Release Notes for Cisco Cyber Vision Knowledge DB

Release 202502

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-5.1.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.1.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.1.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.1.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.1.1.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.1.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.1.1.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.1.1.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.1.1.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.1.1.dat	Knowledge DB embedded in Cisco Cyber Vision 5.1.1
Updates/KDB/KDB.202502	**Description**
CiscoCyberVision_knowledgedb_20250207.db	Knowledge DB version 20250207
CiscoCyberVision_knowledgedb_20250214.db	Knowledge DB version 20250214
CiscoCyberVision_knowledgedb_20250221.db	Knowledge DB version 20250221
CiscoCyberVision_knowledgedb_20250228.db	Knowledge DB version 20250228

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

20250228

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

- **Talos Rules 2025-02-27 (https://www.snort.org/advisories/talos-rules-2025-02-27)**
- **Talos Rules 2025-02-25 (https://www.snort.org/advisories/talos-rules-2025-02-25)**
- **Talos Rules 2025-02-20 (https://www.snort.org/advisories/talos-rules-2025-02-20)**

The new and updated Snort rules span the following categories:

- 1 browser-ie rule with SID 64576
- 2 file-executable rules with SIDs 64613, 64612
- 2 file-office rules with SIDs 301154, 301153
- 1 file-other rule with SID 301142
- 4 file-pdf rules with SIDs 64621, 64620, 64594, 64593
- 2 indicator-compromise rules with SIDs 64595, 64596
- 10 malware-cnc rules with SIDs 64591, 64609, 64592, 64590, 64611, 64610, 64168, 63106, 64169, 64167
- 10 malware-other rules with SIDs 301151, 64589, 301152, 301149, 301150, 301147, 64587, 301145, 301146, 301148
- 6 server-other rules with SIDs 51825, 301144, 64577, 64578, 10407, 52287
- 10 server-webapp rules with SIDs 64600, 64618, 64619, 64597, 64599, 60889, 52235, 60890, 64588, 6459

20250221

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

- **Talos Rules 2025-02-18 (https://www.snort.org/advisories/talos-rules-2025-02-18)**

The new and updated Snort rules span the following categories:

- 4 browser-ie rules with SIDs 28881, 64566, 301143, 28882
- 5 browser-plugins rules with SIDs 35446, 35444, 35445, 35447, 64571
- 1 file-office rule with SID 9431
- 2 file-pdf rules with SIDs 64574, 64575
- 1 indicator-compromise rule with SID 64573
- 2 malware-cnc rules with SIDs 64570, 63215

- 1 protocol-scada rule with SID 20030
- 1 server-apache rule with SID 64569
- 1 server-mail rule with SID 64572
- 9 server-webapp rules with SIDs 47810, 24914, 51121, 24913, 51122, 24339, 18998, 51120, 31373

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

- CVE-2024-9404: (Denial-of-Service Vulnerability Identified in Multiple Moxa PT Switches)
  - Multiple PT switches are affected by a high-severity vulnerability, CVE-2024-9404, which could lead to a denial-of-service condition or cause a system or service crash. This vulnerability allows attackers to exploit the Moxa service, commonly referred to as moxa_cmd, originally designed for deployment purposes. Due to insufficient input validation, this service can be exploited to trigger a cold start or denial-of-service condition.)
- CVE-2024-20306: (Cisco IOS XE Software Unified Threat Defense Command Injection Vulnerability)
  - A vulnerability in the Unified Threat Defense (UTD) configuration CLI of Cisco IOS XE Software could allow an authenticated, local attacker to execute arbitrary commands as root on the underlying host operating system. To exploit this vulnerability, an attacker must have level 15 privileges on the affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by submitting a crafted CLI command to an affected device. A successful exploit could allow the attacker to execute arbitrary commands as root on the underlying operating system.
- CVE-2024-20324: (Cisco IOS XE Software for Wireless LAN Controllers Privilege Escalation Vulnerability)
  - A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, low-privileged, local attacker to access WLAN configuration details including passwords. This vulnerability is due to improper privilege checks. An attacker could exploit this vulnerability by using the show and show tech wireless CLI commands to access configuration details, including passwords. A successful exploit could allow the attacker to access configuration details that they are not authorized to access.
- CVE-2024-20312: (Cisco IOS and IOS XE Software Intermediate System-to-Intermediate System Denial of Service Vulnerability)
  - A vulnerability in the Intermediate System-to-Intermediate System (IS-IS) protocol of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation when parsing an ingress IS-IS packet. An attacker could exploit this vulnerability by sending a crafted IS-IS packet to an affected device after forming an adjacency. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition.
- CVE-2024-20307: (Cisco IOS and IOS XE Software Internet Key Exchange Version 1 Fragmentation Denial of Service Vulnerabilities)

