Release Notes for Cisco Cyber Vision Knowledge DB

Release 202506

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-5.1.3.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.1.3.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.1.3.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.1.3.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.1.3.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.1.3.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.1.3.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.1.3.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.1.3.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.1.3.dat	Knowledge DB embedded in Cisco Cyber Vision 5.1.3
Updates/KDB/KDB.202506	**Description**
CiscoCyberVision_knowledgedb_20250602.db	Knowledge DB version 20250602
CiscoCyberVision_knowledgedb_20250606.db	Knowledge DB version 20250606
CiscoCyberVision_knowledgedb_20250613.db	Knowledge DB version 20250613
CiscoCyberVision_knowledgedb_20250620.db	Knowledge DB version 20250620
CiscoCyberVision_knowledgedb_20250627.db	Knowledge DB version 20250627

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

20250627

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

- **Talos Rules 2025-06-26 (https://www.snort.org/advisories/talos-rules-2025-06-26)**
- **Talos Rules 2025-06-24 (https://www.snort.org/advisories/talos-rules-2025-06-24)**

The new and updated Snort rules span the following categories:

- 1 indicator-compromise rule with SID 44416
- 2 os-windows rules with SIDs 65076, 16238
- 2 server-mail rules with SIDs 65064, 65077
- 4 server-other rules with SIDs 301260, 301261, 65065, 65068
- 10 server-webapp rules with SIDs 65067, 300913, 65066, 65071, 63343, 65069, 65070, 63344, 65074, 65075

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

- CVE-2021-1227: Cisco NX-OS Software NX-API Cross-Site Request Forgery Vulnerability
  - A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the NX-API on an affected device. An attacker could exploit this vulnerability by persuading a user of the NX-API to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. The attacker could view and modify the device configuration.
- CVE-2021-1229: Cisco NX-OS Software ICMP Version 6 Memory Leak Denial of Service Vulnerability
  - A vulnerability in ICMP Version 6 (ICMPv6) processing in Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a slow system memory leak, which over time could lead to a denial of service (DoS) condition. This vulnerability is due to improper error handling when an IPv6-configured interface receives a specific type of ICMPv6 packet. An attacker could exploit this vulnerability by sending a sustained rate of crafted ICMPv6 packets to a local IPv6 address on a targeted device. A successful exploit could allow the attacker to cause a system memory leak in the ICMPv6 process on the device. As a result, the ICMPv6 process could run out of system memory and stop processing traffic. The device could then drop all ICMPv6 packets, causing traffic instability on the device. Restoring device functionality would require a device reboot.
- CVE-2021-1361: Cisco NX-OS Software Unauthenticated Arbitrary File Actions Vulnerability
  - A vulnerability in the implementation of an internal file management service for Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode that are running Cisco NX-OS Software could allow an unauthenticated, remote attacker to create, delete, or

overwrite arbitrary files with root privileges on the device. This vulnerability exists because TCP port 9075 is incorrectly configured to listen and respond to external connection requests. An attacker could exploit this vulnerability by sending crafted TCP packets to an IP address that is configured on a local interface on TCP port 9075. A successful exploit could allow the attacker to create, delete, or overwrite arbitrary files, including sensitive files that are related to the device configuration. For example, the attacker could add a user account without the device administrator knowing.

- CVE-2021-1367: Cisco NX-OS Software Protocol Independent Multicast Denial of Service Vulnerability
    - A vulnerability in the Protocol Independent Multicast (PIM) feature of 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 insufficient input validation. An attacker could exploit this vulnerability by sending a crafted PIM packet to an affected device. A successful exploit could allow the attacker to cause a traffic loop, resulting in a DoS condition.
- CVE-2021-1368: Cisco FXOS and NX-OS Software Unidirectional Link Detection Denial of Service and Arbitrary Code Execution Vulnerability
    - A vulnerability in the Unidirectional Link Detection (UDLD) feature of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code with administrative privileges or cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted Cisco UDLD protocol packets to a directly connected, affected device. A successful exploit could allow the attacker to execute arbitrary code with administrative privileges or cause the Cisco UDLD process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition.
- CVE-2021-1387: Cisco NX-OS Software IPv6 Netstack Denial of Service Vulnerability
    - A vulnerability in the network stack 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 the software improperly releases resources when it processes certain IPv6 packets that are destined to an affected device. An attacker could exploit this vulnerability by sending multiple crafted IPv6 packets to an affected device. A successful exploit could cause the network stack to run out of available buffers, impairing operations of control plane and management plane protocols and resulting in a DoS condition. Manual intervention would be required to restore normal operations on the affected device.
- CVE-2023-20027: Cisco IOS XE Software Virtual Fragmentation Reassembly Denial of Service Vulnerability
    - A vulnerability in the implementation of the IPv4 Virtual Fragmentation Reassembly (VFR) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper reassembly of large packets that occurs when VFR is enabled on either a tunnel interface or on a physical interface that is configured with a maximum transmission unit (MTU) greater than 4,615 bytes. An attacker could exploit this vulnerability by sending fragmented packets through a VFR-enabled interface on

an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.

