Release Notes for Cisco Cyber Vision Knowledge DB

Release 20200618

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 find 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	IE3400, IR1101 sensor installation and update file
CiscoCyberVision-IOx-IC3K-3.1.0.tar	IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.1.0.tar	Cat9k sensor 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	**Description**
CiscoCyberVision_knowledgedb_20200618.db	Knowledge DB version 20200618

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

The new version is available following the publication and the update of several vulnerabilities:

1. CVE-2020-7589: (Missing Authentication For Critical Function in Siemens LOGO!)

   The vulnerability could lead to an attacker reading and modifying the device configuration and obtain project files from affected devices. The security vulnerability could be exploited by an unauthenticated attacker with network access to port 135/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.

2. CVE-2020-7502: (Out-of-bounds Write Vulnerability in Schneider Modicon M218 Logic Controller)

   A CWE-787: Out-of-bounds Write vulnerability exists, which may cause a Denial of Service when specific TCP/IP crafted packets are sent to the Modicon M218 Logic Controller.

3. CVE-2020-10664: (NULL Pointer Dereference Vulnerability in Schneider Modicon LMC078 Logic Controller)

   The IGMP component in VxWorks 6.8.3 IPNET CVE patches created in 2019 has a NULL Pointer Dereference. Additional details on this specific vulnerability can be found on the Wind River security notification web page: https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2020-10664

4. CVE-2015-7937: (Schneider Electric Modicon M340 Buffer Overflow Vulnerability)

   A vulnerability has been identified, in Schneider Electric Industrial Ethernet devices that allows an attacker to cause a buffer overflow situation using the web server login mechanism to halt operation of the device or remotely execute code.

Cisco Cyber Vision detects the presence of these vulnerabilities using this new Knowledge DB.

This release also includes additions and modifications to the Snort ruleset covering the advisories published by Talos between the 5/3/2020 and the 9/6/2020:

https://www.snort.org/advisories

If needed, the Cisco Cyber Vision security team is willing to help you analyze and patch your network.