Release Notes for Cisco Cyber Vision Knowledge DB

Release 202206

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-4.1.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.1.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.1.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.1.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.1.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.1.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.1.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.1.0.dat	Knowledge DB embedded in Cisco Cyber Vision 4.1.0
Updates/KDB/KDB.202206	**Description**
CiscoCyberVision_knowledgedb_20220603.db	Knowledge DB version 20220603
CiscoCyberVision_knowledgedb_20220610.db	Knowledge DB version 20220610
CiscoCyberVision_knowledgedb_20220617.db	Knowledge DB version 20220617
CiscoCyberVision_knowledgedb_20220624.db	Knowledge DB version 20220624

Related Documentation

- Cisco Cyber Vision GUI User Guide:

  https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/GUI/b_Cisco_Cyber_Vision_GUI_User_Guide.html

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

20220624

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

- **Talos Rules 2022-06-23 (https://www.snort.org/advisories/talos-rules-2022-06-23)**
  - Talos has added and modified multiple rules in the browser-chrome, file-pdf, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-06-21 (https://www.snort.org/advisories/talos-rules-2022-06-21)**
  - Talos has added and modified multiple rules in the browser-chrome, file-office, file-pdf, malware-cnc 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:

- CVE-2022-29519: (Cleartext Transmission of Sensitive Information in Yokogawa STARDOM)
  - This vulnerability may allow to an attacker to sniff network traffic with the FCN/FCJ controller. An attacker could read/change configuration or update tampered firmware to the controller by exploitation of this vulnerability.
- CVE-2022-31800: (Insufficient Verification of Data Authenticity in Phoenix Contact classic line industrial controllers)
  - Phoenix Contact classic line industrial controllers are developed and designed for the use in closed industrial networks. The controllers don't feature a function to check integrity and authenticity of uploaded logic.
- CVE-2022-30997: (Use of Hard-coded Credentials in Yokogawa STARDOM)
  - This vulnerability may allow to an attacker to obtain hard-coded credentials. An attacker could read/change configuration or update tampered firmware to the controller by exploitation of this vulnerability.

Note: this week's new vulnerabilities are all linked to the recently disclosed Icefall vulnerabilities. Most of the Icefall vulnerabilities impact either software which is outside of Cyber Vision's vulnerability matching scope, or constructors which Cyber Vision does not yet support. Among the Icefall vulnerabilities, those that fall within Cyber Vision's scope affect Phoenix Contact, Yokogawa, Emerson, and Omron devices. The three vulnerabilities released this week concern Phoenix Contact and Yokogawa. For the Emerson and Omron vulnerabilities, we are still missing crucial information (exact impacted products and firmware versions, CVSS scores). These vulnerabilities will be added as soon as we receive enough information through the constructor's advisories or the NVD.

20220617

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

- **Talos Rules 2022-06-16 (https://www.snort.org/advisories/talos-rules-2022-06-16)**
  - Talos has added and modified multiple rules in the indicator-shellcode and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-06-14 (https://www.snort.org/advisories/talos-rules-2022-06-14)**

- Microsoft Vulnerability CVE-2022-30147: A coding deficiency exists in Microsoft Windows Installer that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 59967 through 59968, Snort3: GID 1, SID 300201.
- Microsoft Vulnerability CVE-2022-30160: A coding deficiency exists in Microsoft Windows Advanced Local Procedure Call that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort2: GID 1, SIDs 59971 through 59972, Snort3: GID 1, SID 300202.
- Talos also has added and modified multiple rules in the file-office, malware-cnc, malware-other, os-windows 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:

- CVE-2021-4034: (PwnKit Vulnerability in Siemens SCALANCE LPE9403)
    - The products listed below contain a local privilege escalation vulnerability (CVE-2021-4034) found on polkit’s pkexec utility, that could allow an unprivileged user to gain administrative rights.
- CVE-2021-41103: (Path Traversal Vulnerability in Siemens SCALANCE LPE9403 before V2.0)
    - A vulnerability was found in containerd where container root directories and some plugins had insufficiently restricted permissions, allowing otherwise unprivileged Linux users to traverse directory contents and execute programs. When containers included executable programs with extended permission bits (such as setuid), unprivileged Linux users could discover and execute those programs. When the UID of an unprivileged Linux user on the host collided with the file owner or group inside a container, the unprivileged Linux user on the host could discover, read, and modify those files.
- CVE-2021-41091: (Incorrect Permission Assignment for Critical Resource Vulnerability in Siemens SCALANCE LPE9403 before V2.0)
    - A vulnerability was found in Moby (Docker Engine) where the data directory (typically /var/lib/docker) contained subdirectories with insufficiently restricted permissions, allowing otherwise unprivileged Linux users to traverse directory contents and execute programs. When containers included executable programs with extended permission bits (such as setuid), unprivileged Linux users could discover and execute those programs. When the UID of an unprivileged Linux user on the host collided with the file owner or group inside a container, the unprivileged Linux user on the host could discover, read, and modify those files.
- CVE-2021-33910: (Allocation of Resources Without Limits Vulnerability in Siemens SCALANCE LPE9403 before V2.0)
    - The use of alloca function with an uncontrolled size in function unit_name_path_escape allows a local attacker, able to mount a filesystem on a very long path, to crash systemd and the whole system by allocating a very large space in the stack.
- CVE-2020-27304: (Path Traversal Vulnerability in Siemens SCALANCE LPE9403 before V2.0)
    - The CivetWeb web library does not validate uploaded filepaths when running on an OS other than Windows, when using the built-in HTTP form-based file upload mechanism, via the mg_handle_form_request API. Web applications that use the file upload form handler, and use parts of the user-controlled filename in the output path, are susceptible to directory traversal
- CVE-2021-39293: (Allocation of Resources Without Limits or Throttling Vulnerability in Siemens SCALANCE LPE9403 before V2.0)

