Release Notes for Cisco Cyber Vision Knowledge DB

Release 202610

Compatible device list 2

Links 2

Software Download 2

Related Documentation 3

Database download 3

How to update the database 3

Release contents 4

20261030 4

Snort rules 4

Vulnerabilities 4

20261023 5

Snort rules 5

Vulnerabilities 5

Vendor Database 7

20261016 7

Snort rules 7

Vulnerabilities 7

20261009 10

Snort rules 10

Vulnerabilities 11

20261002 14

Snort rules 14

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-5.6.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.6.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.6.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.6.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.6.1.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.6.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.6.1.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.6.1.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.6.1.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.6.1.dat	Knowledge DB embedded in Cisco Cyber Vision 5.6.1
Updates/KDB/KDB.202610	**Description**
CiscoCyberVision_knowledgedb_20261002.db	Knowledge DB version 20261002
CiscoCyberVision_knowledgedb_20261009.db	Knowledge DB version 20261009
CiscoCyberVision_knowledgedb_20261016.db	Knowledge DB version 20261016
CiscoCyberVision_knowledgedb_20261023.db	Knowledge DB version 20261023
CiscoCyberVision_knowledgedb_20261030.db	Knowledge DB version 20261030

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

20261030

Snort rules

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

- **Talos Rules 2026-10-28 (https://www.snort.org/advisories/talos-rules-2026-10-28)**
- **Talos Rules 2026-10-27 (https://www.snort.org/advisories/talos-rules-2026-10-27)**

The new and updated Snort rules span the following categories:

- 2 browser-webkit rules with SIDs 67417, 67418
- 33 malware-cnc rules with SIDs 61, 47, 58, 67, 73, 48, 55, 69, 72, 67386, 63, 51, 44, 70, 54, 59, 52, 46, 71, 43, 57, 60, 56, 53, 68, 65, 50, 64, 49, 45, 62, 66, 67385
- 1 malware-other rule with SID 301726
- 1 policy-other rule with SID 67380
- 11 server-webapp rules with SIDs 67421, 67360, 67420, 67422, 67379, 67375, 67419, 67377, 67382, 67376, 67381

Vulnerabilities

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

Moxa

- CVE-2026-111460: Static HTTPS Private Key and CA Private Key in OnCell G3150A-LTE Series
  - A remote unauthenticated attacker may obtain shared HTTPS/CA keys and impersonate affected devices whose keys have not been regenerated.
- CVE-2026-111461: OS Command Injection Vulnerability in OnCell G3150A-LTE Series
  - A remote attacker with the required privileges can inject operating-system commands when SMS management is enabled and configured.
- CVE-2026-111548: Stack Buffer Overflow Vulnerability in Moxa Wireless Device Servers
  - A low-privileged authenticated attacker can make the web management service unresponsive. A power cycle restores service; other device functions remain operational.

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 improves support for assets from Omron.

20261023

Snort rules

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

- **Talos Rules 2026-10-21 (https://www.snort.org/advisories/talos-rules-2026-10-21-10-21-2026)**
- **Talos Rules 2026-10-21 (https://www.snort.org/advisories/talos-rules-2026-10-21)**
- **Talos Rules 2026-10-20 (https://www.snort.org/advisories/talos-rules-2026-10-20)**
- **Talos Rules 2026-10-16 (https://www.snort.org/advisories/talos-rules-2026-10-16)**

The new and updated Snort rules span the following categories:

- 13 file-other rules with SIDs 301725, 67346, 67348, 67338, 67344, 67339, 67341, 67349, 67345, 67342, 67340, 67347, 67343
- 1 malware-cnc rule with SID 42
- 2 policy-other rules with SIDs 61192, 67352
- 1 protocol-snmp rule with SID 67357
- 13 server-other rules with SIDs 67368, 67369, 67371, 67372, 67370, 67374, 67363, 67365, 67367, 67366, 67373, 67364, 67358
- 9 server-webapp rules with SIDs 67360, 67353, 67375, 67359, 67166, 67351, 67361, 67362, 67356

