



Release Notes for Cisco Cyber Vision Knowledge DB

Release 202511

<i>Compatible device list</i>	2
<i>Links</i>	2
Software Download	2
Related Documentation	3
<i>Database download</i>	3
<i>How to update the database</i>	3
<i>Release contents</i>	4
20251128	4
Snort rules	4
20251121	4
Snort rules	4
Vendor Database.....	4
20251114	4
Snort rules	5
Vulnerabilities	5
Vendor Database.....	10
20251107	10
Snort rules	10
Vendor Database.....	11

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.202511	Description
CiscoCyberVision_knowledgedb_20251107.db	Knowledge DB version 20251107
CiscoCyberVision_knowledgedb_20251114.db	Knowledge DB version 20251114
CiscoCyberVision_knowledgedb_20251121.db	Knowledge DB version 20251121
CiscoCyberVision_knowledgedb_20251128.db	Knowledge DB version 20251128

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

20251128

Snort rules

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

- **Talos Rules 2025-11-25** (<https://www.snort.org/advisories/talos-rules-2025-11-25>)

The new and updated Snort rules span the following categories:

- 1 policy-other rule with SID 65537
- 2 server-webapp rules with SIDs 65538, 58708

20251121

Snort rules

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

- **Talos Rules 2025-11-20** (<https://www.snort.org/advisories/talos-rules-2025-11-20>)
- **Talos Rules 2025-11-18** (<https://www.snort.org/advisories/talos-rules-2025-11-18>)

The new and updated Snort rules span the following categories:

- 1 file-image rule with SID 301350
- 2 file-other rules with SIDs 53491, 301349
- 2 malware-cnc rules with SIDs 65533, 65534
- 1 policy-other rule with SID 65525
- 8 server-webapp rules with SIDs 65529, 65524, 64895, 65523, 65532, 65528, 65527, 65526

Vendor Database

The new UI in Cyber Vision relies on a vendor database included in this Knowledge Base to represent physical assets and give them a type. This release adds initial typing support for assets from Palo Alto, Prosoft and SEL. It also improves support for assets from ABB, Rockwell and SICK.

20251114

Snort rules

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

- **Talos Rules 2025-11-13** (<https://www.snort.org/advisories/talos-rules-2025-11-13>)
- **Talos Rules 2025-11-11** (<https://www.snort.org/advisories/talos-rules-2025-11-11>)

The new and updated Snort rules span the following categories:

- 2 malware-cnc rules with SIDs 65502, 65513
- 1 malware-other rule with SID 65512
- 5 os-windows rules with SIDs 301344, 301343, 301345, 301348, 301347
- 3 policy-other rules with SIDs 65494, 65514, 65515
- 5 server-other rules with SIDs 65506, 65519, 65520, 65522, 65521
- 12 server-webapp rules with SIDs 65517, 301346, 65492, 65503, 65495, 65490, 65511, 65516, 65491, 65518, 60117, 65493

Vulnerabilities

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

- CVE-2017-7928: Improper Access Control in Schweitzer Engineering Laboratories SEL-3620 and SEL-3622 products.
 - An Improper Access Control issue was discovered in Schweitzer Engineering Laboratories (SEL) SEL-3620 and SEL-3622 Security Gateway Versions R202 and, R203, R203-V1, R203-V2 and, R204, R204-V1. The device does not properly enforce access control while configured for NAT port forwarding, which may allow for unauthorized communications to downstream devices.
- CVE-2023-2264: Improper input validation could lead to code injection in Schweitzer Engineering Laboratories SEL-411L product.
 - An improper input validation vulnerability in the Schweitzer Engineering Laboratories SEL-411L could allow a malicious actor to manipulate authorized users to click on a link that could allow undesired behavior.
- CVE-2023-2265: Improper restriction of rendered UI layers or frames could lead to clickjacking attack in Schweitzer Engineering Laboratories SEL-411L product.
 - An Improper Restriction of Rendered UI Layers or Frames in the Schweitzer Engineering Laboratories SEL-411L could allow an unauthenticated attacker to perform clickjacking based attacks against an authenticated and authorized user.
- CVE-2023-2266: Improper neutralization of input during web page generation could lead to cross-site scripting based attacks in Schweitzer Engineering Laboratories SEL-411L product.

