Cisco Secure Workload Release Notes, Release 3.9.1.25

First Published: 2024-04-10

Last Modified: 2024-04-29

Introduction to Cisco Secure Workload, Release 3.9.1.25

The Cisco Secure Workload platform is designed to provide comprehensive workload security by establishing a micro perimeter around every workload. The micro perimeter is available across your on-premises and multicloud environment using firewall and segmentation, compliance and vulnerability tracking, behavior-based anomaly detection, and workload isolation. The platform uses advanced analytics and algorithmic approaches to offer these capabilities.

This document describes the features, bug fixes, and behavior changes, if any, in Cisco Secure Workload, Release 3.9.1.25.

For information on how to upgrade the software version, see Cisco Secure Workload Upgrade Guide.

Note As a best practice, we recommend to patch a cluster to the latest available patch version before performing a major version upgrade.

Release Information

Version: 3.9.1.25

Date: April 10, 2024

New Software Features in Cisco Secure Workload, Release 3.9.1.25

Feature Name	Description
Integration	
Integration of Cisco Vulnerability Management for Deep CVE Insights with Cisco Risk Score for Prioritization	To assess the severity of common vulnerabilities and exposures (CVE), you can now view the Cisco Security Risk Score of the CVE, including the attributes on the **Vulnerabilities** page. Use Cisco Security Risk Score to create inventory filters, microsegment policies to block communication from the impacted workloads, and virtual patching rules to publish the CVEs to Cisco Secure Firewall. For more information, see Vulnerability Dashboard, Cisco Security Risk Score-Based Filter, and Cisco Security Risk Score Summary.
Hybrid Multicloud Security	

Feature Name	Description
Visibility and Enforcement of Well-known IPv4 Malicious Traffic	You can now detect malicious traffic from workloads to well-known malicious IPv4 addresses. To block any traffic to these malicious IPs and to create and enforce policies, use a predefined read-only inventory filter **Malicious inventories**. **Note** This feature is disabled by default. To enable it: • For on-premises clusters, see Visibility of Well-Known Malicious IPv4 Addresses . • For SaaS, contact Cisco TAC. For more information, see Visibility of Well-Known Malicious IPv4 Addresses and Malicious Inventory-Based Filter.

Enhancements in Cisco Secure Workload, Release 3.9.1.25

- The following software agents are now supported:
  - AIX-6.1
  - Debian 12
  - Solaris zones
  - Ubuntu 22.04 as Kubernetes node
- Support is now restored to the software agent, SUSE Linux Enterprise Server 11.
- The traffic page now shows the SSH version and ciphers or algorithms used in the observed SSH communications.
- Cisco SSL component inside Windows agent now operates in FIPS mode.
- AIX agent forensic now detects and reports SSH login events.
- Windows agent CPU and memory usage have improved.
- Windows agent impact on network throughput has reduced.
- Secure Connector support has been added to Cloud Connectors.
- Label Management Change Impact Analysis: You can now analyze and preview the impact of changes in label values before committing the changes.

Changes in Behavior in Cisco Secure Workload, Release 3.9.1.25

Clusters force agents to refresh the client certificate if the certificates are close to expiration.

Known Behaviors in Cisco Secure Workload, Release 3.9.1.25

- For more information on known issues for Cisco Secure Workload software release, refer Release notes 3.9.1.1.

- After you apply 3.9.1.25 and if a decommission and commission occurs on a node where `orchestrator and enforcementPolicyStore` is available, it is possible a new service, `agent-status` may go down.

Resolved and Open Issues

The resolved and open issues for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about issues and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Resolved Issues

The following table lists the resolved issues in this release. Click an ID to access Cisco's Bug Search Tool to see additional information about that bug.

Identifier	Headline
CSCwe16875	Not able to push rules from CSW to FMC
CSCwi98814	Error retrieving attack surface details for workload in security dashboard
CSCwi10513	Agent installed on Solaris Sparc is unable to monitor ipmpX devices with IPNET frames
CSCwi98296	tet-enforcer crashes on registry corruption
CSCwi92824	RO user cannot see workspace matching inventory nor scope inventory of their own scope
CSCwj28450	Realtime events not captured on AIX 7.2 TL01
CSCwi89938	API Calls for CSW SaaS Platform result in bad gateway
CSCwi98513	Azure cloud connector inventory ingestion issue with VM NIC with multiple IPs
CSCwi40375	CIMC fw upgrade may fail due to huu iso mount failure
CSCwi57094	M6-39RU Disk Decommission workflow with RAID5 disks

Open Issues

The following table lists the open issues in this release. Click an ID to access Cisco's Bug Search Tool to see additional information about that bug.

Identifier	Headline
CSCwi40277	[Open API] Agent Network Policy Config need to show enf status consistent with data shown in UI

Identifier	Headline
CSCwh95336	Scope and Inventory Page: Scope Query: matches .* returns incorrect results
CSCwf39083	VIP switchover causing segmentation issues
CSCwh45794	ADM port and pid mapping is missing for some ports
CSCwf43558	Services failures after upgrade with orchestrator dns name not resolvable
CSCwj69650	Kubernetes Daemonset agent for Ubuntu 22.04 is missing
CSCwj40716	Secure Connector configuration gets reset during edits
CSCwj71847	Label management usage page not working
CSCwj82989	Flow Export stopped on Windows workload

Compatibility Information

For information about supported operating systems, external systems, and connectors for Secure Workload agents, see the Compatibility Matrix.

Verified Scalability Limits

The following tables provide the scalability limits for Cisco Secure Workload (39RU), Cisco Secure Workload M (8RU), and Cisco Secure Workload Virtual (VMWare ESXi).

Table 1: Scalability Limits for Cisco Secure Workload (39RU)

Configurable Option	Scale
Number of workloads	Up to 37,500 (VM or bare metal) Up to 75,000 when all the sensors are in conversation mode
Flow features per second	Up to 200,000

Table 2: Scalability Limits for Cisco Secure Workload M (8RU)

Configurable Option	Scale
Number of workloads	Up to 10,000 (VM or bare metal) Up to 20,000 when all the sensors are in conversation mode
Flow features per second	Up to 500,000

Table 3: Scalability Limits for Cisco Secure Workload Virtual (VMWare ESXi)

Configurable Option	Scale
Number of workloads	Up to 1,000 (VM or bare metal)
Flow features per second	Up to 70,000

Note The supported scale is based on the parameter that reaches the limit first.

Related Resources

Table 4: Related Resources

Resources	Description
Secure Workload Documentation	Provides information about Cisco Secure Workload, its features, functionality, installation, configuration, and usage.
• Cisco Secure Workload M6 Cluster Deployment Guide • Cisco Tetration (Secure Workload) M5 Cluster Hardware Deployment Guide	Describes the physical configuration, site preparation, and cabling of a single- and dual-rack installation for Cisco Secure Workload (39RU) platform and Cisco Secure Workload M (8RU).
Cisco Secure Workload Virtual (Tetration-V) Deployment Guide	Describes the deployment of Cisco Secure Workload virtual appliances.
Cisco Secure Workload Platform Datasheet	Describes technical specifications, operating conditions, licensing terms, and other product details.
Latest Threat Data Sources	The data sets for the Secure Workload pipeline that identifies and quarantines threats that are automatically updated when your cluster connects with Threat Intelligence update servers. If the cluster is not connected, download the updates and upload them to your Secure Workload appliance.

Contact Cisco Technical Assistance Centers

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.