Release Notes for Cisco Cyber Vision Knowledge DB

Release 202512

Compatible device list

Center	Description
All version 4 and 5 centers	All Cisco Cyber Vision center version 4 and 5 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-5.3.2.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.3.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.3.2.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.3.2.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.3.2.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.3.2.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.3.2.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.3.2.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.3.2.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.3.2.dat	Knowledge DB embedded in Cisco Cyber Vision 5.3.2
Updates/KDB/KDB.202512	**Description**
CiscoCyberVision_knowledgedb_20251205.db	Knowledge DB version 20251205
CiscoCyberVision_knowledgedb_20251212.db	Knowledge DB version 20251212

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

20251212

Snort rules

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

- **Talos Rules 2025-12-11 (https://www.snort.org/advisories/talos-rules-2025-12-11)**
- **Talos Rules 2025-12-09 (https://www.snort.org/advisories/talos-rules-2025-12-09)**

The new and updated Snort rules span the following categories:

- 3 file-other rules with SIDs 301308, 65592, 65591
- 9 malware-cnc rules with SIDs 65577, 65565, 65589, 65579, 65567, 65578, 65590, 65566, 65588
- 5 malware-other rules with SIDs 301361, 301358, 301359, 301360, 301355
- 7 os-windows rules with SIDs 301351, 301356, 301352, 301357, 301353, 301354, 300719
- 1 policy-other rule with SID 64279
- 10 server-webapp rules with SIDs 65593, 65323, 65587, 65082, 59513, 65570, 65568, 65586, 65569, 57921

Vulnerabilities

This release adds support and modifications for the detection of the following vulnerabilities:

- CVE-2022-29872: Improper Neutralization of Parameter/Argument Delimiters Vulnerability in Siemens SICAM T
  - Affected devices do not properly validate parameters of POST requests. This could allow an authenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.
- CVE-2022-29873: Improper Neutralization of Parameter/Argument Delimiters Vulnerability in Siemens SICAM T
  - Affected devices do not properly validate parameters of certain GET and POST requests. This could allow an unauthenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.
- CVE-2022-29874: Cleartext Transmission of Sensitive Information Vulnerability in Siemens SICAM T
  - Affected devices do not encrypt web traffic with clients but communicate in cleartext via HTTP. This could allow an unauthenticated attacker to capture the traffic and interfere with the functionality of the device.
- CVE-2022-29876: Cross-site Scripting Vulnerability in Siemens SICAM T

  - Affected devices do not properly handle the input of a GET request parameter. The provided argument is directly reflected in the web server response. This could allow an unauthenticated attacker to perform reflected XSS attacks.

- CVE-2022-29878: Authentication Bypass by Capture-replay Vulnerability in Siemens SICAM T
  - Affected devices use a limited range for challenges that are sent during the unencrypted challenge-response communication. An unauthenticated attacker could capture a valid challenge-response pair generated by a legitimate user, and request the webpage repeatedly to wait for the same challenge to reappear for which the correct response is known. This could allow the attacker to access the management interface of the device.
- CVE-2022-29879: Missing Authentication for Critical Function Vulnerability in Siemens SICAM T
  - The web based management interface of affected devices does not employ special access protection for certain internal developer views. This could allow authenticated users to access critical device information.
- CVE-2022-29880: Cross-site Scripting Vulnerability in Siemens SICAM T
  - Affected devices do not properly validate input in the configuration interface. This could allow an authenticated attacker to place persistent XSS attacks to perform arbitrary actions in the name of a logged user which accesses the affected views.
- CVE-2022-29881: Missing Authentication for Critical Function Vulnerability in Siemens SICAM T
  - The web based management interface of affected devices does not employ special access protection for certain internal developer views. This could allow unauthenticated users to extract internal configuration details.
- CVE-2022-29882: Cross-site Scripting Vulnerability in Siemens SICAM T
  - Affected devices do not handle uploaded files correctly. An unauthenticated attacker could take advantage of this situation to store an XSS attack, which could - when a legitimate user accesses the error logs - perform arbitrary actions in the name of the user.
- CVE-2022-29883: Improper Authentication Vulnerability in Siemens SICAM T
  - Affected devices do not restrict unauthenticated access to certain pages of the web interface. This could allow an attacker to delete log files without authentication.
- CVE-2022-40226: Session Fixation Vulnerability in Siemens SICAM T
  - Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user's session after login.
- CVE-2022-41665: Improper Neutralization of Parameter/Argument Delimiters Vulnerability in Siemens SICAM T
  - Affected devices do not properly validate the parameter of a specific GET request. This could allow an unauthenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.