- CVE-2023-20029: Cisco IOS XE Software Privilege Escalation Vulnerability
    - A vulnerability in the Cloud Management for Catalyst migration feature of Cisco IOS XE Software could allow an authenticated, local attacker to gain root-level privileges on an affected device. This vulnerability is due to insufficient memory protection in the Cisco IOS XE Meraki migration feature of an affected device. An attacker could exploit this vulnerability by modifying the Meraki registration parameters. A successful exploit could allow the attacker to elevate privileges to root.
- CVE-2023-20033: Cisco IOS XE Software for Catalyst 3650 and Catalyst 3850 Series Switches Denial of Service Vulnerability
    - A vulnerability in Cisco IOS XE Software for Cisco Catalyst 3650 and Catalyst 3850 Series Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper resource management when processing traffic that is received on the management interface. An attacker could exploit this vulnerability by sending a high rate of traffic to the management interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.
- CVE-2023-20035: Cisco IOS XE SD-WAN Software Command Injection Vulnerability
    - A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system.
- CVE-2023-20065: Cisco IOS XE Software IOx Application Hosting Environment Privilege Escalation Vulnerability
    - A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.
- CVE-2023-20066: Cisco IOS XE Software Web UI Path Traversal Vulnerability
    - A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could

exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI.

- CVE-2023-20067: Cisco IOS XE Software for Wireless LAN Controllers HTTP Client Profiling Denial of Service Vulnerability
  - A vulnerability in the HTTP-based client profiling 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 on an affected device. This vulnerability is due to insufficient input validation of received traffic. An attacker could exploit this vulnerability by sending crafted traffic through a wireless access point. A successful exploit could allow the attacker to cause CPU utilization to increase, which could result in a DoS condition on an affected device and could cause new wireless client associations to fail. Once the offending traffic stops, the affected system will return to an operational state and new client associations will succeed.
- CVE-2023-20072: Cisco IOS XE Software Fragmented Tunnel Protocol Packet Denial of Service Vulnerability
  - A vulnerability in the fragmentation handling code of tunnel protocol packets in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected system to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to the improper handling of large fragmented tunnel protocol packets. One example of a tunnel protocol is Generic Routing Encapsulation (GRE). An attacker could exploit this vulnerability by sending crafted fragmented packets to an affected system. A successful exploit could allow the attacker to cause the affected system to reload, resulting in a DoS condition.
- CVE-2023-20080: Cisco IOS and IOS XE Software IPv6 DHCP (DHCPv6) Relay and Server Denial of Service Vulnerability
  - A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.
- CVE-2023-20081: Cisco Adaptive Security Appliance Software, Firepower Threat Defense Software, IOS Software, and IOS XE Software IPv6 DHCP (DHCPv6) Client Denial of Service Vulnerability
  - A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.
- CVE-2023-20100: Cisco IOS XE Software for Wireless LAN Controllers CAPWAP Join Denial of Service Vulnerability

  - A vulnerability in the access point (AP) joining process of the Control and Provisioning of Wireless Access Points (CAPWAP) protocol of Cisco IOS XE Software for Wireless LAN Controllers (WLCs) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to a logic error that occurs when certain conditions are met during the AP joining process. An attacker could exploit this vulnerability by adding an AP that is under their control to the network. The attacker then must ensure that the AP successfully joins an affected wireless controller under certain conditions. Additionally, the attacker would need the ability to restart a valid AP that was previously connected to the controller. A successful exploit could allow the attacker to cause the affected device to restart unexpectedly, resulting in a DoS condition.

- CVE-2023-20109: Cisco IOS and IOS XE Software Cisco Group Encrypted Transport VPN Software Out-of-Bounds Write Vulnerability
  - A vulnerability in the Cisco Group Encrypted Transport VPN (GET VPN) feature of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker who has administrative control of either a group member or a key server to execute arbitrary code on an affected device or cause the device to crash. This vulnerability is due to insufficient validation of attributes in the Group Domain of Interpretation (GDOI) and G-IKEv2 protocols of the GET VPN feature. An attacker could exploit this vulnerability by either compromising an installed key server or modifying the configuration of a group member to point to a key server that is controlled by the attacker. A successful exploit could allow the attacker to execute arbitrary code and gain full control of the affected system or cause the affected system to reload, resulting in a denial of service (DoS) condition. For more information, see the Details section of this advisory.
- CVE-2023-20115: Cisco Nexus 3000 and 9000 Series Switches SFTP Server File Access Vulnerability
  - A vulnerability in the SFTP server implementation for Cisco Nexus 3000 Series Switches and 9000 Series Switches in standalone NX-OS mode could allow an authenticated, remote attacker to download or overwrite files from the underlying operating system of an affected device. This vulnerability is due to a logic error when verifying the user role when an SFTP connection is opened to an affected device. An attacker could exploit this vulnerability by connecting and authenticating via SFTP as a valid, non-administrator user. A successful exploit could allow the attacker to read or overwrite files from the underlying operating system with the privileges of the authenticated user.
- CVE-2023-20135: Cisco IOS XR Software Image Verification Vulnerability
  - A vulnerability in Cisco IOS XR Software image verification checks could allow an authenticated, local attacker to execute arbitrary code on the underlying operating system. This vulnerability is due to a time-of-check, time-of-use (TOCTOU) race condition when an install query regarding an ISO image is performed during an install operation that uses an ISO image. An attacker could exploit this vulnerability by modifying an ISO image and then carrying out install requests in parallel. A successful exploit could allow the attacker to execute arbitrary code on an affected device.
- CVE-2023-20168: Cisco NX-OS Software TACACS+ or RADIUS Remote Authentication Directed Request Denial of Service Vulnerability