Vulnerabilities

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

Cisco

- CVE-2026-20011: Cisco Snort 3 SMTP MIME Denial of Service Vulnerability
  - Crafted SMTP MIME headers can restart the Snort 3 detection engine.
- CVE-2026-20019: Cisco Snort 3 NetFlow Denial of Service Vulnerability
  - Crafted UDP NetFlow packets can restart the detection engine and interrupt packet inspection.
- CVE-2026-20043: Out-of-bounds Write Vulnerabilities in Cisco Snort 3
  - Internally discovered out-of-bounds write flaws are addressed by Cisco’s Snort 3 security hardening release.
- CVE-2026-20179: Cisco Snort 3 GRE Denial of Service Vulnerability
  - Crafted GRE packets can restart the detection engine and interrupt packet inspection.
- CVE-2026-20197: Cisco Snort 3 Teredo Protocol Denial of Service Vulnerability
  - Crafted Teredo packets can restart the detection engine and interrupt packet inspection.

- CVE-2026-20218: Cisco Snort 3 VBA Decompression Buffer Overflow Denial of Service Vulnerability
  - Crafted VBA data can trigger a stack buffer overflow during decompression and restart the detection engine.
- CVE-2026-20221: Cisco Snort 3 GRE Tunnel Decapsulation Denial of Service Vulnerability
  - Crafted GRE traffic can trigger an unexpected detection-engine restart and denial of service.
- CVE-2026-20236: Incorrect Calculation Vulnerabilities in Cisco Snort 3
  - Internally discovered calculation flaws are addressed by Cisco's Snort 3 security hardening release.
- CVE-2026-20291: Improper Privilege Management Vulnerabilities in Cisco Snort 3
  - Privilege-management weaknesses are addressed by Cisco's Snort 3 security hardening release.
- CVE-2026-20356: Uncontrolled Resource Consumption Vulnerabilities in Cisco Snort 3
  - Resource-consumption weaknesses are addressed by Cisco's Snort 3 security hardening release.
- CVE-2026-76445: Cisco Snort 3 GTP Processing Denial of Service Vulnerability
  - Crafted GTP packets can restart the detection engine and interrupt packet inspection.
- CVE-2026-76505: Cisco IOS XR ASR 9000 IPv4 Unicast Packets Denial of Service Vulnerability
  - Crafted IPv4 traffic addressed to affected router interfaces can cause network-processor errors and line-card resets or shutdown.

Moxa

- CVE-2026-109812: Missing Authorization on Secret Endpoints in Moxa AIG-302 Series
  - A low-privileged adjacent attacker can retrieve sensitive information, including cryptographic key material, through insufficiently protected APIs.
- CVE-2026-109813: Shared Hard-coded Root CA Private Key in Moxa AIG-302 Series
  - A shared hard-coded private key can allow an unauthenticated adjacent attacker to compromise communication confidentiality and integrity.

Siemens

- CVE-2026-44414: Path Traversal Vulnerability in Siemens SCALANCE and SIMATIC Industrial Edge Devices
  - An authenticated remote attacker can access sensitive internal information and potentially facilitate unauthorized system access.
- CVE-2026-44415: Path Traversal Vulnerability in Siemens SIMATIC and SIPLUS HMI Unified Comfort Panels
  - An authenticated remote attacker can access sensitive information, potentially facilitating unauthorized system access or deletion of data.
- CVE-2026-89208: Out-of-bounds Read Vulnerability in Siemens Desigo PXC/PXM Devices
  - An unauthenticated remote attacker can trigger memory reads outside intended packet boundaries.

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 improves support for assets from Schneider.

20261016

Snort rules

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

- **Talos Rules 2026-10-15 (https://www.snort.org/advisories/talos-rules-2026-10-15)**
- **Talos Rules 2026-10-13 (https://www.snort.org/advisories/talos-rules-2026-10-13)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 301716
- 1 file-other rule with SID 301707
- 11 malware-cnc rules with SIDs 10, 34, 33, 36, 39, 40, 35, 37, 38, 67335, 41
- 4 malware-other rules with SIDs 301723, 301721, 301720, 301722
- 3 os-linux rules with SIDs 301698, 67205, 67204
- 56 os-windows rules with SIDs 301678, 301684, 301705, 301665, 301709, 301718, 301708, 301669, 301685, 301671, 301696, 301702, 301681, 301694, 301664, 301683, 301667, 301717, 301670, 301673, 301699, 301697, 301712, 301695, 301680, 301675, 301677, 301691, 301674, 301719, 301689, 301713, 301711, 301668, 301692, 301704, 301686, 301676, 301663, 301693, 301715, 301724, 301703, 301714, 301706, 301710, 301688, 301700, 301679, 301701, 301690, 301672, 301687, 301666, 301682, 33053
- 1 policy-other rule with SID 67312
- 1 protocol-dns rule with SID 32959
- 5 server-webapp rules with SIDs 67323, 67324, 67209, 67207, 67208