  - Multiple vulnerabilities in the Internet Key Exchange version 1 (IKEv1) fragmentation feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a heap overflow or corruption on an affected system.

- CVE-2024-20308: (Cisco IOS and IOS XE Software Internet Key Exchange Version 1 Fragmentation Denial of Service Vulnerabilities)
  - Multiple vulnerabilities in the Internet Key Exchange version 1 (IKEv1) fragmentation feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a heap overflow or corruption on an affected system.
- CVE-2024-20303: (Cisco IOS XE Software for Wireless LAN Controllers Multicast DNS Denial of Service Vulnerability)
  - A vulnerability in the multicast DNS (mDNS) gateway feature of Cisco IOS XE Software for Wireless LAN Controllers (WLCs) could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper management of mDNS client entries. An attacker could exploit this vulnerability by connecting to the wireless network and sending a continuous stream of specific mDNS packets. A successful exploit could allow the attacker to cause the wireless controller to have high CPU utilization, which could lead to access points (APs) losing their connection to the controller and result in a DoS condition.
- CVE-2024-20319: (Cisco IOS XR Software SNMP Management Plane Protection ACL Bypass Vulnerability)
  - A vulnerability in the UDP forwarding code of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to bypass configured management plane protection policies and access the Simple Network Management Plane (SNMP) server of an affected device. This vulnerability is due to incorrect UDP forwarding programming when using SNMP with management plane protection. An attacker could exploit this vulnerability by attempting to perform an SNMP operation using broadcast as the destination address that could be processed by an affected device that is configured with an SNMP server. A successful exploit could allow the attacker to communicate to the device on the configured SNMP ports. Although an unauthenticated attacker could send UDP datagrams to the configured SNMP port, only an authenticated user can retrieve or modify data using SNMP requests.
- CVE-2024-20320: (Cisco IOS XR Software SSH Privilege Escalation Vulnerability)
  - A vulnerability in the SSH client feature of Cisco IOS XR Software for Cisco 8000 Series Routers and Cisco Network Convergence System (NCS) 540 Series and 5700 Series Routers could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient validation of arguments that are included with the SSH client CLI command. An attacker with low-privileged access to an affected device could exploit this vulnerability by issuing a crafted SSH client command to the CLI. A successful exploit could allow the attacker to elevate privileges to root on the affected device.
- CVE-2024-20266: (Cisco IOS XR Software DHCP Version 4 Server Denial of Service Vulnerability)
  - A vulnerability in the DHCP version 4 (DHCPv4) server feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to trigger a crash of the dhcpd process, resulting in a denial

  - of service (DoS) condition. This vulnerability exists because certain DHCPv4 messages are improperly validated when they are processed by an affected device. An attacker could exploit this vulnerability by sending a malformed DHCPv4 message to an affected device. A successful exploit could allow the attacker to cause a crash of the dhcpd process. While the dhcpd process is restarting, which may take approximately two minutes, DHCPv4 server services are unavailable on the affected device. This could temporarily prevent network access to clients that join the network during that time period and rely on the DHCPv4 server of the affected device.

