Release Notes for Cisco Cyber Vision Knowledge DB

Release 202011

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.202011	**Description**
CiscoCyberVision_knowledgedb_20201106.db	Knowledge DB version 20201106
CiscoCyberVision_knowledgedb_20201113.db	Knowledge DB version 20201113
CiscoCyberVision_knowledgedb_20201120.db	Knowledge DB version 20201120
CiscoCyberVision_knowledgedb_20201127.db	Knowledge DB version 20201127

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

20201127

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

- **Talos Rules 2020-11-24 (**https://www.snort.org/advisories/talos-rules-2020-11-24**)**
    - 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.

20201120

Starting from this release, the Cisco Cyber Vision Knowledge DB introduces a distinction between registered and subscriber rules:

- **Subscribers will receive rulesets in real-time as they are released to Cisco customers - 30 days ahead of registered users.**
- **Registered users will receive rulesets 30 days after subscribers.**

Unless otherwise specified, all updates reported in the subsequent Knowledge DB release notes are specific to the subscriber ruleset.
For users with registered ruleset support, these updates should be effective within 30 days.
Subscriber ruleset is not accessible for users with a Cisco Cyber Vision version prior to 3.2.0. Users running the 3.2.0 version can switch between the registered and the subscriber ruleset through the dedicated Snort page on the Cisco Cyber Vision Center webapp.

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

- **Talos Rules 2020-11-19 (https://www.snort.org/advisories/talos-rules-2020-11-19)**
    - Talos has added and modified multiple rules in the browser-chrome, exploit-kit, file-image, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-11-17 (https://www.snort.org/advisories/talos-rules-2020-11-17)**
    - Talos has added and modified multiple rules in the browser-webkit, file-image, file-office, indicator-shellcode, malware-backdoor, malware-cnc, malware-other, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20201113

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

- **Talos Rules 2020-11-12 (https://www.snort.org/advisories/talos-rules-2020-11-12)**
    - Talos has added and modified multiple rules in the malware-other, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-11-10 (https://www.snort.org/advisories/talos-rules-2020-11-10)**
    - Microsoft Vulnerability CVE-2020-16998: A coding deficiency exists in DirectX Graphics Kernel 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 56254 through 56255.
- Microsoft Vulnerability CVE-2020-17010: 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 56263 through 56264.
- Microsoft Vulnerability CVE-2020-17038: 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 56261 through 56262.
- Microsoft Vulnerability CVE-2020-17047: A coding deficiency exists in Microsoft Windows Network File System 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 56309.
- Microsoft Vulnerability CVE-2020-17051: A coding deficiency exists in Microsoft Windows Network File System 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 56311 through 56312.
- Microsoft Vulnerability CVE-2020-17052: A coding deficiency exists in Microsoft Windows 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 56286 through 56287.
- Microsoft Vulnerability CVE-2020-17053: A coding deficiency exists in Microsoft Internet Explorer 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 56288 through 56289.
- Microsoft Vulnerability CVE-2020-17056: A coding deficiency exists in Microsoft Windows Network File System that may lead to information disclosure.
- Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 56301 through 56302.
- Microsoft Vulnerability CVE-2020-17057: 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 56259 through 56260.
- Microsoft Vulnerability CVE-2020-17061: A coding deficiency exists in Microsoft SharePoint 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 56303 through 56305.
- Microsoft Vulnerability CVE-2020-17087: A coding deficiency exists in Microsoft Windows Kernel that may lead to an escalation of privilege.
- Previously released rules will detect attacks targeting these vulnerabilities and have been updated with the appropriate reference information. They are also included in this release and are identified with GID 1, SIDs 56230 through 56231.
- Microsoft Vulnerability CVE-2020-17088: A coding deficiency exists in Microsoft Windows Common Log File System 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 56295 through 56296.

- Talos also has added and modified multiple rules in the browser-ie, file-executable, file-office, file-other, malware-cnc, malware-other, os-windows, protocol-rpc and server-webapp rule sets to provide coverage for emerging threats from these technologies.

This release introduces the support of Phoenix Contact vulnerabilities. All recent Phoenix Contact vulnerabilities have now been added as part of the Cisco Cyber Vision KDB. Cisco Cyber Vision is thus able to match the latest vulnerabilities to Phoenix Contact devices detected on the network. This release also contains additions and modifications following the publication of several vulnerabilities:

- CVE-2020-8597: (Buffer Overflow Vulnerability in Siemens SCALANCE, RUGGEDCOM)
  - The version of pppd shipped with this product has a vulnerability that may allow an unauthenticated remote attacker to cause a stack buffer overflow, which may allow arbitrary code execution on the target system.