Vulnerabilities

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

Cisco

- CVE-2026-15579: Out-of-bounds Write Vulnerability in Moxa TN-4500B Series
  - An overly long username can trigger a buffer overflow and crash the authentication process.
- CVE-2026-20032: Cisco NX-OS Software Python Sandbox Escape Vulnerability
  - An authenticated low-privileged attacker can escape the Python sandbox and execute commands on the underlying operating system.

- CVE-2026-20173: Cisco NX-OS Software Control Plane Denial of Service Vulnerability
    - A high rate of UDP or TCP connections can exhaust resources and disrupt routing and control-plane protocols.
- CVE-2026-76453: Improper Neutralization Vulnerability in Cisco NX-OS Software
    - Command, operating-system, and argument injection issues can affect confidentiality, integrity, and availability.
- CVE-2026-76455: Improper Access Control Vulnerability in Cisco NX-OS Software
    - Authentication, authorization, privilege, and bypass weaknesses can expose protected functionality.
- CVE-2026-76456: Improper Input Validation Vulnerability in Cisco NX-OS Software
    - Improper input, path, and external-path validation can cause high-impact availability issues.
- CVE-2026-76457: Out-Of-Bounds Read Vulnerability in Cisco NX-OS Software
    - Out-of-bounds reads can expose sensitive information and affect availability.
- CVE-2026-76458: Improper Handling of Exceptional Conditions Vulnerability in Cisco NX-OS Software
    - Uncaught exceptions and reachable assertions can cause denial of service.
- CVE-2026-76459: Out-Of-Bounds Write Vulnerability in Cisco NX-OS Software
    - Buffer overflows and incorrect buffer-size calculations can enable high-impact compromise.
- CVE-2026-76465: Cisco Nexus 3000 and 9000 Series Switches MPLS OAM Remote Code Execution Vulnerability
    - A crafted MPLS echo-request packet can enable arbitrary code execution with root privileges or cause a device reload.
- CVE-2026-76471: Cisco NX-OS Software NX-API Remote Code Execution Vulnerability
    - A crafted HTTP request to NX-API can enable arbitrary code execution with root privileges or cause denial of service.
- CVE-2026-76485: Cisco Nexus 3000 and 9000 Series Switches NGOAM Remote Code Execution Vulnerabilities
    - Crafted packets sent while NGOAM is enabled can enable code execution with root privileges or cause denial of service.
- CVE-2026-76486: Cisco Nexus 3000 and 9000 Series Switches NGOAM Remote Code Execution Vulnerabilities
    - Crafted packets sent while NGOAM is enabled can enable code execution with root privileges or cause denial of service.
- CVE-2026-76501: Cisco Nexus 3000 and 9000 Series Switches NGOAM Remote Code Execution Vulnerabilities

    - Crafted packets sent while NGOAM is enabled can enable code execution with root privileges or cause denial of service.

Rockwell Automation

- CVE-2026-12655: Authentication Bypass Vulnerability in Rockwell Automation 1732E ArmorBlock I/O
    - An unauthenticated attacker can change the web-server password and potentially take over the administrator account.
- CVE-2026-12656: Denial-of-Service Vulnerability in Rockwell Automation 1732E ArmorBlock I/O
    - Network storm traffic can interrupt communication and fault the device, requiring a power cycle for recovery.

Schneider Electric

- CVE-2026-96434: Use of Unmaintained Third-Party Components in Schneider Electric Pro-face STW6000 and Harmony STW6
    - Unmaintained components could allow unauthorized control when a user visits a malicious webpage from the HMI.
- CVE-2026-102250: Insufficient Firmware Authenticity Verification in Schneider Electric SAGE RTU
    - Insufficient firmware verification could allow modified firmware to be installed and give an attacker control of the device.