  - A vulnerability in TACACS+ and RADIUS remote authentication for Cisco NX-OS Software could allow an unauthenticated, local attacker to cause an affected device to unexpectedly reload. This vulnerability is due to incorrect input validation when processing an authentication attempt if the directed request option is enabled for TACACS+ or RADIUS. An attacker could exploit this vulnerability by entering a crafted string at the login prompt of an affected device. A successful exploit could allow the attacker to cause the affected device to unexpectedly reload, resulting in a denial of service (DoS) condition.

- CVE-2023-20169: Cisco Nexus 3000 and 9000 Series Switches IS-IS Protocol Denial of Service Vulnerability

  - A vulnerability in the Intermediate System-to-Intermediate System (IS-IS) protocol of Cisco NX-OS Software for the Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, adjacent attacker to cause the IS-IS process to unexpectedly restart, which could cause an affected device to reload. 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. A successful exploit could allow the attacker to cause a denial of service (DoS) condition due to the unexpected restart of the IS-IS process, which could cause the affected device to reload.

- CVE-2023-20186: Cisco IOS and IOS XE Software Command Authorization Bypass Vulnerability

  - A vulnerability in the Authentication, Authorization, and Accounting (AAA) feature of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to bypass command authorization and copy files to or from the file system of an affected device using the Secure Copy Protocol (SCP). This vulnerability is due to incorrect processing of SCP commands in AAA command authorization checks. An attacker with valid credentials and level 15 privileges could exploit this vulnerability by using SCP to connect to an affected device from an external machine. A successful exploit could allow the attacker to obtain or change the configuration of the affected device and put files on or retrieve files from the affected device.

- CVE-2023-20187: Cisco IOS XE Software for ASR 1000 Series Aggregation Services Routers IPv6 Multicast Denial of Service Vulnerability

  - A vulnerability in the Multicast Leaf Recycle Elimination (mLRE) feature of Cisco IOS XE Software for Cisco ASR 1000 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to incorrect handling of certain IPv6 multicast packets when they are fanned out more than seven times on an affected device. An attacker could exploit this vulnerability by sending a specific IPv6 multicast or IPv6 multicast VPN (MVPNv6) packet through the affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition.

- CVE-2023-20190: Cisco IOS XR Software Compression ACL Bypass Vulnerability

  - A vulnerability in the classic access control list (ACL) compression feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass the protection that is offered by a configured ACL on an affected device. This vulnerability is due to incorrect destination address range encoding in the compression module of an ACL that is applied to an interface of an affected device. An attacker could exploit this vulnerability by sending traffic through the affected device that should be denied by the configured ACL. A successful exploit could allow the attacker to bypass configured ACL protections on the affected device, allowing the attacker to access trusted networks that the device might be protecting.

- CVE-2023-20191: Cisco IOS XR Software Access Control List Bypass Vulnerability
  - A vulnerability in the access control list (ACL) processing on MPLS interfaces in the ingress direction of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to incomplete support for this feature. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to bypass an ACL on the affected device.
- CVE-2023-20202: Cisco IOS XE Software for Wireless LAN Controllers Wireless Network Control Denial of Service Vulnerability
  - A vulnerability in the Wireless Network Control daemon (wncd) of Cisco IOS XE Software for Wireless LAN Controllers could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper memory management. An attacker could exploit this vulnerability by sending a series of network requests to an affected device. A successful exploit could allow the attacker to cause the wncd process to consume available memory and eventually cause the device to reload, resulting in a DoS condition.
- CVE-2023-20226: Cisco IOS XE Software Application Quality of Experience and Unified Threat Defense Denial of Service Vulnerability
  - A vulnerability in Application Quality of Experience (AppQoE) and Unified Threat Defense (UTD) on Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to the mishandling of a crafted packet stream through the AppQoE or UTD application. An attacker could exploit this vulnerability by sending a crafted packet stream through an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.
- CVE-2023-20227: Cisco IOS XE Software Layer 2 Tunneling Protocol Denial of Service Vulnerability
  - A vulnerability in the Layer 2 Tunneling Protocol (L2TP) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of certain L2TP packets. An attacker could exploit this vulnerability by sending crafted L2TP packets to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.
- CVE-2023-20231: Cisco IOS XE Software Web UI Command Injection Vulnerability
  - A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform an injection attack against an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to execute arbitrary Cisco IOS XE Software CLI commands with level 15 privileges.