- An Improper neutralization of input during web page generation in the Schweitzer Engineering Laboratories SEL-411L could allow an attacker to generate cross-site scripting based attacks against an authorized and authenticated user.
- CVE-2023-2267: Improper input validation could lead to reflection injection attacks in Schweitzer Engineering Laboratories SEL-411L product.
 - An Improper Input Validation vulnerability in Schweitzer Engineering Laboratories SEL-411L could allow an attacker to perform reflection attacks against an authorized and authenticated user.
- CVE-2023-2310: Channel Accessible by Non-Endpoint in Schweitzer Engineering Laboratories SEL RTAC product.
 - A Channel Accessible by Non-Endpoint vulnerability in the Schweitzer Engineering Laboratories SEL Real-Time Automation Controller (RTAC) could allow a remote attacker to perform a man-in-the-middle (MiTM) that could result in denial of service.
- CVE-2023-31148: Improper Input Validation in Web Interface in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Input Validation vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to execute arbitrary code.
- CVE-2023-31149: Improper Input Validation in Web Interface in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Input Validation vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to execute arbitrary code.
- CVE-2023-31150: Storing Passwords in a Recoverable Format in Schweitzer Engineering Laboratories SEL RTAC product.
 - A Storing Passwords in a Recoverable Format vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) database system could allow an authenticated attacker to retrieve passwords.
- CVE-2023-31151: Improper Certificate Validation in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Certificate Validation vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote unauthenticated attacker to conduct a man-in-the-middle (MitM) attack.
- CVE-2023-31152: Authentication Bypass Using an Alternate Path or Channel in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Authentication Bypass Using an Alternate Path or Channel vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface allows Authentication Bypass.

- CVE-2023-31153: Improper Neutralization of Input During Web Page Generation in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code. See SEL Service Bulletin dated 2022-11-15 for more details.
- CVE-2023-31154: Improper Neutralization of Input During Web Page Generation in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code.
- CVE-2023-31155: Improper Neutralization of Input During Web Page Generation in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code.
- CVE-2023-31156: Improper Neutralization of Input During Web Page Generation in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code.
- CVE-2023-31157: Improper Neutralization of Input During Web Page Generation in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code.
- CVE-2023-31158: Improper Neutralization of Input During Web Page Generation in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code.
- CVE-2023-31159: Improper Neutralization of Input During Web Page Generation in Schweitzer Engineering Laboratories SEL RTAC product.

- An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code.
- CVE-2023-31160: Improper Neutralization of Input During Web Page Generation in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code.
- CVE-2023-31161: Improper Input Validation in Web Interface in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Input Validation vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow an authenticated remote attacker to use internal resources, allowing a variety of potential effects.
- CVE-2023-31162: Improper Input Validation in Web Interface in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Input Validation vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to arbitrarily alter the content of a configuration file.
- CVE-2023-31163: Improper Neutralization of Input During Web Page Generation in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code.
- CVE-2023-31164: Improper Neutralization of Input During Web Page Generation in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code.
- CVE-2023-31165: Improper Neutralization of Input During Web Page Generation in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to inject and execute arbitrary script code.