- CVE-2022-43439: Improper Input Validation Vulnerability in Siemens SICAM T
  - Affected devices do not properly validate the Language-parameter in requests to the web interface on port 443/tcp. This could allow an authenticated remote attacker to crash the device (followed by an automatic reboot) or to execute arbitrary code on the device.
- CVE-2023-30901: Cross-Site Request Forgery Vulnerability in Siemens SICAM T
  - The web interface of the affected devices are vulnerable to Cross-Site Request Forgery attacks. By tricking an authenticated victim user to click a malicious link, an attacker could perform arbitrary actions on the device on behalf of the victim user.
- CVE-2023-31238: Incorrect Permission Assignment for Critical Resource Vulnerability in Siemens SICAM T
  - Affected devices are missing cookie protection flags when using the default settings. An attacker who gains access to a session token can use it to impersonate a legitimate application user.
- CVE-2024-56835: Improper Neutralization Vulnerability in Siemens RUGGEDCOM ROX
  - The DHCP Server configuration file of the affected products is subject to code injection. An attacker could leverage this vulnerability to spawn a reverse shell and gain root access on the affected system.
- CVE-2024-56836: Command Injection Vulnerability in Siemens RUGGEDCOM ROX
  - During the Dynamic DNS configuration of the affected product it is possible to inject additional configuration parameters. Under certain circumstances, an attacker could leverage this vulnerability to spawn a reverse shell and gain root access on the affected system.
- CVE-2024-56837: Command Injection Vulnerability in Siemens RUGGEDCOM ROX
  - Due to the insufficient validation during the installation and load of certain configuration files of the affected device, an attacker could spawn a reverse shell and gain root access on the affected system.
- CVE-2024-56838: Improper Neutralization Vulnerability in Siemens RUGGEDCOM ROX
  - The SCEP client available in the affected device for secure certificate enrollment lacks validation of multiple fields. An attacker could leverage this scenario to execute arbitrary code as root user.
- CVE-2024-56839: Improper Neutralization Vulnerability in Siemens RUGGEDCOM ROX
  - Code injection can be achieved when the affected device is using VRF (Virtual Routing and Forwarding). An attacker could leverage this scenario to execute arbitrary code as root user.
- CVE-2024-56840: Improper Neutralization Vulnerability in Siemens RUGGEDCOM ROX
  - Under certain conditions, IPsec may allow code injection in the affected device. An attacker could leverage this scenario to execute arbitrary code as root user.
- CVE-2025-40820: Improper Verification of Source of a Communication Channel in Siemens Interniche IP-Stack based Industrial Devices
  - Affected products do not properly enforce TCP sequence number validation in specific scenarios but accept values within a broad range. This could allow an unauthenticated remote attacker e.g.

  - to interfere with connection setup, potentially leading to a denial of service. The attack succeeds only if an attacker can inject IP packets with spoofed addresses at precisely timed moments, and it affects only TCP-based services.