- CVE-2023-20233: Cisco IOS XR Software Connectivity Fault Management Denial of Service Vulnerability
  - A vulnerability in the Connectivity Fault Management (CFM) feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to incorrect processing of invalid continuity check messages (CCMs). An attacker could exploit this vulnerability by sending crafted CCMs to an affected device. A successful exploit could allow the attacker to cause the CFM service to crash when a user displays information about maintenance end points (MEPs) for peer MEPs on an affected device.
- CVE-2023-20235: Cisco IOx Application Hosting Environment Privilege Escalation Vulnerability
  - A vulnerability in the on-device application development workflow feature for the Cisco IOx application hosting infrastructure in Cisco IOS XE Software could allow an authenticated, remote attacker to access the underlying operating system as the root user. This vulnerability exists because Docker containers with the privileged runtime option are not blocked when they are in application development mode. An attacker could exploit this vulnerability by using the Docker CLI to access an affected device. The application development workflow is meant to be used only on development systems and not in production systems.
- CVE-2023-20236: Cisco IOS XR Software iPXE Boot Signature Bypass Vulnerability
  - A vulnerability in the iPXE boot function of Cisco IOS XR software could allow an authenticated, local attacker to install an unverified software image on an affected device. This vulnerability is due to insufficient image verification. An attacker could exploit this vulnerability by manipulating the boot parameters for image verification during the iPXE boot process on an affected device. A successful exploit could allow the attacker to boot an unverified software image on the affected device.

20250620

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

- **Talos Rules 2025-06-18 (https://www.snort.org/advisories/talos-rules-2025-06-18)**
- **Talos Rules 2025-06-17 (https://www.snort.org/advisories/talos-rules-2025-06-17)**

The new and updated Snort rules span the following categories:

- 1 malware-cnc rule with SID 65061
- 4 server-other rules with SIDs 65062, 301257, 301258, 52287
- 6 server-webapp rules with SIDs 65059, 65060, 64619, 65058, 65013, 65057

20250613

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

- **Talos Rules 2025-06-12 (https://www.snort.org/advisories/talos-rules-2025-06-12)**
- **Talos Rules 2025-06-10 (https://www.snort.org/advisories/talos-rules-2025-06-10)**

The new and updated Snort rules span the following categories:

- 1 browser-chrome rule with SID 65051
- 4 file-office rules with SIDs 301250, 301256, 301251, 301252
- 4 malware-cnc rules with SIDs 65056, 64995, 64994, 64996
- 7 os-windows rules with SIDs 55802, 56290, 301220, 65037, 301255, 301254, 301253
- 10 server-webapp rules with SIDs 65046, 64814, 65048, 65044, 64242, 65027, 65047, 65045, 64731, 65026

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

- CVE-2002-20001: Resource Exhaustion Vulnerability in Moxa ICS-G7848A/ICS-G7850A/ICS-G7852A Series
  - A resource exhaustion vulnerability, CVE-2002-20001, exists in the implementation of the Diffie-Hellman key exchange protocol. The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys and trigger expensive server-side DHE modular-exponentiation calculations, also known as a D(HE)at or D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive where a client can require a server to select its largest supported key size. The basic attack scenario requires the client to claim DHE-only communication capabilities, and the server must be configured to permit DHE. This vulnerability affects any product or service that accepts DHE cipher suites.
- CVE-2024-9404: Denial-of-Service Vulnerability in Moxa PT-G7728 & PT-G7828 Switches
  - Moxa PT-G7728 and PT-G7828 series 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. This vulnerability poses a significant remote threat if the affected products are exposed to publicly accessible networks. Attackers could potentially disrupt operations by shutting down the affected systems.
- CVE-2025-0133: Cross-site Scripting Vulnerability in Palo Alto Networks Virtual NGFW on RUGGEDCOM APE1808 Devices
  - A reflected cross-site scripting (XSS) vulnerability in the GlobalProtect™ gateway and portal features of Palo Alto Networks PAN-OS® software enables execution of malicious JavaScript in the context of an authenticated Captive Portal user’s browser when they click on a specially crafted link. The primary risk is phishing attacks that can lead to credential theft—particularly if you enabled Clientless VPN.
- CVE-2025-20137: Cisco IOS Software on Cisco Catalyst 1000 and 2960L Switches Access Control List Bypass Vulnerability
  - A vulnerability in the access control list (ACL) programming of Cisco IOS Software that is running on Cisco Catalyst 1000 Switches and Cisco Catalyst 2960L Switches could allow an unauthenticated,

remote attacker to bypass a configured ACL. This vulnerability is due to the use of both an IPv4 ACL and a dynamic ACL of IP Source Guard on the same interface, which is an unsupported configuration. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to bypass an ACL on the affected device.

