Release Notes for Cisco Cyber Vision Knowledge DB

Release 202010

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-3.1.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-3.1.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-sensor-management-3.1.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-3.1.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-3.1.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.1.0.tar	Cisco Catalyst 9300 installation and update file
Updates/3/3.1.0	**Description**
CiscoCyberVision-update-center-3.1.0.dat	Center update file
CiscoCyberVision-update-sensor-3.1.0.dat	Sentryo Sensor3, 5, 7 update file
CiscoCyberVision-update-combined-3.1.0.dat	Center and Legacy Sensor update file from GUI
CiscoCyberVision-Embedded-KDB-3.1.0.dat	Knowledge DB embedded in Cisco Cyber Vision 3.1.0
Updates/KDB/KDB.202009	**Description**
CiscoCyberVision_knowledgedb_20201002.db	Knowledge DB version 20201002
CiscoCyberVision_knowledgedb_20201009.db	Knowledge DB version 20201009
CiscoCyberVision_knowledgedb_20201016.db	Knowledge DB version 20201016

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_Release_3_1_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 below. 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.

Please note that the product may not show the CVSS score for some of these vulnerabilities due to ongoing work on the integration of CVSSv3 scores.

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 and update network data.

Release contents

20201030

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

- **Talos Rules 2020-10-20 (https://www.snort.org/advisories/talos-rules-2020-10-20)**
    - Talos has added and modified multiple rules in the browser-webkit, file-pdf, indicator-compromise, malware-cnc, malware-other, os-linux and server-webapp rule sets to provide coverage for emerging threats from these technologies..
- **Talos Rules 2020-10-22 (https://www.snort.org/advisories/talos-rules-2020-10-22)**
    - 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 2020-10-27 (https://www.snort.org/advisories/talos-rules-2020-10-27)**
    - Talos has added and modified multiple rules in the browser-chrome, browser-ie, browser-plugins, browser-webkit, exploit-kit, file-flash, file-identify, file-java, file-multimedia, file-office, file-other, file-pdf, malware-backdoor, malware-cnc, malware-other, malware-tools, os-other, os-windows, policy-other, protocol-other, protocol-scada, protocol-telnet, pua-adware, server-apache, server-other and sql rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-10-29 (https://www.snort.org/advisories/talos-rules-2020-10-29)**
    - Talos has added and modified multiple rules in the browser-chrome, browser-ie, browser-plugins, exploit-kit, file-executable, file-flash, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, indicator-compromise, malware-backdoor, malware-cnc, malware-other, os-linux, os-windows, policy-other, pua-other, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20201016

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

- **Talos Rules 2020-10-13 (https://www.snort.org/advisories/talos-rules-2020-10-13)**
    - Microsoft Vulnerability CVE-2020-16896: A coding deficiency exists in Remote Desktop Protocol (RDP) that may lead to information disclosure.
    - A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 1, SID 55994.
    - Microsoft Vulnerability CVE-2020-16898: A coding deficiency exists in Microsoft Windows TCP/IP 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 55984.
    - Microsoft Vulnerability CVE-2020-16899: A coding deficiency exists in Microsoft Windows TCP/IP that may lead to denial of service.
    - A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID

1, SID 55993.

- Microsoft Vulnerability CVE-2020-16907: 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 55942 through 55943.
- Microsoft Vulnerability CVE-2020-16913: 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 55989 through 55990.
- Microsoft Vulnerability CVE-2020-16915: A coding deficiency exists in Microsoft Media Foundation 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 55979 through 55980.
- Microsoft Vulnerability CVE-2020-16922: A coding deficiency exists in Microsoft Windows that may lead to spoofing.
- Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 55982 through 55983.
- Talos also has added and modified multiple rules in the file-multimedia, file-other, malware-cnc, malware-other, os-windows, protocol-icmp and server-webapp rule sets to provide coverage for emerging threats from these technologies.

- **Talos Rules 2020-10-15 (https://www.snort.org/advisories/talos-rules-2020-10-15)**
  - Talos has added and modified multiple rules in the browser-webkit, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.

This release also contains additions and modifications following the publication of several vulnerabilities:

1. **CVE-2020-7548: (Use of Insufficiently Random Values vulnerability in Smartlink, PowerTag, and Wiser Series Gateways)**
   - A CWE-330 - Use of Insufficiently Random Values vulnerability exists that could allow unauthorized users to login.
2. **CVE-2020-7533: (Credentials Management vulnerability in Web Server on Modicon M340, Modicon Quantum and Modicon Premium Legacy offers and their Communication Modules)**
   - A CWE-255: Credentials Management vulnerability exists which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests.
3. **CVE-2020-6087: (Allen-Bradley Flex IO 1794-AENT/B ENIP Request Path Data Segment Denial of Service Vulnerability)**
   - An exploitable denial of service vulnerability exists in the ENIP Request Path Data Segment functionality of Allen-Bradley Flex IO 1794-AENT/B. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability.

