522, 62520, 62523, 62521

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

- CVE-2023-22779: (Classic Buffer Overflow Vulnerability in Siemens SCALANCE W1750D)
    - There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.
- CVE-2023-22785: (Classic Buffer Overflow Vulnerability in Siemens SCALANCE W1750D)
    - There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.
- CVE-2023-22780: (Classic Buffer Overflow Vulnerability in Siemens SCALANCE W1750D)

  - There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.

- CVE-2023-22788: (Command Injection Vulnerability in Siemens SCALANCE W1750D)
  - Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.
- CVE-2023-22784: (Classic Buffer Overflow Vulnerability in Siemens SCALANCE W1750D)
  - There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.
- CVE-2023-37195: (Uncontrolled Resource Consumption Vulnerability in Siemens SIMATIC CP Devices)
  - Affected devices insufficiently control continuous mapping of direct memory access (DMA) requests. This could allow local attackers with administrative privileges to cause a denial of service situation on the host. A physical power cycle is required to get the system working again.
- CVE-2023-22787: (Improper Input Validation Vulnerability in Siemens SCALANCE W1750D)
  - An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point.
- CVE-2023-22789: (Command Injection Vulnerability in Siemens SCALANCE W1750D)
  - Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.
- CVE-2023-42796: (Path Traversal Vulnerability in Web Server of Siemens SICAM A8000 Devices)
  - The web server of affected devices fails to properly sanitize user input for the /sicweb-ajax/tmproot/ endpoint. This could allow an authenticated remote attacker to traverse directories on the system and download arbitrary files. By exploring active session IDs, the vulnerability could potentially be leveraged to escalate privileges to the administrator role.
- CVE-2023-22782: (Classic Buffer Overflow Vulnerability in Siemens SCALANCE W1750D)
  - There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.

- CVE-2023-22783: (Classic Buffer Overflow Vulnerability in Siemens SCALANCE W1750D)
    - There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.
- CVE-2023-22781: (Classic Buffer Overflow Vulnerability in Siemens SCALANCE W1750D)
    - There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.
- CVE-2023-37194: (Improper Access Control Vulnerability in Siemens SIMATIC CP Devices)
    - The kernel memory of affected devices is exposed to user-mode via direct memory access (DMA) which could allow a local attacker with administrative privileges to execute arbitrary code on the host system without any restrictions.
- CVE-2023-22791: (Command Injection Vulnerability in Siemens SCALANCE W1750D)
    - A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge-case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive information can occur are complex and depend on factors that are beyond the control of the attacker.
- CVE-2023-22790: (Command Injection Vulnerability in Siemens SCALANCE W1750D)
    - Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.
- CVE-2023-22786: (Classic Buffer Overflow Vulnerability in Siemens SCALANCE W1750D)
    - There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.

20231006

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

- **Talos Rules 2023-10-05 (https://www.snort.org/advisories/talos-rules-2023-10-05)**
- **Talos Rules 2023-10-03 (https://www.snort.org/advisories/talos-rules-2023-10-03)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 300718
- 2 browser-ie rules with SIDs 40661, 40662
- 1 file-image rule with SID 300717
- 2 malware-cnc rules with SIDs 62086, 62084
- 1 server-mail rule with SID 62480
- 2 server-webapp rules with SIDs 62483, 62484