- CVE-2025-20140: Cisco IOS XE Software for WLC Wireless IPv6 Clients Denial of Service Vulnerability
  - A vulnerability in the Wireless Network Control daemon (wncd) of Cisco IOS XE Software for Wireless LAN Controllers (WLCs) could allow an unauthenticated, adjacent wireless attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper memory management. An attacker could exploit this vulnerability by sending a series of IPv6 network requests from an associated wireless IPv6 client to an affected device. To associate a client to a device, an attacker may first need to authenticate to the network, or associate freely in the case of a configured open network. A successful exploit could allow the attacker to cause the wncd process to consume available memory and eventually cause the device to stop responding, resulting in a DoS condition.
- CVE-2025-20151: Cisco IOS and IOS XE Software SNMPv3 Configuration Restriction Vulnerability
  - A vulnerability in the implementation of the Simple Network Management Protocol Version 3 (SNMPv3) feature of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to poll an affected device using SNMP, even if the device is configured to deny SNMP traffic from an unauthorized source or the SNMPv3 username is removed from the configuration. This vulnerability exists because of the way that the SNMPv3 configuration is stored in the Cisco IOS Software and Cisco IOS XE Software startup configuration. An attacker could exploit this vulnerability by polling an affected device from a source address that should have been denied. A successful exploit could allow the attacker to perform SNMP operations from a source that should be denied. Note: The attacker has no control of the SNMPv3 configuration. To exploit this vulnerability, the attacker must have valid SNMPv3 user credentials.
- CVE-2025-20154: Cisco IOS, IOS XE, and IOS XR Software TWAMP Denial of Service Vulnerability
  - A vulnerability in the Two-Way Active Measurement Protocol (TWAMP) server feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. For Cisco IOS XR Software, this vulnerability could cause the ipsla_ippm_server process to reload unexpectedly if debugs are enabled. This vulnerability is due to out-of-bounds array access when processing specially crafted TWAMP control packets. An attacker could exploit this vulnerability by sending crafted TWAMP control packets to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: For Cisco IOS XR Software, only the ipsla_ippm_server process reloads unexpectedly and only when debugs are enabled. The vulnerability details for Cisco IOS XR Software are as follows: Security Impact Rating (SIR): Low CVSS Base Score: 3.7 CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
- CVE-2025-20155: Cisco IOS XE Software Bootstrap Arbitrary File Write Vulnerability

  - A vulnerability in the bootstrap loading of Cisco IOS XE Software could allow an authenticated, local attacker to write arbitrary files to an affected system. This vulnerability is due to insufficient input validation of the bootstrap file that is read by the system software when a device is first deployed in SD-WAN mode or when an administrator configures SD-Routing on the device. An attacker could exploit this vulnerability by modifying a bootstrap file generated by Cisco Catalyst SD-WAN Manager, loading it into the device flash, and then either reloading the device in a green field deployment in SD-WAN mode or configuring the device with SD-Routing. A successful exploit could allow the attacker to perform arbitrary file writes to the underlying operating system.

- CVE-2025-20162: Cisco IOS XE Software DHCP Snooping Denial of Service Vulnerability
  - A vulnerability in the DHCP snooping security feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a full interface queue wedge, which could result in a denial of service (DoS) condition.This vulnerability is due to improper handling of DHCP request packets. An attacker could exploit this vulnerability by sending DHCP request packets to an affected device. A successful exploit could allow the attacker to cause packets to wedge in the queue, creating a DoS condition for downstream devices of the affected system and requiring that the system restart to drain the queue. Note: This vulnerability can be exploited with either unicast or broadcast DHCP packets on a VLAN that does not have DHCP snooping enabled.

- CVE-2025-20164: Cisco IOS Software Industrial Ethernet Switch Device Manager Privilege Escalation Vulnerability
  - A vulnerability in the Cisco Industrial Ethernet Switch Device Manager (DM) of Cisco IOS Software could allow an authenticated, remote attacker to elevate privileges. This vulnerability is due to insufficient validation of authorizations for authenticated users. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to elevate privileges to privilege level 15. To exploit this vulnerability, the attacker must have valid credentials for a user account with privilege level 5 or higher. Read-only DM users are assigned privilege level 5.

- CVE-2025-20181: Cisco IOS Software for Cisco Catalyst 2960X, 2960XR, 2960CX, and 3560CX Series Switches Secure Boot Bypass Vulnerability
  - A vulnerability in Cisco IOS Software for Cisco Catalyst 2960X, 2960XR, 2960CX, and 3560CX Series Switches could allow an authenticated, local attacker with privilege level 15 or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to missing signature verification for specific files that may be loaded during the device boot process. An attacker could exploit this vulnerability by placing a crafted file into a specific location on an affected device. A successful exploit could allow the attacker to execute arbitrary code at boot time. Because this allows the attacker to bypass a major security feature of the device, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High

- CVE-2025-20182: Cisco Adaptive Security Appliance Software, Firepower Threat Defense Software, IOS Software, and IOS XE Software IKEv2 Denial of Service Vulnerability

  - A vulnerability in the Internet Key Exchange version 2 (IKEv2) protocol processing of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation when processing IKEv2 messages. An attacker could exploit this vulnerability by sending crafted IKEv2 traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition on the affected device.