- CVE-2020-7568: (Information Disclosure Vulnerability on Modicon M221 Programmable Logic Controller)
  - A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists that could allow non sensitive information disclosure when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M221 controller

- CVE-2020-7567: (Missing Encryption of Sensitive Data Vulnerability on Modicon M221 Programmable Logic Controller)
  - A CWE-311: Missing Encryption of Sensitive Data vulnerability exists that could allow the attacker to find the password hash when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M221 controller and broke the encryption keys

- CVE-2020-7566: (Small Space of Random Values Vulnerability on Modicon M221 Programmable Logic Controller)
  - A CWE-334: Small Space of Random Values vulnerability exists that could allow the attacker to break the encryption keys when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M221 controller

- CVE-2020-7565: (Inadequate Encryption Strength Vulnerability on Modicon M221 Programmable Logic Controller)
  - A CWE-326: Inadequate Encryption Strength vulnerability exists that could allow the attacker to break the encryption key when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M221 controller

- CVE-2020-7564: (Buffer Overflow Vulnerability in Modicon M340, Modicon Quantum and Modicon Premium Legacy)
  - A CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability exists which could cause write access and the execution of commands when uploading a specially crafted file on the controller over FTP.

- CVE-2020-7563: (Out-of-Bounds Write Vulnerability in Modicon M340, Modicon Quantum and Modicon Premium Legacy)

        - A CWE-787: Out-of-bounds Write vulnerability exists which could cause corruption of data, a crash, or code execution when uploading a specially crafted file on the controller over FTP.

    - CVE-2020-7562: (Out-of-Bounds Read Vulnerability in Modicon M340, Modicon Quantum and Modicon Premium Legacy)
        - A CWE-125: Out-of-Bounds Read vulnerability exists which could cause a segmentation fault or a buffer overflow when uploading a specially crafted file on the controller over FTP

    - CVE-2020-7561: (Improper Access Control Vulnerability on Easergy T300)
        - A CWE-284: Improper Access Control vulnerability exists that could cause a wide range of problems, including information exposure, denial of service, and command execution when access to a resource from an attacker is not restricted or incorrectly restricted

    - CVE-2020-7488: (Cleartext Transmission of Sensitive Information Vulnerability in Modicon M218/M241/M251/M258 Logic Controllers, SoMachine/SoMachine Motion, and EcoStruxure Machine Expert)
        - A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers

    - CVE-2020-7487: (Insufficient Verification of Data Authenticity Vulnerability in Modicon M218/M241/M251/M258 Logic Controllers, SoMachine/SoMachine Motion, and EcoStruxure Machine Expert)
        - A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers

    - 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.

    - CVE-2020-15783: (Uncontrolled Resource Consumption in Siemens SIMATIC S7-300 CPUs and SINUMERIK Controller)
        - Sending multiple specially crafted packets to the affected devices could cause a Denial-of-Service on port 102. A cold restart is required to recover the service.

    - CVE-2020-14483: (TLS Timeout Vulnerability in Emalytics, ILC 2050 BI and ILC 2050 BI-L)
        - A timeout during a TLS handshake can result in the connection failing to terminate. This can result in a Niagara thread hanging and requires a manual restart to correct.

    - CVE-2019-6849: (UMAS REST API getcominfo information disclosure vulnerability)

        - Information Exposure vulnerability exists, which could cause the disclosure of sensitive information when using specific Modbus services provided by the REST API of the controller/communication module.

    - CVE-2019-6848: (UMAS REST API getcominfo denial-of-service vulnerability)
        - Uncaught Exception vulnerability exists, which could cause a Denial of Service attack on the PLC when sending specific data on the REST API of the controller/communication module.

    - CVE-2016-2031: (Improper Input Validation in Siemens SCALANCE W 1750D)
        - Multiple vulnerabilities exist in Aruba Instate before 4.1.3.0 and 4.2.3.1 due to insufficient validation of user-supplied input and insufficient checking of parameters, which could allow a malicious user to bypass security restrictions, obtain sensitive information, perform unauthorized actions and execute arbitrary code.

20201106

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

- **Talos Rules 2020-11-04 (https://www.snort.org/advisories/talos-rules-2020-11-04)**
    - Talos has added and modified multiple rules in the file-office, file-other, malware-cnc, malware-other, os-windows, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2020-11-02 (https://www.snort.org/advisories/talos-rules-2020-11-02)**
    - Talos has added and modified multiple rules in the file-office, file-other, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

© 2020 Cisco Systems, Inc. All rights reserved.