Siemens

- CVE-2024-7322: Improper Verification of Source of a Communication Channel Vulnerability in Siemens SENTRON 3NA COM Fuse
    - An authenticated network attacker can alter the device node ID and cause a denial of service.
- CVE-2026-72895: Use of Default Cryptographic Key Vulnerability in Siemens SIMATIC IPCs
    - A vendor test key in the UEFI Secure Boot database can allow an attacker to bypass Secure Boot protections.
- CVE-2026-102073: Integer Underflow Vulnerability in Siemens APOGEE, TALON and Desigo PXC/PXM Products
    - Improper input-length validation can expose device memory or cause denial of service.
- CVE-2026-102074: Stack-based Buffer Overflow Vulnerability in Siemens APOGEE, TALON and Desigo PXC/PXM Products
    - Improper FTP input validation can allow an unauthenticated attacker to cause denial of service.
- CVE-2026-102075: Stack-based Buffer Overflow Vulnerability in Siemens APOGEE, TALON and Desigo PXC/PXM Products
    - Improper multipart-input validation can allow an unauthenticated attacker to cause denial of service.

- CVE-2026-102076: Stack-based Buffer Overflow Vulnerability in Siemens APOGEE, TALON and Desigo PXC/PXM Products
    - Improper upload-input validation can allow an unauthenticated attacker to cause denial of service.
- CVE-2026-63350: Eval Injection Vulnerability in Siemens SIMATIC S7 PLCs Web Server
    - Crafted trace files can execute attacker-controlled JavaScript in an authorized user's browser and perform PLC operations.
- CVE-2026-63351: Cross-site Scripting Vulnerability in Siemens SIMATIC S7 PLCs Web Server
    - Crafted CSV trace-file data can execute attacker-controlled JavaScript in an authorized user's browser.
- CVE-2026-63352: Cross-site Scripting Vulnerability in Siemens SIMATIC S7 PLCs Web Server
    - Crafted calculated-signal data can execute attacker-controlled JavaScript in an authorized user's browser.
- CVE-2026-63353: Cross-site Scripting Vulnerability in Siemens SIMATIC S7 PLCs Web Server
    - Crafted comment fields in trace files can execute attacker-controlled JavaScript and perform PLC operations.
- CVE-2026-63354: Cross-site Scripting Vulnerability in Siemens SIMATIC S7 PLCs Web Server
    - Crafted visual-marker data can execute attacker-controlled JavaScript and perform PLC operations.
- CVE-2026-63355: Cross-site Scripting Vulnerability in Siemens SIMATIC S7 PLCs Web Server
    - Crafted signal names can execute attacker-controlled JavaScript in an authorized user's browser.
- CVE-2026-63356: Cross-site Scripting Vulnerability in Siemens SIMATIC S7 PLCs Web Server
    - Crafted calculated-signal names can execute attacker-controlled JavaScript through displayed error messages.
- CVE-2026-63357: Cross-site Scripting Vulnerability in Siemens SIMATIC S7 PLCs Web Server
    - Crafted calculated-signal files can execute attacker-controlled JavaScript in an authorized user's browser.

20261009

Snort rules

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

- **Talos Rules 2026-10-08 (https://www.snort.org/advisories/talos-rules-2026-10-08)**
- **Talos Rules 2026-10-06 (https://www.snort.org/advisories/talos-rules-2026-10-06)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rules with SIDs 301662

- 2 file-other rules with SIDs 67182, 67181
- 1 malware-cnc rules with SIDs 31
- 3 policy-other rules with SIDs 67202, 63753, 67203
- 15 server-webapp rules with SIDs 67190, 67200, 67189, 67187, 67197, 67191, 67183, 67194, 67201, 67193, 67185, 67188, 67186, 67184, 67192

Vulnerabilities

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

Moxa

- CVE-2026-15579: Out-of-bounds Write Vulnerability in Moxa TN-4500B Series
  - An overly long username can trigger a buffer overflow and crash the authentication process.
- CVE-2026-86325: Stack-based Buffer Overflow Vulnerability in Moxa MGate Protocol Gateways
  - An improperly validated account name can corrupt execution flow, expose credentials, or disrupt availability.
- CVE-2026-86326: Improper Firmware Signature Verification Vulnerability in Moxa MGate Protocol Gateways
  - An attacker with access to the update interface could install a crafted firmware image and execute unauthorized code.

