Release Notes for Cisco Cyber Vision Knowledge DB

Release 202108

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-4.0.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.0.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.0.0..ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.0.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.0.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.0.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.0.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.0.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates/4/4.0.0	**Description**
CiscoCyberVision-Embedded-KDB-4.0.0.dat	Knowledge DB embedded in Cisco Cyber Vision 4.0.0
Updates/KDB/KDB.202108	**Description**
CiscoCyberVision_knowledgedb_20210827.db	Knowledge DB version 20210827

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

20210827

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

- **Talos Rules 2021-08-26 (https://www.snort.org/advisories/talos-rules-2021-08-26)**
  - Talos has added and modified multiple rules in the malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-08-24 (https://www.snort.org/advisories/talos-rules-2021-08-24)**
  - Talos has added and modified multiple rules in the file-image, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20210820

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

- **Talos Rules 2021-08-19 (https://www.snort.org/advisories/talos-rules-2021-08-19)**
  - Talos has added and modified multiple rules in the malware-cnc, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-08-17 (https://www.snort.org/advisories/talos-rules-2021-08-17)**
  - Talos has added and modified multiple rules in the 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 vulnerabilities:

1. CVE-2021-22704: (Improper Limitation of a Pathname to a Restricted Directory in Harmony/Magelis HMI)
   A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists that could cause a Denial of Service or unauthorized access to system information when connecting to the Harmony HMI over FTP.
2. CVE-2021-22792: (NULL Pointer Dereference in Modicon controllers)
   A CWE-476: NULL Pointer Dereference vulnerability exists that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file.
3. CVE-2021-22789: (Improper Restriction of Operations within the Bounds of a Memory Buffer in Modicon controllers)
   A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file.
4. CVE-2021-22790: (Out-of-bounds Read Modicon controllers)
   A CWE-125: Out-of-bounds Read vulnerability exists that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file.
5. CVE-2021-22791: (Out-of-bounds Write in Modicon controllers)
   A CWE-787: Out-of-bounds Write vulnerability exists that could cause a Denial of Service on the Modicon

PLC controller / simulator when updating the controller application with a specially crafted project file.

6. CVE-2021-22793: (Exposure of Sensitive Information to an Unauthorized Actor in Modicon controllers)
   A CWE-200: exposure of Sensitive Information to an Unauthorized Actor vulnerability exists that could allow an authenticated attacker to access the device via FTP protocol.
7. CVE-2021-30188: (Stack-based buffer overflow in Pacdrive M (CODESYS V2))
   A crafted request may cause a stack-based buffer overflow in the affected CODESYS products, resulting in a denial-of-service condition or being utilized for remote code execution.
8. CVE-2021-30186: (Heap-based buffer overflow in Pacdrive M (CODESYS V2))
   A crafted request may cause a heap-based buffer overflow in the affected CODESYS products, resulting in a denial-of-service condition.
9. CVE-2021-30195: (Buffer over-read in Pacdrive M (CODESYS V2))
   A crafted request may cause a buffer over-read in the affected CODESYS products, resulting in a denial-of service condition.
10. CVE-2021-37172: (Improper Authentification in Siemens S7-1200 CPU family)

    Affected devices fail to authenticate against configured passwords when provisioned using TIA Portal v13. This could allow an attacker using TIA Portal v17 or later versions to bypass authentication and download arbitrary programs to the PLC. The vulnerability does not occur when TIA Portal v13 SP1 or later version was used to provision the device.
11. CVE-2020-24486: (Missing Encryption of Sensitive Data Vulnerability in Siemens SIMATIC and SINUMERIK)