- CVE-2025-20186: Cisco IOS XE Software Web-Based Management Interface Command Injection Vulnerability
  - A vulnerability in the web-based management interface of the Wireless LAN Controller feature of Cisco IOS XE Software could allow an authenticated, remote attacker with a lobby ambassador user account to perform a command injection attack against an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary Cisco IOS XE Software CLI commands with privilege level 15. Note: This vulnerability is exploitable only if the attacker obtains the credentials for a lobby ambassador account. This account is not configured by default.
- CVE-2025-20188: Cisco IOS XE Wireless Controller Software Arbitrary File Upload Vulnerability
  - A vulnerability in the Out-of-Band Access Point (AP) Image Download, the Clean Air Spectral Recording, and the client debug bundles features of Cisco IOS XE Software for Wireless LAN Controllers (WLCs) could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system. This vulnerability is due to the presence of a hard-coded JSON Web Token (JWT) on an affected system. An attacker could exploit this vulnerability by sending crafted HTTPS requests to the AP file upload interface. A successful exploit could allow the attacker to upload files, perform path traversal, and execute arbitrary commands with root privileges.
- CVE-2025-20189: Cisco IOS XE Software for Cisco ASR 903 Aggregation Services Routers ARP Denial of Service Vulnerability
  - A vulnerability in the Cisco Express Forwarding functionality of Cisco IOS XE Software for Cisco ASR 903 Aggregation Services Routers with Route Switch Processor 3 (RSP3C) could allow an unauthenticated, adjacent attacker to trigger a denial of service (DoS) condition. This vulnerability is due to improper memory management when Cisco IOS XE Software is processing Address Resolution Protocol (ARP) messages. An attacker could exploit this vulnerability by sending crafted ARP messages at a high rate over a period of time to an affected device. A successful exploit could allow the attacker to exhaust system resources, which eventually triggers a reload of the active route switch processor (RSP). If a redundant RSP is not present, the router reloads.

CVE-2025-20190: Cisco IOS XE Wireless Controller Software Unauthorized User Deletion Vulnerability

A vulnerability in the lobby ambassador web interface of Cisco IOS XE Wireless Controller Software could allow an authenticated, remote attacker to remove arbitrary users that are defined on an affected device. This vulnerability is due to insufficient access control of actions executed by lobby ambassador users. An attacker could exploit this vulnerability by logging in to an affected device with a lobby ambassador user account and sending crafted HTTP requests to the API. A successful exploit could allow the attacker to delete arbitrary user accounts on the device, including users with administrative privileges. Note: This vulnerability is exploitable only if the attacker obtains the credentials for a lobby ambassador account. This account is not configured by default.

- CVE-2025-20191: Multiple Cisco Products Switch Integrated Security Features DHCPv6 Denial of Service Vulnerability
  - A vulnerability in the Switch Integrated Security Features (SISF) of Cisco IOS Software, Cisco IOS XE Software, Cisco NX-OS Software, and Cisco Wireless LAN Controller (WLC) AireOS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to the incorrect handling of DHCPv6 packets. An attacker could exploit this vulnerability by sending a crafted DHCPv6 packet to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.
- CVE-2025-20192: Cisco IOS XE Software Internet Key Exchange Version 1 Denial of Service Vulnerability
  - A vulnerability in the Internet Key Exchange version 1 (IKEv1) implementation of Cisco IOS XE Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The attacker must have valid IKEv1 VPN credentials to exploit this vulnerability. This vulnerability is due to improper validation of IKEv1 phase 2 parameters before the IPsec security association creation request is handed off to the hardware cryptographic accelerator of an affected device. An attacker could exploit this vulnerability by sending crafted IKEv1 messages to the affected device. A successful exploit could allow the attacker to cause the device to reload.
- CVE-2025-20193: Cisco IOS XE Software Web-Based Management Interface Vulnerabilities
  - Multiple vulnerabilities in the web-based management interface of Cisco IOS XE Software could allow a remote attacker to read files from the underlying operating system, read limited parts of the configuration file, clear the syslog, or conduct a cross-site request forgery (CSRF) attack on an affected device, depending on their privilege level.
- CVE-2025-20194: Cisco IOS XE Software Web-Based Management Interface Vulnerabilities
  - Multiple vulnerabilities in the web-based management interface of Cisco IOS XE Software could allow a remote attacker to read files from the underlying operating system, read limited parts of the configuration file, clear the syslog, or conduct a cross-site request forgery (CSRF) attack on an affected device, depending on their privilege level.
- CVE-2025-20195: Cisco IOS XE Software Web-Based Management Interface Vulnerabilities
  - Multiple vulnerabilities in the web-based management interface of Cisco IOS XE Software could allow a remote attacker to read files from the underlying operating system, read limited parts of the configuration file, clear the syslog, or conduct a cross-site request forgery (CSRF) attack on an affected device, depending on their privilege level.
- CVE-2025-20196: Cisco IOx Application Hosting Environment Denial of Service Vulnerability
  - A vulnerability in the Cisco IOx application hosting environment of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause the Cisco IOx application

hosting environment to stop responding, resulting in a denial of service (DoS) condition. This vulnerability is due to the improper handling of HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to cause the Cisco IOx application hosting environment to stop responding. The IOx process will need to be manually restarted to recover services.

