Release Notes for Cisco Cyber Vision Knowledge DB

Release 202012

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-3.2.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-3.2.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-3.2.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-3.2.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-3.2.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-3.2.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.2.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-3.2.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
Updates/3/3.2.0	**Description**
CiscoCyberVision-sysupgrade-3.2.0.dat	System Upgrade file for Center and Sensors 3.1.x to 3.2.0
CiscoCyberVision-sysupgrade-sensor-3.2.0.dat	Cisco Cyber Vision System Upgrade file for IC3000 Sensors or other non IOx Sensors 3.x to 3.2.0
CiscoCyberVision-Embedded-KDB-3.2.0.dat	Knowledge DB embedded in Cisco Cyber Vision 3.2.0
Updates/KDB/KDB.202012	**Description**
CiscoCyberVision_knowledgedb_20201204.db	Knowledge DB version 20201204
CiscoCyberVision_knowledgedb_20201211.db	Knowledge DB version 20201211
CiscoCyberVision_knowledgedb_20201218.db	Knowledge DB version 20201218
CiscoCyberVision_knowledgedb_20201229.db	Knowledge DB version 20201229

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.

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

20201229

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

- **Talos Rules 2020-12-22 (https://www.snort.org/advisories/talos-rules-2020-12-22)**
    - Talos has added and modified multiple rules in the deleted, file-other, malware-cnc, malware-other, malware-tools, policy-other, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20201218

This release contains Snort rules relative to the backdoor tracked as SUNBURST by FireEye. This backdoor is used as part of a supply chain attack where adversaries compromised updates to the SolarWinds Orion IT monitoring and management software. More information on the breach can be found in the following Talos blog post: https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html

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

- **Talos Rules 2020-12-14 (https://www.snort.org/advisories/talos-rules-2020-12-14)**
    - 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.
- **Talos Rules 2020-12-17 (https://www.snort.org/advisories/talos-rules-2020-12-17)**
    - Talos has added and modified multiple rules in the file-other, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20201211

This release contains Snort rules which protect users against the vulnerabilities related to the recent FireEye security breach in which various internally developed offensive security tools were inadvertently disclosed. More information on the breach can be found in the following Talos blog post: https://blog.talosintelligence.com/2020/12/fireeye-breach-guidance.html

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

- **Talos Rules 2020-12-08 (https://www.snort.org/advisories/talos-rules-2020-12-08)**
    - Talos Microsoft Vulnerability CVE-2020-17096: A coding deficiency exists in NTFS 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 56561 through 56562.
    - Microsoft Vulnerability CVE-2020-17121: 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 56560.
    - Microsoft Vulnerability CVE-2020-17144: A coding deficiency exists in Microsoft Exchange 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 56554.
- Microsoft Vulnerability CVE-2020-17152: A coding deficiency exists in Microsoft Dynamics 365 for Finance and Operations (on-premises) 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 56558.
- Microsoft Vulnerability CVE-2020-17158: A coding deficiency exists in Microsoft Dynamics 365 for Finance and Operations (on-premises) 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 56557.
- Talos also has added and modified multiple rules in the file-multimedia, malware-other, os-windows, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

- **Talos Rules 2020-12-09 (https://www.snort.org/advisories/talos-rules-2020-12-09)**
  - Talos has added and modified multiple rules in the browser-other, indicator-compromise, malware-backdoor, malware-cnc, malware-other, malware-tools, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-12-10 (https://www.snort.org/advisories/talos-rules-2020-12-10)**
  - Talos has added and modified multiple rules in the browser-other and server-other rule sets to provide coverage for emerging threats from these technologies.

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

- CVE-2020-7549: (Improper Check for Unusual or Exceptional Conditions vulnerability in Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules)
  - A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of HTTP and FTP services when a series of specially crafted requests is sent to the controller over HTTP
- CVE-2020-7543: (Improper Check for Unusual or Exceptional Conditions vulnerability in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium)
  - A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause a denial of service of the controller when a malformed Routing request over Modbus is send to the controller
- CVE-2020-7542: (Improper Check for Unusual or Exceptional Conditions vulnerability in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium)
  - A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a specially crafted Read request over Modbus is send to the controller
- CVE-2020-7541: (Direct Request vulnerability in Web Server on Modicon M340, Legacy Offers Modicon Quantum

and Modicon Premium and associated Communication Modules)

- A CWE-425: Direct Request ('Forced Browsing') vulnerability exists that could cause disclosure of sensitive data when sending a specially crafted request to the controller over HTTP