    - The fix for CVE-2021-33196 can be bypassed by crafted inputs. As a result, the NewReader and OpenReader functions in archive/zip can still cause a panic or an unrecoverable fatal error when reading an archive that claims to contain a large number of files, regardless of its actual size.
  - CVE-2022-30937: (Memory Corruption Vulnerability in EN100 Ethernet Module)
    - EN100 Ethernet module is affected by memory corruption vulnerability.
  - CVE-2021-20317: (Improper Initialization Vulnerability in Siemens SCALANCE LPE9403 before V2.0)
    - Multiple vulnerabilities in the third-party components CivetWeb, Docker, Linux Kernel and systemd could allow an attacker to impact SCALANCE LPE9403 confidentiality, integrity and availability.
  - CVE-2022-0778: (Denial of Service Vulnerability in OpenSSL Affecting Industrial Products)
    - A vulnerability in the openSSL component (CVE-2022-0778, [0]) could allow an attacker to create a denial-of-service condition by providing specially crafted elliptic curve certificates to products that use a vulnerable version of openSSL.
  - CVE-2021-36221: (Race Condition Vulnerability in Siemens SCALANCE LPE9403 before V2.0)
    - A race condition vulnerability was found in Go. The incoming requests body weren't closed after the handler panic and as a consequence this could lead to ReverseProxy crash.
  - CVE-2021-41089: (Improper Preservation of Permissions Vulnerability in Siemens SCALANCE LPE9403 before V2.0)
    - A vulnerability was found in Moby (Docker Engine) where attempting to copy files using docker cp into a specially crafted container can result in Unix file permission changes for existing files in the host's filesystem, widening access to others. This bug does not directly allow files to be read, modified, or executed without an additional cooperating process.
  - CVE-2022-32513: (Weak Password Requirements Vulnerability in Schneider Electric C-Bus Home Automation Products)
    - A CWE-521: Weak Password Requirements vulnerability exists that could allow an attacker to gain control of the device when the attacker brute forces the password.
  - CVE-2021-37182: (Improper Validation of Integrity Check Value Vulnerability in OSPF Packet Handling of Siemens SCALANCE XM-400 and XR-500 Devices)
    - SCALANCE XM-400 and XR-500 devices contain a vulnerability in the OSPF protocol implementation that could allow an unauthenticated remote attacker to cause interruptions in the network.
  - CVE-2021-41092: (Exposure of Sensitive Information to an Unauthorized Actor Vulnerability in Siemens SCALANCE LPE9403 before V2.0)
    - A vulnerability was found in the Docker CLI where running docker login my-private-registry.example.com with a misconfigured configuration file (typically ~/.docker/config.json) listing a credsStore or credHelpers that could not be executed would result in any provided credentials being sent to registry-1.docker.io rather than the intended private registry.
  - CVE-2022-0847: (Improper Preservation of Permissions Vulnerability in Siemens SCALANCE LPE9403 before V2.0)
    - A vulnerability was found in containerd where container root directories and some plugins had insufficiently restricted permissions, allowing otherwise unprivileged Linux users to traverse directory contents and execute programs. When containers included executable programs with extended permission bits (such as setuid), unprivileged Linux users could discover and execute those programs. When the UID of an unprivileged Linux user on the host collided with the file owner or group inside a container, the unprivileged Linux user on the host could discover, read, and modify those files.
  - CVE-2022-20821: (Cisco IOS XR Software Health Check Open Port Vulnerability)
    - A vulnerability in the health check RPM of Cisco IOS XR Software could allow an unauthenticated, remote attacker to access the Redis instance that is running within the NOSi container. This vulnerability exists because the health check RPM opens TCP port 6379 by default upon activation. An attacker could exploit this vulnerability by connecting to the Redis instance on the open port. A

successful exploit could allow the attacker to write to the Redis in-memory database, write arbitrary files to the container filesystem, and retrieve information about the Redis database. Given the configuration of the sandboxed container that the Redis instance runs in, a remote attacker would be unable to execute remote code or abuse the integrity of the Cisco IOS XR Software host system. Cisco has released software updates that address this vulnerability.

20220610

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

- **Talos Rules 2022-06-09 (https://www.snort.org/advisories/talos-rules-2022-06-09)**
  - 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 2022-06-07 (https://www.snort.org/advisories/talos-rules-2022-06-07)**
  - 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 2022-06-03 (https://www.snort.org/advisories/talos-rules-2022-06-03)**
  - Talos has added and modified multiple rules in the indicator-compromise and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20220603

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

- **Talos Rules 2022-06-02 (https://www.snort.org/advisories/talos-rules-2022-06-02)**
  - 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 2022-06-01 (https://www.snort.org/advisories/talos-rules-2022-06-01-6-1-2022-21)**
  - Talos has added and modified multiple rules in the malware-cnc, os-windows, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-05-26 (https://www.snort.org/advisories/talos-rules-2022-05-26)**
  - Talos has added and modified multiple rules in the file-other, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.