- CVE-2025-20197: Cisco IOS XE Software Privilege Escalation Vulnerabilities
    - Multiple vulnerabilities in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with privilege level 15 to elevate privileges to root on the underlying operating system of an affected device. These vulnerabilities are due to insufficient input validation when processing specific configuration commands. An attacker could exploit these vulnerabilities by including crafted input in specific configuration commands. A successful exploit could allow the attacker to elevate privileges to root on the underlying operating system of an affected device. The Security Impact Rating (SIR) of this advisory has been raised to High because an attacker could gain access to the underlying operating system of the affected device and perform potentially undetected actions. Note: The attacker must have privileges to enter configuration mode on the affected device. This is usually referred to as privilege level 15.
- CVE-2025-20198: Cisco IOS XE Software Privilege Escalation Vulnerabilities
    - Multiple vulnerabilities in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with privilege level 15 to elevate privileges to root on the underlying operating system of an affected device. These vulnerabilities are due to insufficient input validation when processing specific configuration commands. An attacker could exploit these vulnerabilities by including crafted input in specific configuration commands. A successful exploit could allow the attacker to elevate privileges to root on the underlying operating system of an affected device. The Security Impact Rating (SIR) of this advisory has been raised to High because an attacker could gain access to the underlying operating system of the affected device and perform potentially undetected actions. Note: The attacker must have privileges to enter configuration mode on the affected device. This is usually referred to as privilege level 15.
- CVE-2025-20199: Cisco IOS XE Software Privilege Escalation Vulnerabilities
    - Multiple vulnerabilities in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with privilege level 15 to elevate privileges to root on the underlying operating system of an affected device. These vulnerabilities are due to insufficient input validation when processing specific configuration commands. An attacker could exploit these vulnerabilities by including crafted input in specific configuration commands. A successful exploit could allow the attacker to elevate privileges to root on the underlying operating system of an affected device. The Security Impact Rating (SIR) of this advisory has been raised to High because an attacker could gain access to the underlying operating system of the affected device and perform potentially undetected actions. Note: The attacker must have privileges to enter configuration mode on the affected device. This is usually referred to as privilege level 15
- CVE-2025-20200: Cisco IOS XE Software Privilege Escalation Vulnerabilities

  - Multiple vulnerabilities in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with privilege level 15 to elevate privileges to root on the underlying operating system of an affected device. These vulnerabilities are due to insufficient input validation when processing specific configuration commands. An attacker could exploit these vulnerabilities by including crafted input in specific configuration commands. A successful exploit could allow the attacker to elevate privileges to root on the underlying operating system of an affected device. The Security Impact Rating (SIR) of this advisory has been raised to High because an attacker could gain access to the underlying operating system of the affected device and perform potentially undetected actions. Note: The attacker must have privileges to enter configuration mode on the affected device. This is usually referred to as privilege level 15.

- CVE-2025-20201: Cisco IOS XE Software Privilege Escalation Vulnerabilities
  - Multiple vulnerabilities in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with privilege level 15 to elevate privileges to root on the underlying operating system of an affected device. These vulnerabilities are due to insufficient input validation when processing specific configuration commands. An attacker could exploit these vulnerabilities by including crafted input in specific configuration commands. A successful exploit could allow the attacker to elevate privileges to root on the underlying operating system of an affected device. The Security Impact Rating (SIR) of this advisory has been raised to High because an attacker could gain access to the underlying operating system of the affected device and perform potentially undetected actions. Note: The attacker must have privileges to enter configuration mode on the affected device. This is usually referred to as privilege level 15.

- CVE-2025-20202: Cisco IOS XE Wireless Controller Software Cisco Discovery Protocol Denial of Service Vulnerability
  - A vulnerability in Cisco IOS XE Wireless Controller 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 of access point (AP) Cisco Discovery Protocol (CDP) neighbor reports when they are processed by the wireless controller. An attacker could exploit this vulnerability by sending a crafted CDP packet to an AP. A successful exploit could allow the attacker to cause an unexpected reload of the wireless controller that is managing the AP, resulting in a DoS condition that affects the wireless network.

- CVE-2025-20214: Cisco IOS XE Software Model-Driven Programmability Authorization Bypass Vulnerability
  - A vulnerability in the Network Configuration Access Control Module (NACM) of Cisco IOS XE Software could allow an authenticated, remote attacker to obtain unauthorized read access to configuration or operational data. This vulnerability exists because a subtle change in inner API call behavior causes results to be filtered incorrectly. An attacker could exploit this vulnerability by using either NETCONF, RESTCONF, or gRPC Network Management Interface (gNMI) protocols and query data on paths that may have been denied by the NACM configuration. A successful exploit could allow the attacker to access data that should have been restricted according to the NACM configuration. Note: This vulnerability requires that the attacker obtain the credentials from a valid user with privileges lower than 15, and that NACM was configured to provide restricted read access for that user.