- CVE-2020-7540: (Missing Authentication for Critical Function vulnerability in Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules)
  - A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause unauthenticated command execution in the controller when sending special HTTP requests
- CVE-2020-7539: (Improper Check for Unusual or Exceptional Conditions vulnerability in Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules)
  - A CWE-754 Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause a denial of service vulnerability when a specially crafted packet is sent to the controller over HTTP
- CVE-2020-7537: (Improper Check for Unusual or Exceptional Conditions vulnerability in Modicon M580, Modicon M340, Legacy Controllers Modicon Quantum & Modicon Premium)
  - A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service when a specially crafted Read Physical Memory request over Modbus is sent to the controller
- CVE-2020-7536: (Improper Check for Unusual or Exceptional Conditions vulnerability in SNMP Service on Modicon M340 and associated Communication Modules)
  - A CWE-754:Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause the device to be unreachable when modifying network parameters over SNMP
- CVE-2020-7535: (Path Traversal in Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules)
  - A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal' Vulnerability Type) vulnerability exists that could cause disclosure of information when sending a specially crafted request to the controller over HTTP
- CVE-2020-6111: (IPv4 denial-of-service vulnerability in MicroLogix 1100)
  - An exploitable denial-of-service vulnerability exists in the IPv4 functionality of Allen-Bradley MicroLogix 1100 Programmable Logic Controller Systems Series B FRN 16.000, Series B FRN 15.002, Series B FRN 15.000, Series B FRN 14.000, Series B FRN 13.000, Series B FRN 12.000, Series B FRN 11.000 and Series B FRN 10.000. A specially crafted packet can cause a major error, resulting in a denial of service. An attacker can send a malicious packet to trigger this vulnerability.
- CVE-2020-28396: (Protection Mechanism Failure in SICAM A8000)
  - A web server misconfiguration of the affected device can cause insecure ciphers usage by a user´s browser. An attacker in a privileged position could decrypt the communication and compromise confidentiality and integrity of the transmitted information.
- CVE-2020-28220: (Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in Modicon M258 Logic Controllers)
  - A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause a buffer overflow when the length of a file transferred to the webserver is not verified

- CVE-2020-28218: (Improper Restriction of Rendered UI Layers or Frames vulnerability in Easergy T300)
  - A CWE-1021: Improper Restriction of Rendered UI Layers or Frames vulnerability exists that would allow an attacker to trick a user into initiating an unintended action
- CVE-2020-28217: (Missing Encryption of Sensitive Data vulnerability in Easergy T300)
  - A CWE-311: Missing Encryption of Sensitive Data vulnerability exists that would allow an attacker to read network traffic over IEC60870-5-104 protocol
- CVE-2020-28216: (Missing Encryption of Sensitive Data vulnerability in Easergy T300)
  - A CWE-311: Missing Encryption of Sensitive Data vulnerability exists that would allow an attacker to read network traffic over HTTP protocol
- CVE-2020-28215: (Missing Authorization vulnerability in Easergy T300)
  - A CWE-862: Missing Authorization vulnerability exists that could cause a wide range of problems, including information exposures, denial of service, and arbitrary code execution when access control checks are not applied consistently
- CVE-2020-28214: (Use of a One-Way Hash with a Predictable Salt vulnerability in Modicon M221)
  - A CWE-760: Use of a One-Way Hash with a Predictable Salt vulnerability exists that could allow an attacker to pre-compute the hash value using dictionary attack technique such as rainbow tables, effectively disabling the protection that an unpredictable salt would provide
- CVE-2020-25235: (Insufficiently Protected Credentials in Siemens LOGO! 8 BM)
  - The password used for authentication for the LOGO! Website and the LOGO! Access Tool is sent in a recoverable format. An attacker with access to the network traffic could derive valid logins
- CVE-2020-25234: (Use of Hard-coded Cryptographic Key in Siemens LOGO! 8 BM)
  - The LOGO! program files generated and used by the affected components offer the possibility to save user-defined functions (UDF) in a password protected way. This protection is implemented in the software that displays the information. An attacker could reverse engineer the UDFs directly from stored program files
- CVE-2020-25233: (Use of Hard-coded Cryptographic Key in Siemens LOGO! 8 BM)
  - The firmware update of affected devices contains the private RSA key that is used as a basis for encryption of communication with the device.
- CVE-2020-25232: (Use of a Broken or Risky Cryptographic Algorithm in Siemens LOGO! 8 BM)
  - Due to the usage of an insecure random number generation function and a deprecated cryptographic function, an attacker could extract the key that is used when communicating with an affected device on port 8080/tcp.
- CVE-2020-25231: (Use of Hard-coded Cryptographic Key in Siemens LOGO! 8 BM)
  - The encryption of program data for the affected devices uses a static key. An attacker could use this key to extract confidential information from protected program files.
- CVE-2020-25230: (Use of a Broken or Risky Cryptographic Algorithm in Siemens LOGO! 8 BM)
  - Due to the usage of an outdated cipher mode on port 10005/tcp, an attacker could extract the encryption key from a captured communication with the device.

