Release Notes for Cisco Cyber Vision Knowledge DB

Release 202105

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-3.2.3.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-3.2.3.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-3.2.3.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-3.2.3.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-3.2.3.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-3.2.3.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.2.3.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-3.2.3.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-3.2.3.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates/3/3.2.3	**Description**
CiscoCyberVision-sysupgrade-3.2.3.dat	System Upgrade file for Center and Sensors 3.1.x to 3.2.3
CiscoCyberVision-sysupgrade-sensor-3.2.3.dat	Cisco Cyber Vision System Upgrade file for IC3000 Sensors or other non IOx Sensors 3.x to 3.2.2
CiscoCyberVision-Embedded-KDB-3.2.3.dat	Knowledge DB embedded in Cisco Cyber Vision 3.2.3
Updates/KDB/KDB.202105	**Description**
CiscoCyberVision_knowledgedb_20210507.db	Knowledge DB version 20210507
CiscoCyberVision_knowledgedb_20210517.db	Knowledge DB version 20210517
CiscoCyberVision_knowledgedb_20210521.db	Knowledge DB version 20210521
CiscoCyberVision_knowledgedb_20210528.db	Knowledge DB version 20210528

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

20210528

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

- **Talos Rules 2021-05-27 (https://www.snort.org/advisories/talos-rules-2021-05-27)**
  - Talos has added and modified multiple rules in the file-multimedia, file-pdf, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-05-25 (https://www.snort.org/advisories/talos-rules-2021-05-25)**
  - Talos has added and modified multiple rules in the browser-firefox, browser-ie, file-flash, file-image, file-multimedia, indicator-shellcode, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20210521

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

- **Talos Rules 2021-05-20 (https://www.snort.org/advisories/talos-rules-2021-05-20-5-20-2021)**
  - Talos has added a new rule in the os-windows rule set to provide coverage for CVE-2021-31166, a remote code execution vulnerability on Windows IIS web servers.
- **Talos Rules 2021-05-20 (https://www.snort.org/advisories/talos-rules-2021-05-20)**
  - Talos has added and modified multiple rules in the file-other, protocol-dns, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-05-18 (https://www.snort.org/advisories/talos-rules-2021-05-18)**
  - Talos has added and modified multiple rules in the browser-ie, file-java, file-other, malware-cnc, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20210517

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

- **Talos Rules 2021-05-13 (https://www.snort.org/advisories/talos-rules-2021-05-13)**
  - Talos has added and modified multiple rules in the file-pdf, malware-cnc, os-other, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-05-11 (https://www.snort.org/advisories/talos-rules-2021-05-11)**
  - Microsoft Vulnerability CVE-2021-26419: A coding deficiency exists in Microsoft Scripting Engine 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 57542 through 57543.
  - Microsoft Vulnerability CVE-2021-31166: A coding deficiency exists in HTTP Protocol Stack 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 57549 through 57550.

- Microsoft Vulnerability CVE-2021-31170: 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 57539 through 57540.
- Microsoft Vulnerability CVE-2021-31181: A coding deficiency exists in Microsoft SharePoint 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 57548.
- Microsoft Vulnerability CVE-2021-31188: 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 57544 through 57545.
- Talos also has added and modified multiple rules in the browser-ie, file-image, file-other, malware-backdoor, 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:

- CVE-2021-25155: (Improper Input Validation in Aruba Instant Access Point)
  - A remote arbitrary file modification vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2021-27383: (Improper Restriction of Operations within the Bounds of a Memory Buffer in SmartVNC)
  - SmartVNC has a heap allocation leak vulnerability in the server Tight encoder, which could result in a Denial-of-Service condition.
- CVE-2021-22740: (Information Exposure vulnerability in homeLYnk (Wiser For KNX) and spaceLYnk)
  - A CWE-200: Information Exposure vulnerability exists that could cause information to be exposed when an unauthorized file is uploaded.
- CVE-2021-22736: (Path Traversal vulnerability in homeLYnk (Wiser For KNX) and spaceLYnk)
  - A CWE-22: Improper Limitation of a Path name to a Restricted Directory ('Path Traversal') vulnerability exists that could cause a denial of service when an unauthorized file is uploaded.
- CVE-2021-25148: (Improper Input Validation in Aruba Instant Access Point)
  - A remote buffer overflow vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2021-27384: (Access of Memory Location After End of Buffer in SmartVNC)
  - SmartVNC has an out-of-bounds memory access vulnerability in the device layout handler, represented by a binary data stream on client side, which can potentially result in code execution
- CVE-2019-19276: (Out-of-bounds Write in Siemens SNMP Implementation of WinCC Runtime)
  - Specially crafted packets sent to port 161/udp can cause the SNMP service of affected devices tocrash. A manual restart of the device is required to resume operation of the service.
- CVE-2020-24635: (Command Injection in Aruba Instant Access Point)

- A remote buffer overflow vulnerability was discovered in some Aruba Instant Access Point (IAP).