Rockwell Automation

- CVE-2025-12768: Out-of-Bounds Write Vulnerability in Rockwell Automation FactoryTalk Historian Machine Edition
  - An authenticated attacker could exploit the vulnerability to achieve remote code execution.
- CVE-2026-12661: Denial-of-Service Vulnerability in Rockwell Automation FactoryTalk Historian Machine Edition
  - Crafted requests sent by an authenticated adjacent attacker can cause buffer overflows and make the device unresponsive.
- CVE-2016-9334: Cleartext Transmission of Credentials Vulnerability in Rockwell MicroLogix 1100 and 1400 Controllers
  - User credentials are transmitted in clear text and may be exposed to an attacker observing network traffic.
- CVE-2016-9338: Incorrect Permission Assignment Vulnerability in Rockwell MicroLogix 1100 and 1400 Controllers
  - An administrator may remove all administrative users, requiring a factory reset to restore web-server functionality.

- CVE-2023-1834: Open Port Exposure Vulnerability in Rockwell Kinetix 5500 Drives
    - Telnet and FTP ports may be open by default, potentially allowing unauthorized device access.
- CVE-2023-2072: Cross-Site Scripting Vulnerability in Rockwell PowerMonitor 1000
    - Stored cross-site scripting can enable attacks against authenticated users, potentially leading to remote code execution.
- CVE-2024-12371: Remote Code Execution Vulnerability in Rockwell PowerMonitor 1000
    - An unauthenticated attacker can create a highly privileged user through the API and take control of the device.
- CVE-2024-12372: Denial-of-Service Vulnerability in Rockwell PowerMonitor 1000
    - Heap-memory corruption may allow remote code execution or cause a denial of service
- CVE-2024-12373: Denial-of-Service Vulnerability in Rockwell PowerMonitor 1000
    - A buffer overflow can cause a denial of service.
- CVE-2024-40619: Malformed Packet Denial-of-Service Vulnerability in Rockwell ControlLogix and GuardLogix 5580 Controllers
    - A malformed CIP packet can cause a major non-recoverable fault and denial of service.
- CVE-2024-6089: PTP Packet Denial-of-Service Vulnerability in Rockwell 5015-AENFTXT Adapters
    - A manipulated PTP packet can trigger a major non-recoverable fault and require a power cycle.
- CVE-2024-7507: Input Validation Denial-of-Service Vulnerability in Rockwell CompactLogix and ControlLogix Controllers
    - A malformed PCCC message can cause the controller to fault.
- CVE-2024-7567: CIP and Modbus Denial-of-Service Vulnerability in Rockwell Micro850 and Micro870 Controllers
    - Exploitation can temporarily disrupt CIP/Modbus communications.
- CVE-2025-8008: Crafted Forward Close Message Denial-of-Service Vulnerability in Rockwell 1756-EN4TR and 1756-EN4TRXT Modules
    - Crafted messages during a Forward Close operation can cause the device to crash.

Schneider Electric

- CVE-2026-77120: OS Command Injection Vulnerability in Schneider Electric PowerLogic T300
    - An authenticated SSH user can escalate privileges and execute unauthorized administrative commands.
- CVE-2026-81861: Insufficiently Protected Credentials Vulnerability in Schneider Electric SCADAPack x70 Products

    - Exposed authentication information could permit unauthorized access to SCADAPack RTU functionality.
- CVE-2026-3869: Incorrect Authentication Algorithm Implementation Vulnerability in Schneider Electric Modicon M580 and M580 Safety
    - An incorrectly implemented authentication algorithm can compromise confidentiality, integrity, and availability.
- CVE-2016-2278: OS Command Injection in Schneider Electric Automation Server AS and AS-P
    - An authenticated administrator can bypass Minimal Shell controls and execute arbitrary operating-system commands.
- CVE-2024-5557: Sensitive Information in Log Files in Schneider Electric SpaceLogic AS-P and AS-B
    - Controller logs may expose SNMP credentials to an attacker with log access.
- CVE-2024-5558: TOCTOU Race Condition in Schneider Electric SpaceLogic AS-P and AS-B
    - A limited administrator account can be abused for privilege escalation through a time-of-check/time-of-use race condition.