- CVE-2024-20315: (Cisco IOS XR Software MPLS and Pseudowire Interfaces Access Control List Bypass Vulnerabilities)
  - Multiple vulnerabilities in the IP access control list (ACL) processing in the ingress direction on MPLS and Pseudowire (PW) interfaces of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass a configured ACL.
- CVE-2024-20322: (Cisco IOS XR Software MPLS and Pseudowire Interfaces Access Control List Bypass Vulnerabilities)
  - Multiple vulnerabilities in the IP access control list (ACL) processing in the ingress direction on MPLS and Pseudowire (PW) interfaces of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass a configured ACL.
- CVE-2024-20262: (Cisco IOS XR Software Authenticated CLI Secure Copy Protocol and SFTP Denial of Service Vulnerability)
  - A vulnerability in the Secure Copy Protocol (SCP) and SFTP feature of Cisco IOS XR Software could allow an authenticated, local attacker to create or overwrite files in a system directory, which could lead to a denial of service (DoS) condition. The attacker would require valid user credentials to perform this attack. This vulnerability is due to a lack of proper validation of SCP and SFTP CLI input parameters. An attacker could exploit this vulnerability by authenticating to the device and issuing SCP or SFTP CLI commands with specific parameters. A successful exploit could allow the attacker to impact the functionality of the device, which could lead to a DoS condition. The device may need to be manually rebooted to recover.
- CVE-2024-20318: (Cisco IOS XR Software Layer 2 Services Denial of Service Vulnerability)
  - A vulnerability in the Layer 2 Ethernet services of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause the line card network processor to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of specific Ethernet frames that are received on line cards that have the Layer 2 services feature enabled. An attacker could exploit this vulnerability by sending specific Ethernet frames through an affected device. A successful exploit could allow the attacker to cause the ingress interface network processor to reset, resulting in a loss of traffic over the interfaces that are supported by the network processor. Multiple resets of the network processor would cause the line card to reset, resulting in a DoS condition.
- CVE-2024-20327: (Cisco IOS XR Software for ASR 9000 Series Aggregation Services Routers PPPoE Denial of Service Vulnerability)

  - A vulnerability in the PPP over Ethernet (PPPoE) termination feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers could allow an unauthenticated, adjacent attacker to crash the ppp_ma process, resulting in a denial of service (DoS) condition. This vulnerability is due to the improper handling of malformed PPPoE packets that are received on a router that is running Broadband Network Gateway (BNG) functionality with PPPoE termination on a Lightspeed-based or Lightspeed-Plus-based line card. An attacker could exploit this vulnerability by sending a crafted PPPoE packet to an affected line card interface that does not terminate PPPoE. A successful exploit could allow the attacker to crash the ppp_ma process, resulting in a DoS condition for PPPoE traffic across the router.

- CVE-2024-20294: (Cisco FXOS and NX-OS Software Link Layer Discovery Protocol Denial of Service Vulnerability)
  - A vulnerability in the Link Layer Discovery Protocol (LLDP) feature of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of specific fields in an LLDP frame. An attacker could exploit this vulnerability by sending a crafted LLDP packet to an interface of an affected device and having an authenticated user retrieve LLDP statistics from the affected device through CLI show commands or Simple Network Management Protocol (SNMP) requests. A successful exploit could allow the attacker to cause the LLDP service to crash and stop running on the affected device. In certain situations, the LLDP crash may result in a reload of the affected device.
- CVE-2024-20267: (Cisco NX-OS Software MPLS Encapsulated IPv6 Denial of Service Vulnerability)
  - A vulnerability with the handling of MPLS traffic for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the netstack process to unexpectedly restart, which could cause the device to stop processing network traffic or to reload. This vulnerability is due to lack of proper error checking when processing an ingress MPLS frame. An attacker could exploit this vulnerability by sending a crafted IPv6 packet that is encapsulated within an MPLS frame to an MPLS-enabled interface of the targeted device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition.
- CVE-2024-20291: (Cisco Nexus 3000 and 9000 Series Switches Port Channel ACL Programming Vulnerability)
  - A vulnerability in the access control list (ACL) programming for port channel subinterfaces of Cisco Nexus 3000 and 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, remote attacker to send traffic that should be blocked through an affected device. This vulnerability is due to incorrect hardware programming that occurs when configuration changes are made to port channel member ports. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to access network resources that should be protected by an ACL that was applied on port channel subinterfaces.
- CVE-2024-20321: (Cisco NX-OS Software External Border Gateway Protocol Denial of Service Vulnerability)
  - A vulnerability in the External Border Gateway Protocol (eBGP) implementation of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS)

condition on an affected device. This vulnerability exists because eBGP traffic is mapped to a shared hardware rate-limiter queue. An attacker could exploit this vulnerability by sending large amounts of network traffic with certain characteristics through an affected device. A successful exploit could allow the attacker to cause eBGP neighbor sessions to be dropped, leading to a DoS condition in the network.