- CVE-2023-31166: Improper Limitation of a Pathname to a Restricted Directory in Schweitzer Engineering Laboratories SEL RTAC product.
 - An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to create folders in arbitrary paths of the file system.
- CVE-2023-31176: Insufficient entropy vulnerability could lead to authentication bypass in Schweitzer Engineering Laboratories SEL-451 product.
 - An Insufficient Entropy vulnerability in the Schweitzer Engineering Laboratories SEL-451 could allow an unauthenticated remote attacker to brute-force session tokens and bypass authentication.
- CVE-2023-31177: Improper neutralization of input could lead to execution of arbitrary code in Schweitzer Engineering Laboratories SEL-451 product.
 - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in the Schweitzer Engineering Laboratories SEL-451 could allow an attacker to craft a link that could execute arbitrary code on a victim's system.
- CVE-2023-34388: Improper authentication could lead to session hijacking in Schweitzer Engineering Laboratories SEL-451 product.
 - An Improper Authentication vulnerability in the Schweitzer Engineering Laboratories SEL-451 could allow a remote unauthenticated attacker to potentially perform session hijacking attack and bypass authentication.
- CVE-2023-34389: Allocation of resources without limits could lead to denial of service in Schweitzer Engineering Laboratories SEL-451 product.
 - An allocation of resources without limits or throttling vulnerability in the Schweitzer Engineering Laboratories SEL-451 could allow a remote authenticated attacker to make the system unavailable for an indefinite amount of time.
- CVE-2023-34390: Improper input validation could lead to denial of service in Schweitzer Engineering Laboratories SEL-451 product.
 - An input validation vulnerability in the Schweitzer Engineering Laboratories SEL-451 could allow a remote authenticated attacker to create a denial of service against the system and locking out services.
- CVE-2024-2103: Inclusion of Undocumented Features in Schweitzer Engineering Laboratories various products.
 - Inclusion of undocumented features vulnerability accessible when logged on with a privileged access level on the following Schweitzer Engineering Laboratories relays could allow the relay to behave unpredictably: SEL-700BT Motor Bus Transfer Relay, SEL-700G Generator Protection Relay, SEL-710-5 Motor Protection Relay, SEL-751 Feeder Protection Relay, SEL-787-2/-3/-4 Transformer Protection Relay, SEL-787Z High-Impedance Differential Relay
- CVE-2025-40815: Classic Buffer Overflow Vulnerability in Siemens LOGO! 8 BM Devices

- Affected devices do not properly validate the structure of TCP packets in several methods. This could allow an attacker to cause buffer overflows, get control over the instruction counter and run custom code.
- CVE-2025-40816: Missing Authentication for Critical Function Vulnerability in Siemens LOGO! 8 BM Devices
 - Affected devices do not conduct certain validations when interacting with them. This could allow an unauthenticated remote attacker to manipulate the devices IP address, which means the device would not be reachable.
- CVE-2025-40817: Missing Authentication for Critical Function Vulnerability in Siemens LOGO! 8 BM Devices
 - Affected devices do not conduct certain validations when interacting with them. This could allow an unauthenticated remote attacker to change time of the device, which means the device could behave differently.
- CVE-2023-31238: Incorrect Permission Assignment for Critical Resource in Siemens SICAM P850 and SICAM P855 Devices
 - 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-2023-30901: Cross-Site Request Forgery Vulnerability in Siemens SICAM P850 and SICAM P855 Devices
 - 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.

Vendor Database

The new UI in Cyber Vision relies on a vendor database included in this Knowledge Base to represent physical assets and give them a type. This release adds initial typing support for assets from Danfoss, Fanuc, and SMC . It also improves support for assets from ABB, Atlas Copco, Cognex, Festo, HMS, Keyence, Rockwell, SICK, Siemens, and TURCK.

20251107

Snort rules

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

- **Talos Rules 2025-11-06** (<https://www.snort.org/advisories/talos-rules-2025-11-06>)
- **Talos Rules 2025-11-04** (<https://www.snort.org/advisories/talos-rules-2025-11-04>)

The new and updated Snort rules span the following categories:

- 4 file-office rules with SIDs 65487, 65488, 65485, 65486
- 2 malware-other rules with SIDs 65480, 65479
- 2 os-windows rules with SIDs 46503, 301342
- 1 policy-other rule with SID 65489
- 13 server-webapp rules with SIDs 65484, 301340, 65478, 65477, 65459, 55639, 65481, 55640, 55637, 65473, 55638, 301341, 65474

Vendor Database

The new UI in Cyber Vision relies on a vendor database included in this Knowledge Base to represent physical assets and give them a type. This release adds initial typing support for assets from ABB, Atlas Copco, Cognex, and Festo. It also improves support for assets from Turck.