4. **CVE-2020-6086: (Allen-Bradley Flex IO 1794-AENT/B ENIP Request Path Data Segment Denial of Service Vulnerability)**
    - An exploitable denial of service vulnerability exists in the ENIP Request Path Data Segment functionality of Allen-Bradley Flex IO 1794-AENT/B. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability.
5. **CVE-2020-6085: (Allen-Bradley Flex IO 1794-AENT/B ENIP Request Path Logical Segment Denial of Service Vulnerability)**
    - An exploitable denial of service vulnerability exists in the ENIP Request Path Logical Segment functionality of Allen-Bradley Flex IO 1794-AENT/B. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability.
6. **CVE-2020-6084: (Allen-Bradley Flex IO 1794-AENT/B ENIP Request Path Logical Segment Denial of Service Vulnerability)**
    - An exploitable denial of service vulnerability exists in the ENIP Request Path Logical Segment functionality of Allen-Bradley Flex IO 1794-AENT/B. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability.
7. **CVE-2020-6083: (Allen-Bradley Flex IO 1794-AENT/B ENIP Request Path Port Segment Denial of Service Vulnerability)**
    - An exploitable denial of service vulnerability exists in the ENIP Request Path Port Segment functionality of Allen-Bradley Flex IO 1794-AENT/B. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability.
8. **CVE-2020-16233: (Disclosure of internal memory in Wibu-Systems CodeMeter)**
    - An attacker could send a specially crafted packet that could have CodeMeter (All versions prior to 7.10) send back packets containing data from the heap
9. **CVE-2020-15791: (Insufficiently Protected Credentials Vulnerability in Siemens SIMATIC S7-300 and S7-400 CPUs)**
    - The authentication protocol between a client and a PLC via port 102/tcp (ISO-TSAP) insufficiently protects the transmitted password. This could allow an attacker that is able to intercept the network traffic to obtain valid PLC credentials.
10. **CVE-2020-14519: (Possible use of internal websocket in Wibu-Systems CodeMeter)**
    - This vulnerability allows an attacker to use the internal WebSockets API for CodeMeter (All versions prior to 7.00 are affected, including Version 7.0 or newer with the affected WebSockets API still enabled. This is especially relevant for systems or devices where a web browser is used to access a web server) via a specifically crafted Java Script payload, which may allow alteration or creation of license files for when combined with CVE-2020-14515.
11. **CVE-2020-14517: (Weak protocol encryption in Wibu-Systems CodeMeter)**

- Protocol encryption can be easily broken for CodeMeter (All versions prior to 6.90 are affected, including Version 6.90 or newer only if CodeMeter Runtime is running as server) and the server accepts external connections, which may allow an attacker to remotely communicate with the CodeMeter API.

12. **CVE-2020-14515: (Possible arbitrary licence file in Wibu-Systems CodeMeter)**
    - CodeMeter (All versions prior to 6.90 when using CmActLicense update files with CmActLicense Firm Code) has an issue in the license-file signature checking mechanism, which allows attackers to build arbitrary license files, including forging a valid license file as if it were a valid license file of an existing vendor. Only CmActLicense update files with CmActLicense Firm Code are affected.
13. **CVE-2020-14513: (Possible crash in Wibu-Systems CodeMeter)**
    - CodeMeter (All versions prior to 6.81) and the software using it may crash while processing a specifically crafted license file due to unverified length fields
14. **CVE-2020-14509: (Multiple memory corruption vulnerabilities in Wibu-Systems CodeMeter)**
    - Multiple memory corruption vulnerabilities exist where the packet parser mechanism of CodeMeter (All versions prior to 7.10a) does not verify length fields. An attacker could send specially crafted packets to exploit these vulnerabilities.
15. **CVE-2020-0543: (Exposure of Sensitive Information to an Unauthorized Actor Vulnerability in Siemens Industrial Products (Special Register Buffer Data Sampling aka Crosstalk))**
    - Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access
16. **CVE-2018-7857: (Multiple vulnerabilities in modicon controllers)**
    - Schneider Electric is aware of multiple vulnerabilities in its Modicon Controller products.
17. **CVE-2018-7856: (Multiple vulnerabilities in modicon controllers)**
    - Schneider Electric is aware of multiple vulnerabilities in its Modicon Controller products.
18. **CVE-2018-7843: (Multiple vulnerabilities in modicon controllers)**
    - Schneider Electric is aware of multiple vulnerabilities in its Modicon Controller products.
19. **CVE-2017-6028: (Schneider Electric Modicon PLCs vulnerabilities - Insufficiently Protected Credentials)**
    - Modicon M221, M241, and M251 programmable logic controllers (PLCs) are affected by the following vulnerabilities: Predictable Value Range from Previous Values, Use of Insufficiently Random Values, Insufficiently Protected Credentials
20. **CVE-2017-14496: (DNSMasq vulnerability (Integer Underflow) in Siemens products)**
    - An attacker could cause a crash of the DNSmasq process by sending specially crafted requestmessages to the service on port 53/udp
21. **CVE-2017-14495: (DNSMasq vulnerability (Resource Management Errors) in Siemens products)**
    - An attacker could cause a crash of the DNSmasq process by sending specially crafted requestmessages to the service on port 53/udp
22. **CVE-2017-14491: (DNSMasq vulnerability (mproper Restriction of Operations within the Boundsof a Memory Buffer) in Siemens products)**

- An attacker could cause a crash or potentially execute arbitrary code by sending specially crafted DNS responses to the DNSmasq process. In order to exploit this vulnerability, an attacker must be able to trigger DNS requests from the device, and must be in a privileged position to inject malicious DNSresponses

23. **CVE-2017-13704: (DNSMasq vulnerability (Improper Input Validation) in Siemens products)**
    - An attacker could cause a crash of the DNSmasq process by sending specially crafted requestmessages to the service on port 53/udp.

20201009

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

- **Talos Rules 2020-10-08 (https://www.snort.org/advisories/talos-rules-2020-10-08)**
  - Talos has added and modified multiple rules in the malware-cnc and server-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-10-06 (https://www.snort.org/advisories/talos-rules-2020-10-06)**
  - Talos has added and modified multiple rules in the malware-cnc, malware-other, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20201002

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

- **Talos Rules 2020-09-29 (https://www.snort.org/advisories/talos-rules-2020-09-29)**
  - Talos has added and modified multiple rules in the file-other, file-pdf, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-10-01 (https://www.snort.org/advisories/talos-rules-2020-10-01)**
  - Talos has added and modified multiple rules in the malware-backdoor, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.