- CVE-2025-40935: Improper Input Validation Vulnerability in Siemens Ruggedcom ROS devices
  - Affected devices do not properly validate input during the TLS certificate upload process of the web service. This could allow an authenticated remote attacker to trigger a device crash and reboot, leading to a temporary Denial of Service on the device.
- CVE-2025-40937: Command Injection Vulnerability in Siemens SIMATIC CN 4100
  - The affected application do not properly validate input parameters in its REST API, resulting in improper handling of unexpected arguments. This could allow an authenticated attacker to execute arbitrary code with limited privileges.
- CVE-2025-40938: Use of Hard-coded Credentials Vulnerability in Siemens SIMATIC CN 4100
  - The affected device stores sensitive information in the firmware. This could allow an attacker to access and misuse this information, potentially impacting the device's confidentiality, integrity, and availability.
- CVE-2025-40939: Improper Access Control Vulnerability in Siemens SIMATIC CN 4100
  - The affected device contains a USB port which allows unauthenticated connections. This could allow an attacker with physical access to the device to trigger reboot that could cause denial of service condition.
- CVE-2025-40940: Exposure of Sensitive Information Vulnerability in Siemens SIMATIC CN 4100
  - The affected application exhibits inconsistent SNMP behavior, such as unexpected service availability and unreliable configuration handling across protocol versions. This could allow an attacker to access sensitive data, potentially leading to a breach of confidentiality.
- CVE-2025-40941: Exposure of Sensitive Information Vulnerability in Siemens SIMATIC CN 4100
  - The affected devices exposes server information in its responses. This could allow an attacker with network access to gain useful information, increasing the likelihood of targeted attacks.
- CVE-2025-41692: Use of Weak Hash Vulnerability in Phoenix Contact FL SWITCH 2xxx series
  - A high privileged remote attacker with admin privileges for the webUI can brute-force the "root" and "user" passwords of the underlying OS due to a weak password generation algorithm
- CVE-2025-41693: Authenticated Denial-of-Service via SSH Vulnerability in Phoenix Contact FL SWITCH 2xxx series
  - A low privileged remote attacker can use the ssh feature to execute commands directly after login. The process stays open and uses resources which leads to a reduced performance of the management functions. Switching functionality is not affected.
- CVE-2025-41694: Authenticated Denial-of-Service via Webshell Vulnerability in Phoenix Contact FL SWITCH 2xxx series

    - A low privileged remote attacker can run the webshell with an empty command containing whitespace. The server will then block until it receives more data, resulting in a DoS condition of the websserver.

- CVE-2025-41695: Reflected XSS Vulnerability in Phoenix Contact FL SWITCH 2xxx series
    - A XSS vulnerability in dyn_conn.php can be used by an unauthenticated remote attacker to trick an authenticated user to send a manipulated POST request to the device in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is secured by the httpOnly Flag. Therefore an attacker is not able to take over the session of an authenticated user.
- CVE-2025-41696: Hardcoded User Password Vulnerability in Phoenix Contact FL SWITCH 2xxx series
    - An attacker can use an undocumented UART port on the PCB as a side-channel with the user hardcoded credentials obtained from CVE-2025-41692 to gain read access to parts of the filesystem of the device.
- CVE-2025-41697: Shell access to UART Console Vulnerability in Phoenix Contact FL SWITCH 2xxx series
    - An attacker can use an undocumented UART port on the PCB as a side-channel to get root access e.g. with the credentials obtained from CVE-2025-41692.
- CVE-2025-9368: Denial-of-Service Vulnerability in Rockwell 432ES-IG3 Series A
    - A security issue exists within 432ES-IG3 Series A, which affects GuardLink® EtherNet/IP Interface, resulting in denial-of-service. A manual power cycle is required to recover the device.

20251205

Snort rules

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

- **Talos Rules 2025-12-04 (https://www.snort.org/advisories/talos-rules-2025-12-04-12-4-2025)**
- **Talos Rules 2025-12-04 (https://www.snort.org/advisories/talos-rules-2025-12-04)**
- **Talos Rules 2025-12-02 (https://www.snort.org/advisories/talos-rules-2025-12-02)**

The new and updated Snort rules span the following categories:

- 1 browser-webkit rule with SID 65553
- 4 malware-cnc rules with SIDs 65541, 65540, 65551, 65548
- 1 policy-other rule with SID 65542

- 10 server-webapp rules with SIDs 65544, 65554, 65547, 65545, 65546, 65550, 65543, 65549, 65552, 65539