    Improper input validation in the firmware for some Intel processors may allow an authenticated user to potentially enable a denial of service via local access.
12. CVE-2020-9273: (Use After Free Vulnerability in Siemens SIMATIC)
    A malicious attacker could corrupt the memory pool by interrupting the data transfer channel. This triggers a use-after-free condition in alloc_pool in pool.c, which could lead to remote code execution.
13. CVE-2020-9272: (Out-of-Bounds Read Vulnerability in Siemens SIMATIC)
    The affected products are vulnerable to an out-of-bounds read vulnerability in mod_cap via the cap_text.ccap_to_text function, which could lead to information disclosure.
14. CVE-2020-24513: (Missing Encryption of Sensitive Data Vulnerability in Siemens SIMATIC and SINUMERIK)
    A domain-bypass transient execution vulnerability in some Intel Atom processors may allow an authenticated user to enable information disclosure via local access.
15. CVE-2020-24512: (Missing Encryption of Sensitive Data Vulnerability in Siemens SIMATIC and SINUMERIK)
    An observable timing discrepancy in some Intel processors may allow an authenticated user to enable information disclosure via local access.
16. CVE-2020-24511: (Missing Encryption of Sensitive Data Vulnerability in Siemens SIMATIC and SINUMERIK)
    Improper isolation of shared resources in some Intel processors may allow an authenticated user to enable information disclosure via local access.
17. CVE-2020-24507: (Missing Encryption of Sensitive Data Vulnerability in Siemens SIMATIC and SINUMERIK)
    Improper initialization in a subsystem in the Intel CSME versions prior 11.8.86, 11.12.86, 11.22.86, 12.0.81, 13.0.47, 13.30.17, 14.1.53, 14.5.32, 13.50.11, and 15.0.22 may allow a privileged user to enable information disclosure via local access.
18. CVE-2020-24506: (Missing Encryption of Sensitive Data Vulnerability in Siemens SIMATIC and SINUMERIK)
    Out-of-bounds read in a subsystem in the Intel CSME versions prior to 12.0.81, 13.0.47, 13.30.17, 14.1.53, and 14.5.32 may allow a privileged user to enable information disclosure via local access.
19. CVE-2020-12360: (Missing Encryption of Sensitive Data Vulnerability in Siemens SIMATIC and SINUMERIK)

An out-of-bounds read in the firmware for some Intel processors may allow an authenticated user to enable an escalation of privilege via local access.

20. CVE-2020-12358: (Missing Encryption of Sensitive Data Vulnerability in Siemens SIMATIC and SINUMERIK)
    An out-of-bounds write in the firmware for some Intel processors may allow a privileged user to cause a denial-of-service condition via local access.
21. CVE-2020-12357: (Missing Encryption of Sensitive Data Vulnerability in Siemens SIMATIC and SINUMERIK)
    Improper initialization in the firmware for some Intel processors may allow a privileged user to enable escalation of privilege via local access.
22. CVE-2020-8704: (Missing Encryption of Sensitive Data Vulnerability in Siemens SIMATIC and SINUMERIK)
    A race condition in a subsystem in the Intel LMS versions prior to 2039.1.0.0 may allow a privileged user to enable escalation of privilege via local access.
23. CVE-2020-8703: (Missing Encryption of Sensitive Data Vulnerability in Siemens SIMATIC and SINUMERIK)
    Improper buffer restrictions in a subsystem in the Intel CSME versions prior to 11.8.86, 11.12.86, 11.22.86, 12.0.81, 13.0.47, 13.30.17, 14.1.53, 14.5.32, and 15.0.22 may allow a privileged user to enable escalation of privilege via local access.
24. CVE-2020-8670: (Missing Encryption of Sensitive Data Vulnerability in Siemens SIMATIC and SINUMERIK)

    A race condition in the firmware for some Intel processors may allow a privileged user to enable escalation of privilege via local access.

20210813

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

- **Talos Rules 2021-08-12 (https://www.snort.org/advisories/talos-rules-2021-08-12)**
  - 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 2021-08-10 (https://www.snort.org/advisories/talos-rules-2021-08-10)**
  - Microsoft Vulnerability CVE-2021-26432: A coding deficiency exists in Microsoft Windows Services for NFS ONCRPC XDR Driver 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 58003.
  - Microsoft Vulnerability CVE-2021-34480: 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 57998 through 57999.
  - Microsoft Vulnerability CVE-2021-34535: A coding deficiency exists in Remote Desktop Client 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 57997.
  - Talos has added and modified multiple rules in the browser-chrome, browser-ie, malware-cnc, malware-other, os-linux and server-other rule sets to provide coverage for emerging threats from these technologies.

- **Talos Rules 2021-08-06 (https://www.snort.org/advisories/talos-rules-2021-08-06)**
  - Talos is releasing new and updated coverage for a Microsoft Exchange vulnerability patched in July 2021, CVE-2021-34473. This vulnerability is a pre-authentication ACL bypass vulnerability, and the updates provided in this latest SRU offer additional protection against exploitation based on new information shared at and after Black Hat USA 2021.
  - The covering SIDs are: 57906-57909 and 57983. Talos has added and modified multiple rules in the server-webapp rule sets to provide coverage for emerging threats from these technologies.