Siemens

- CVE-2026-62645: Missing Authentication for Critical Function Vulnerability in Siemens Reyrolle 7SR5
    - Session-ID information can be used to bypass authentication and gain unauthorized access.
- CVE-2026-62646: Insufficient Entropy Vulnerability in Siemens Reyrolle 7SR5
    - Predictable session identifiers can be brute-forced to bypass authentication.
- CVE-2026-62647: Improper Input Validation Vulnerability in Siemens Reyrolle 7SR5
    - Predictable security-sensitive values can allow an attacker to impersonate an authenticated user.
- CVE-2026-62648: Out-of-bounds Write Vulnerability in Siemens Reyrolle 7SR5
    - Improper URL-length validation can cause an out-of-bounds write, crashing and rebooting the device.
- CVE-2026-62649: Allocation of Resources Without Limits or Throttling Vulnerability in Siemens Reyrolle 7SR5
    - Unauthenticated HTTP requests can exhaust resources and crash the device.
- CVE-2026-62650: Authentication Bypass Using an Alternate Path or Channel Vulnerability in Siemens Reyrolle 7SR5
    - A low-privileged attacker can manipulate web-management requests to obtain administrative privileges.
- CVE-2026-62652: Insertion of Sensitive Information Into Debugging Code Vulnerability in Siemens Reyrolle 7SR5

    - Public firmware files containing debugging symbols can facilitate reverse engineering and vulnerability research.
- CVE-2026-62653: Out-of-bounds Write Vulnerability in Siemens Reyrolle 7SR5
    - Improper validation of proprietary-protocol input can corrupt memory, crash the device, or enable code execution.
- CVE-2026-62654: Download of Code Without Integrity Check Vulnerability in Siemens Reyrolle 7SR5
    - Maintenance mode can execute code downloaded from a network server without verifying its authenticity or integrity.
- CVE-2026-89207: Improper Validation of Specified Type of Input Vulnerability in Siemens WTV676 and WTV776 Devices
    - Invalid backend-service input can force the device into protection mode and disable remote Web Access.
- CVE-2026-54798: Active Debug Code Vulnerability in Siemens SICAM 8 Products
    - An exposed HTTP debugging interface can be abused to crash the web process.
- CVE-2026-54799: Active Debug Code Vulnerability in Siemens SICAM 8 Products
    - Insufficient firmware-signature validation can allow installation of malicious firmware.
- CVE-2026-54800: Initialization of a Resource with an Insecure Default Vulnerability in Siemens SICAM 8 Products
    - OPC UA security mechanisms are disabled by default, potentially allowing unauthorized access to critical device functions.
- CVE-2026-54801: Unverified Password Change Vulnerability in Siemens SICAM 8 Products
    - Insufficient validation during administrative account changes can allow privilege escalation.

Schweitzer Engineering Laboratories

- PVT-2026-00009: Session Hijacking Vulnerability in Web Server on Schweitzer Engineering Laboratories SEL-751 Feeder Protection Relays
    - A weakness in the web server could allow an attacker to hijack a web user's session. The issue is fixed in SEL-751 firmware R302-V9.

20261002

Snort rules

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

- **Talos Rules 2026-10-01 (https://www.snort.org/advisories/talos-rules-2026-10-01)**

- **Talos Rules 2026-09-29 (https://www.snort.org/advisories/talos-rules-2026-09-29)**
- **Talos Rules 2026-09-24 (https://www.snort.org/advisories/talos-rules-2026-09-24)**

The new and updated Snort rules span the following categories:

- 4 os-other rules with SIDs 67171, 67170, 67169, 67168
- 2 policy-other rules with SIDs 67161, 67162
- 2 protocol-rpc rules with SIDs 67156, 67155
- 2 server-other rules with SIDs 67154, 67165
- 18 server-webapp rules with SIDs 67153, 65229, 67166, 67177, 67173, 67178, 67174, 67172, 67176, 67175, 67157, 67179, 67164, 67163, 67159, 67158, 67160, 67180