- CVE-2021-22731: (Weak Password Recovery Mechanism for Forgotten Password vulnerability)
  - A CWE-640: Weak Password Recovery Mechanism for Forgotten Password vulnerability exists that could cause an unauthorized password change through HTTP/HTTPS when basic user information is known by a remote attacker.
- CVE-2020-6081: (Code execution vulnerability in CODESYS Runtime)
  - An exploitable code execution vulnerability exists in the PLC_Task functionality of 3S-Smart Software Solutions GmbH CODESYS Runtime 3.5.14.30. A specially crafted network request can cause remote code execution. An attacker can send a malicious packet to trigger this vulnerability.
- CVE-2020-10245: (Buffer Overflow in CODESYS V3 web server)
  - CODESYS V3 web server before 3.5.15.40, as used in CODESYS Control runtime systems, has a buffer overflow.
- CVE-2021-25160: (Improper Input Validation in Aruba Instant Access Point)
  - A remote arbitrary file modification vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2020-28393: (Denial-of-Service Vulnerability in OSPF Packet Handling of XR-500 and SCALANCE XM-400)
  - The OSPF protocol implementation in affected devices incorrectly handles the number of LSA fields in combination with other modified fields. An unauthenticated remote attacker could create a permanent denial-of-service condition by sending specially crafted OSPF packets. Successful exploitation requires OSPF to be enabled on an affected device.
- CVE-2020-0591: (Improper buffer restrictions in BIOS firmware for some Intel(R) Processors)
  - Improper buffer restrictions in BIOS firmware for some Intel(R) Processors may allow a privileged userto potentially enable escalation of privilege via local access.
- CVE-2021-25150: (Command Injection in Aruba Instant Access Point)
  - A remote execution of arbitrary commands vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2021-25662: (Improper Handling of Exceptional Conditions in SmartVNC)
  - SmartVNC client fails to handle an exception properly if the program execution process is modified after sending a packet from the server, which could result in a Denial-of-Service condition.
- CVE-2021-25144: (Buffer Overflow in Aruba Instant Access Point)
  - A remote buffer overflow vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2021-25156: (Improper Input Validation in Aruba Instant Access Point)
  - A remote arbitrary directory create vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2021-27385: (Uncontrolled Resource Consumption in SmartVNC)
  - A remote attacker could send specially crafted packets to SmartVNC device layout handler on client side, which could influence the amount of resources consumed and result in a Denial-of-Service (infinite loop) condition.

- CVE-2021-22732: (Improper Privilege Management vulnerability in homeLYnk (Wiser For KNX) and spaceLYnk)
  - A CWE-269: Improper Privilege Management vulnerability exists that could cause a code execution issue when an attacker loads unauthorized code on the web server.
- CVE-2021-25157: (Improper Input Validation in Aruba Instant Access Point)
  - A remote arbitrary file read vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2021-25161: (Cross-site Scripting in Aruba Instant Access Point)
  - A remote cross-site scripting (xss) vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2021-22734: (Improper Verification of Cryptographic Signature in homeLYnk (Wiser For KNX) and spaceLYnk)
  - A CWE-347: Improper Verification of Cryptographic Signature vulnerability exists that could cause remote code execution when an attacker loads unauthorized code.
- CVE-2021-22738: (Use of a Broken or Risky Cryptographic Algorithm in homeLYnk (Wiser For KNX) and spaceLYnk)
  - A CWE-327: Use of a Broken or Risky Cryptographic Algorithm vulnerability exists that could cause unauthorized access when credentials are discovered after a brute force attack.
- CVE-2021-25158: (Race Condition in Aruba Instant Access Point)
  - A remote arbitrary file read vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2019-5317: (Improper Authentication in Aruba Instant Access Point)
  - A local authentication bypass vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2021-25661: (Access of Memory Location After End of Buffer in SmartVNC)
  - SmartVNC has an out-of-bounds memory access vulnerability that could be triggered on the serverside when sending data from the client, which could result in a Denial-of-Service condition.
- CVE-2020-25705: (SAD DNS Attack in Linux Based Products)
  - A flaw in ICMP packets in the Linux kernel was found to allow to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypass source port UDP randomization. Software that relies on UDP source port randomization are indirectly affected as well. Kernel versions before 5.10 may be vulnerable to this issue.
- CVE-2021-22699: (Improper Input Validation vulnerability in Modicon M241 & M251 Logic Controllers)
  - A CWE-20: Improper Input Validation vulnerability exists that could cause denial of service when specific crafted requests are sent to the controller over HTTP.
- CVE-2011-4859: (Use of Hard-coded Credentials vulnerability in Schneider M340,premium and quantum controllers)
  - A CWE-798: Use of Hard-coded Credentials vulnerability exists in the Operating System that could cause access by an unauthorized user to the controller when FTP protocol is enabled.
- CVE-2021-22733: (Improper Privilege Management vulnerability in homeLYnk (Wiser For KNX) and spaceLYnk)
  - A CWE-269: Improper Privilege Management vulnerability exists that could cause shell access when unauthorized code is loaded into the system folder.