- CVE-2020-25229: (Use of Hard-coded Cryptographic Key in Siemens LOGO! 8 BM)
  - The implemented encryption for communication with affected devices is prone to replay attacks due to the usage of a static key. An attacker could change the password or change the configuration on any affected device if using prepared messages that were generated for another device.
- CVE-2020-25228: (Missing Authentication for Critical Function in Siemens LOGO! 8 BM)
  - A service available on port 10005/tcp of the affected devices could allow complete access to all services without authorization. An attacker could gain full control over an affected device, if he has access to this service. The system manual recommends to protect access to this port.
- CVE-2020-15796: (Uncaught Exception in Siemens SIMATIC Controller Web Servers)
  - The web server of the affected products contains a vulnerability that could allow a remote attacker to trigger a denial-of-service condition by sending a specially crafted HTTP request.
- CVE-2020-13988: (Integer Overflow in embedded TCP/IP Stack (Amnesia:33))
  - The TCP/IP stack (uIP) in affected devices is vulnerable due to Integer Overflow when processing TCP Maximum Segment Size (MSS) options. (FSCT-2020-0008)
- CVE-2020-12524: (BTP Touch Panels uncontrolled resource consumption)
  - Uncontrolled Resource Consumption can be exploited to cause the HMI to become unresponsive and not accurately update the display content (Denial of Service).
- CVE-2019-8287: (Buffer overflow in TightVNC)
  - TightVNC code version 1.3.10 contains global buffer overflow in HandleCoRREBBP macro function,which can potentially result in code execution. This attack appear to be exploitable via network connectivity.
- CVE-2019-15680: (Null pointer dereference in TightVNC)
  - TightVNC code version 1.3.10 contains null pointer dereference in HandleZlibBPP function, whichcould result in a Denial-of-Service (DoS). This attack appears to be exploitable via network connectivity.
- CVE-2019-15679: (Heap buffer overflow in TightVNC)
  - TightVNC code version 1.3.10 contains heap buffer overflow in InitialiseRFBConnection function, which can potentially result in code execution. This attack appears to be exploitable via network connectivity.
- CVE-2019-15678: (Heap buffer overflow in TightVNC)
  - TightVNC code version 1.3.10 contains heap buffer overflow in rfbServerCutText handler, which canpotentially result in code execution. This attack appears to be exploitable via network connectivity.
- CVE-2019-13946: (Uncontrolled Resource Consumption Vulnerability in Siemens PROFINET-IO Stack)
  - Successful exploitation of this vulnerability could lead to a denial-of-service condition.
- CVE-2019-10919: (Siemens LOGO!8 BM Multiple Information Disclosure Vulnerabilities)
  - A vulnerability has been identified in LOGO!8 BM (All versions). Attackers with access to port 10005/tcp could perform device reconfigurations and obtain project files from the devices. The system manual recommends to protect access to this port. The security vulnerability could be exploited by an unauthenticated attacker with network access to port 10005/tcp. No user interaction is required to exploit this security vulnerability. The vulnerability impacts confidentiality, integrity, and availability of the device. At the time of advisory publication, no public exploitation of this security vulnerability was

known.

- CVE-2017-12735: (Man-in-the-Middle in Siemens LOGO!)
  - An attacker who performs a Man-in-the-Middle attack between the LOGO! BM and other devices could potentially decrypt and modify network traffic.
- CVE-2017-12734: (Insufficiently Protected Credentials in Siemens LOGO!)
  - An attacker with network access to the integrated web server on port 80/tcp could obtain the sessionID of an active user session. A user must be logged in to the web interface. Siemens recommends touse the integrated web server on port 80/tcp only in trusted networks.

20201204

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

- **Talos Rules 2020-12-01 (https://www.snort.org/advisories/talos-rules-2020-12-01)**
  - Talos has added and modified multiple rules in the browser-chrome, file-office, file-other, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-12-03 (https://www.snort.org/advisories/talos-rules-2020-12-03)**
  - Talos has added and modified multiple rules in the browser-firefox, browser-ie, file-other, malware-cnc, malware-other, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-12-03 (https://www.snort.org/advisories/talos-rules-2020-12-03-12-3-2020)**
  - Talos has added and modified multiple rules in the malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.