- CVE-2025-20221: Cisco IOS XE SD-WAN Software Packet Filtering Bypass Vulnerability
    - A vulnerability in the packet filtering features of Cisco IOS XE SD-WAN Software could allow an unauthenticated, remote attacker to bypass Layer 3 and Layer 4 traffic filters. This vulnerability is due to improper traffic filtering conditions on an affected device. An attacker could exploit this vulnerability by sending a crafted packet to the affected device. A successful exploit could allow the attacker to bypass the Layer 3 and Layer 4 traffic filters and inject a crafted packet into the network.
- CVE-2025-3112: Denial of Service Vulnerability in Schneider Modicon Controllers M241/M251/M258/LMC058/M262
    - Uncontrolled Resource Consumption vulnerability exists that could cause Denial of Service when an authenticated malicious user sends manipulated HTTPS Content-Length header to the webserver.
- CVE-2025-3116: Improper Input Validation Vulnerability in Schneider Modicon Controllers M241/M251/M258/LMC058/M262
    - An Improper Input Validation vulnerability exists that could cause Denial of Service when an authenticated malicious user sends special malformed HTTPS request containing improper formatted body data to the controller
- CVE-2025-3117: Cross-site Scripting Vulnerability in Schneider Modicon Controllers M241/M251/M258/LMC058/M262
    - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists impacting configuration file paths that could cause an unvalidated data injected by authenticated malicious user leading to modify or read data in a victim’s browser.
- CVE-2025-3898: Improper Input Validation Vulnerability in Schneider Modicon Controllers M241/M251/M258/LMC058/M262
    - An Improper Input Validation vulnerability exists that could cause Denial of Service when an authenticated malicious user sends HTTPS request containing invalid data type to the webserver.
- CVE-2025-3899: Cross-site Scripting Vulnerability in Schneider Modicon Controllers M241/M251/M258/LMC058/M262
    - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists in Certificates page on Webserver that could cause an unvalidated data injected by authenticated malicious user leading to modify or read data in a victim’s browser.
- CVE-2025-3905: Cross-site Scripting Vulnerability in Schneider Modicon Controllers M241/M251/M258/LMC058/M262
    - An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists impacting PLC system variables that could cause an unvalidated data injected by authenticated malicious user leading to modify or read data in a victim’s browser.
- CVE-2025-40567: Incorrect Authorization Vulnerability in Siemens Industrial Communication Devices based on SINEC OS before V3.2

  - The “Load Rollback” functionality in the web interface of affected products contains an incorrect authorization check vulnerability. This could allow an authenticated remote attacker with “guest” role to make the affected product roll back configuration changes made by privileged users.
- CVE-2025-5740: Path Traversal Vulnerability in Schneider EVLink WallBox
  - An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause arbitrary file writes when an unauthenticated user on the web server manipulates file path.
- CVE-2025-5741: Path Traversal Vulnerability in Schneider EVLink WallBox
  - An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause arbitrary file reads from the charging station. The exploitation of this vulnerability does require an authenticated session of the web server.
- CVE-2025-5742: Cross-scripting Vulnerability in Schneider EVLink WallBox
  - An Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’) vulnerability exists when an authenticated user modifies configuration parameters on the web server
- CVE-2025-5743: OS Command Injection Vulnerability in Schneider EVLink WallBox
  - An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that could cause remote control over the charging station when an authenticated user modifies configuration parameters on the web server.

20250606

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

  - **Talos Rules 2025-06-05 (https://www.snort.org/advisories/talos-rules-2025-06-05)**
  - **Talos Rules 2025-06-03 (https://www.snort.org/advisories/talos-rules-2025-06-03)**

The new and updated Snort rules span the following categories:

- 1 file-office rule with SID 301230
- 2 file-pdf rules with SIDs 65011, 65012
- 11 malware-cnc rules with SIDs 64982, 64996, 64988, 64995, 64986, 64984, 64994, 64991, 64983, 64987, 64985
- 18 malware-other rules with SIDs 301225, 301235, 301236, 301229, 301232, 301237, 301234, 301240, 301226, 301243, 301233, 301239, 301227, 301231, 301238, 301241, 301242, 301228
- 2 malware-tools rules with SIDs 50479, 50478
- 2 os-linux rules with SIDs 301244, 301245
- 2 os-windows rules with SIDs 301191, 301248
- 1 policy-other rule with SID 65023

- 1 server-mail rule with SID 64965
- 8 server-webapp rules with SIDs 65018, 65024, 301247, 301246, 65020, 64941, 65025, 65013

20250602

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

- **Talos Rules 2025-05-29 (https://www.snort.org/advisories/talos-rules-2025-05-29)**
- **Talos Rules 2025-05-27 (https://www.snort.org/advisories/talos-rules-2025-05-27)**

The new and updated Snort rules span the following categories:

- 1 browser-plugins rule with SID 24335
- 1 file-office rule with SID 301219
- 2 file-other rules with SIDs 64955, 64954
- 2 os-windows rules with SIDs 55802, 301220
- 2 protocol-other rules with SIDs 64953, 64952
- 1 server-mail rule with SID 64938
- 20 server-webapp rules with SIDs 64960, 301221, 64961, 64937, 301218, 64942, 64935, 64936, 64945, 58833, 64949, 41504, 64948, 64941, 64950, 301223, 301222, 301224, 64951, 64962