20210806

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

- **Talos Rules 2021-08-05 (https://www.snort.org/advisories/talos-rules-2021-08-05)**
  - Talos has added and modified multiple rules in the and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-08-03 (https://www.snort.org/advisories/talos-rules-2021-08-03)**
  - Talos has added and modified multiple rules in the file-other and server-other rule sets to provide coverage for emerging threats from these technologies.
- **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.

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

1. CVE-2021-34570: (Denial of service attack using special crafted JSON request)
   A device on the same network as the controller sending a special crafted JSON request to the /auth/access-token endpoint may cause the controller to restart (CWE-20).
2. CVE-2020-35684: ([NicheLite] Integer overflow Vulnerability in Multiple Vendors Hardware)
   The code that parses TCP packets relies on an unchecked value of the IP payload size (extracted from the IP header) to compute the length of the TCP payload within the TCP checksum computation function. When the IP payload size is set to be smaller than the size of the IP header, the TCP checksum computation function may read out of bounds. A low-impact write-out-of-bounds is also possible.
3. CVE-2020-25928: ([NicheLite] Out-of-bounds read/write Vulnerability in Multiple Vendors Hardware)
   The routine for parsing DNS responses does not check the “response data length” field of individual DNS answers, which may cause OOB-R/W.
4. CVE-2020-25926: ([NicheLite] DNS cache poisoning weakness Vulnerability in Multiple Vendors Hardware)
   The DNS client does not set sufficiently random transaction IDs.

5. CVE-2021-31400: ([NicheLite] Loop with Unreachable Exit Condition Vulnerability in Multiple Vendors Hardware)
   The TCP out of band urgent data processing function would invoke a panic function if the pointer to the end of the out of band urgent data points out of the TCP segment's data. If the panic function hadn't a trap invocation removed it will result in an infite loop and therefore a DoS (continuous loop or a device reset).
6. CVE-2020-25767: ([NicheLite] Out-of-bounds read Vulnerability in Multiple Vendors Hardware)
   The routine for parsing DNS domain names does not check whether a compression pointer points within the bounds of a packet, which leads to OOB-R.
7. CVE-2020-35683: ([NicheLite] Integer overflow Vulnerability in Multiple Vendors Hardware)
   The code that parses ICMP packets relies on an unchecked value of the IP payload size (extracted from the IP header) to compute the ICMP checksum. When the IP payload size is set to be smaller than the size of the IP header, the ICMP checksum computation function may read out of bounds.
8. CVE-2021-31401: ([NicheLite] Integer overflow Vulnerability in Multiple Vendors Hardware)
   The TCP header processing code doesn't sanitize the length of the IP length (header + data). With a crafted IP packet an integer overflow would occur whenever the length of the IP data is calculated by subtracting the length of the header from the length of the total IP packet.
9. CVE-2021-31228: ([NicheLite] DNS cache poisoning weakness Vulnerability in Multiple Vendors Hardware)
   Attackers can predict the source port of DNS queries to send forged DNS response packets that will be accepted as valid answers to the DNS client's request.
10. CVE-2020-25927: ([NicheLite] Out-of-bounds read Vulnerability in Multiple Vendors Hardware)
    The routine for parsing DNS responses does not check whether the number of queries/responses specified in the packet header corresponds to the query/response data available in the DNS packet, leading to OOB-R.
11. CVE-2020-35685: ([NicheLite] Predictable ISNs Vulnerability in Multiple Vendors Hardware)
    TCP ISNs are generated in a predictable manner.
12. CVE-2021-31227: ([NicheLite] HTTP heap overflow Vulnerability in Multiple Vendors Hardware)
    A heap buffer overflow exists in the code that parses the HTTP POST request due to an incorrect signed integer comparison.
13. CVE-2021-27565: ([NicheLite] Unnecessary panic triggered Vulnerability in Multiple Vendors Hardware)
    Whenever an unknown HTTP request is received, a panic is invoked.
14. CVE-2021-36762: ([NicheLite] Read out of bounds Vulnerability in Multiple Vendors Hardware)
    The TFTP packet processing function doesn't ensure that a filename is null-terminated, therefore a subsequent call to strlen() upon the file name might read out of bounds of the protocol packet buffer.
15. CVE-2021-31226: ([NicheLite] HTTP heap overflow Vulnerability in Multiple Vendors Hardware)
    A heap buffer overflow exists in the code that parses the HTTP POST request due to lack of size validation.