- CVE-2025-20169: (Cisco IOS, IOS XE, and IOS XR Software SNMP Denial of Service Vulnerabilities)
  - Multiple vulnerabilities in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.
- CVE-2025-20170: (Cisco IOS, IOS XE, and IOS XR Software SNMP Denial of Service Vulnerabilities)
  - Multiple vulnerabilities in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.
- CVE-2025-20171: (Cisco IOS, IOS XE, and IOS XR Software SNMP Denial of Service Vulnerabilities)
  - Multiple vulnerabilities in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.
- CVE-2025-20172: (Cisco IOS, IOS XE, and IOS XR Software SNMP Denial of Service Vulnerabilities)
  - Multiple vulnerabilities in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.
- CVE-2025-20173: (Cisco IOS, IOS XE, and IOS XR Software SNMP Denial of Service Vulnerabilities)
  - Multiple vulnerabilities in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.
- CVE-2025-20174: (Cisco IOS, IOS XE, and IOS XR Software SNMP Denial of Service Vulnerabilities)
  - Multiple vulnerabilities in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.
- CVE-2025-20175: (Cisco IOS, IOS XE, and IOS XR Software SNMP Denial of Service Vulnerabilities)
  - Multiple vulnerabilities in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.
- CVE-2025-20176: (Cisco IOS, IOS XE, and IOS XR Software SNMP Denial of Service Vulnerabilities)
  - Multiple vulnerabilities in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

20250214

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

- **Talos Rules 2025-02-13 (https://www.snort.org/advisories/talos-rules-2025-02-13)**
- **Talos Rules 2025-02-11 (https://www.snort.org/advisories/talos-rules-2025-02-11)**

The new and updated Snort rules span the following categories:

- 2 file-executable rules with SIDs 16022, 16023
- 1 file-office rule with SID 301138
- 3 file-other rules with SIDs 301142, 51235, 51236
- 8 malware-cnc rules with SIDs 64561, 64558, 64554, 64560, 64556, 64557, 64559, 64555
- 6 os-other rules with SIDs 64565, 63960, 63959, 64563, 64564, 64562
- 7 os-windows rules with SIDs 301140, 300612, 301139, 64545, 301141, 301136, 301137
- 1 policy-other rule with SID 64547
- 2 server-apache rules with SIDs 64548, 17387
- 1 server-iis rule with SID 3087
- 3 server-mail rules with SIDs 11837, 64546, 31650
- 13 server-other rules with SIDs 59077, 64534, 31406, 46474, 16052, 29966, 24802, 64550, 32672, 64527, 10135, 13843, 64549
- 20 server-webapp rules with SIDs 64538, 64528, 64533, 58316, 54162, 64537, 51287, 301135, 36195, 51961, 3469, 15264, 50392, 38288, 38286, 38287, 36196, 64551, 58317, 46791

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

- CVE-2024-9404: (Denial-of-Service Vulnerability in Multiple Moxa EDS, ICS, IKS, and SDS Switches)
  - Multiple Moxa EDS, ICS, IKS, and SDS switches are affected by a high-severity vulnerability, CVE-2024-9404, which could lead to a denial-of-service condition or cause a system or service crash. This vulnerability allows attackers to exploit the Moxa service, commonly referred to as moxa_cmd, originally designed for deployment purposes. Due to insufficient input validation, this service can be exploited to trigger a cold start or denial-of-service condition.
- CVE-2024-7695: (Out-of-bounds Write Vulnerability in Multiple Moxa EDS, ICS, IKS, and SDS Switches)
  - Multiple Moxa EDS, ICS, IKS, and SDS switches are affected by an out-of-bounds write vulnerability. This vulnerability is caused by insufficient input validation, which allows writing data beyond buffer boundaries. Successful exploitation could result in a denial-of-service (DoS) attack.
- CVE-2024-53651: (Cleartext Storage of Sensitive Information Vulnerability in Siemens SIPROTEC 5)