- CVE-2021-25162: (Command Injection in Aruba Instant Access Point)
  - A remote execution of arbitrary commands vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2020-25242: (Uncontrolled Resource Consumption in Siemens SIMATIC CP343-1 devices)
  - Specially crafted packets sent to TCP port 102 could cause a Denial-of-Service condition on the affected devices. A cold restart might be necessary in order to recover.
- CVE-2019-13538: (Cross-site Scripting vulnerability in CODESYS V3 Library Manager)
  - 3S-Smart Software Solutions GmbH CODESYS V3 Library Manager, all versions prior to 3.5.16.0, allows the system to display active library content without checking its validity, which may allow the contents of manipulated libraries to be displayed or executed.
- CVE-2021-22737: (Insufficiently Protected Credentials vulnerability in homeLYnk (Wiser For KNX) and spaceLYnk)
  - A CWE-522: Insufficiently Protected Credentials vulnerability exists that could cause unauthorized access of when credentials are discovered after a brute force attack.
- CVE-2019-9009: (Improper Input Validation in CODESYS)
  - An issue was discovered in 3S-Smart CODESYS before 3.5.15.0 . Crafted network packets cause the Control Runtime to crash.
- CVE-2021-22739: (Information Exposure vulnerability in homeLYnk (Wiser For KNX) and spaceLYnk)
  - A CWE-200: Information Exposure vulnerability exists that could cause a device to be compromised when it is first configured.
- CVE-2021-25149: (Buffer Overflow in Aruba Instant Access Point)
  - A remote buffer overflow vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2021-25159: (Improper Input Validation in Aruba Instant Access Point)
  - A remote arbitrary file modification vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2019-5319: (Buffer Overflow in Aruba Instant Access Point)
  - A remote buffer overflow vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2021-22735: (Improper Verification of Cryptographic Signature in homeLYnk (Wiser For KNX) and spaceLYnk)
  - A CWE-347: Improper Verification of Cryptographic Signature vulnerability exists that could allow remote code execution when unauthorized code is copied to the device.
- CVE-2020-8744: (Improper initialization in subsystem for Intel(R) CSME)
  - Improper initialization in subsystem for Intel(R) CSME versions before 12.0.70, 13.0.40, 13.30.10,14.0.45 and 14.5.25, Intel(R) TXE versions before 4.0.30 Intel(R) SPS versions before E3_05.01.04.200 may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2021-25145: (Improper Input Validation in Aruba Instant Access Point)
  - A remote unauthorized disclosure of information vulnerability was discovered in some Aruba Instant Access Point (IAP).

- CVE-2021-25143: (Improper Input Validation in Aruba Instant Access Point)
  - A remote Denial of Service (DoS) vulnerability was discovered in some Aruba Instant Access Point(IAP).
- CVE-2020-7052: (Uncontrolled Resource Consumption in CODESYS)
  - CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition.
- CVE-2019-9008: (Incorrect Permission Assignment for Critical Resource in CODESYS)
  - An issue was discovered in 3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime.
- CVE-2021-25146: (Command Injection in Aruba Instant Access Point)
  - A remote arbitrary file modification vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2020-24636: (Command Injection in Aruba Instant Access Point)
  - A remote buffer overflow vulnerability was discovered in some Aruba Instant Access Point (IAP).
- CVE-2021-27386: (Improper Restriction of Operations within the Bounds of a Memory Buffer in SmartVNC)
  - SmartVNC has a heap allocation leak vulnerability in the device layout handler on client side, which could result in a Denial-of-Service condition.

20210507

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

- **Talos Rules 2021-05-06 (https://www.snort.org/advisories/talos-rules-2021-05-06)**
  - Talos has added and modified multiple rules in the file-java, os-windows, policy-other, server-apache, server-iis and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-05-04 (https://www.snort.org/advisories/talos-rules-2021-05-04)**
  - Talos has added and modified multiple rules in the browser-ie, browser-other, file-flash, file-image, file-java, file-other, file-pdf, indicator-compromise, os-windows, policy-other, server-mail, server-mysql, server-oracle and server-webapp rule sets to provide coverage for emerging threats from these technologies.