  - Affected devices do not encrypt certain data within the on-board flash storage on their PCB. This could allow an attacker with physical access to read the entire filesystem of the device.
- CVE-2023-37482: (Sensitive Information Exposure Vulnerability in Webserver of Siemens SIMATIC Products)
  - The login functionality of the web server in affected devices does not normalize the response times of login attempts. An unauthenticated remote attacker could exploit this side-channel information to distinguish between valid and invalid usernames.
- CVE-2025-24812: (Improper Validation Vulnerability in Siemens SIMATIC S7-1200 CPU Family)
  - Affected devices do not process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial of service in the device.
- CVE-2025-24811: (Improper Resource Shutdown or Release Vulnerability in Siemens SIMATIC S7-1200 CPU Family)
  - Affected devices do not process correctly certain special crafted packets sent to port 80/tcp, which could allow an unauthenticated attacker to cause a denial of service in the device.
- CVE-2024-54090: (Out-of-bounds Read Vulnerability in Siemens Apogee PXC and Talon TC Devices)
  - Affected devices contain an out-of-bounds read in the memory dump function. This could allow an attacker with Medium (MED) or higher privileges to cause the device to enter an insecure cold start state.
- CVE-2024-54089: (Inadequate Encryption Strength in Siemens Apogee PXC and Talon TC Devices)
  - Affected devices contain a weak encryption mechanism based on a hard-coded key. This could allow an attacker to guess or decrypt the password from the ciphertext.
- CVE-2024-53648: (Accessible Development Shell via Physical Interface in Siemens SIPROTEC 5)
  - Affected devices do not properly limit access to a development shell accessible over a physical interface. This could allow an unauthenticated attacker with physical access to the device to execute arbitrary commands on the device.
- CVE-2024-54015: (Use of Default Credentials Vulnerability in Siemens SIPROTEC 5 Devices)
  - Affected devices do not properly validate SNMP GET requests. This could allow an unauthenticated, remote attacker to retrieve sensitive information of the affected devices with SNMPv2 GET requests using default credentials.

20250207

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

- **Talos Rules 2025-02-06 (https://www.snort.org/advisories/talos-rules-2025-02-06)**
- **Talos Rules 2025-02-04 (https://www.snort.org/advisories/talos-rules-2025-02-04)**

The new and updated Snort rules span the following categories:

- 1 file-office rule with SID 301128
- 4 malware-cnc rules with SIDs 64509, 64511, 64510, 64498
- 5 malware-other rules with SIDs 64505, 301125, 64487, 301130, 301129
- 3 os-linux rules with SIDs 301132, 301134, 301133
- 4 os-windows rules with SIDs 58615, 58617, 2589, 58616
- 2 policy-other rules with SIDs 64497, 51631
- 6 protocol-snmp rules with SIDs 64524, 64515, 64523, 64516, 64513, 64514
- 2 protocol-voip rules with SIDs 301126, 301127
- 18 server-webapp rules with SIDs 64503, 40784, 34799, 31956, 59608, 58844, 64504, 64488, 58843, 301131, 43324, 55981, 39387, 58845, 64506, 18795, 31798, 64512

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

- CVE-2025-0631: (Credential Exposure Vulnerability in Rockwell PowerFlex 755)
    - A Credential Exposure Vulnerability exists in the above-mentioned product and version. The vulnerability is due to using HTTP resulting in credentials being sent in clear text.
- CVE-2025-24478: (Denial-of-Service Vulnerability in Rockwell GuardLogix 5580 and 5380)
    - A denial-of-service vulnerability exists in the affected products. The vulnerability could allow a remote, non-privileged user to send malicious requests resulting in a major nonrecoverable fault causing a denial-of-service.