Cisco Secure Workload Release Notes, Release 3.7.1.39

First Published: 2023-05-10

Introduction

This document describes the features, bug fixes and any behavior changes for the Cisco Secure Workload software patch release 3.7.1.39. This patch is associated with the Cisco Secure Workload software major release 3.7.1.5. Details of the major release can be found here.

Release Version and Date

Version: **3.7.1.39**

Date: **10 May, 2023**

New and Changed Information

This section lists the new and enhanced features, and known behaviors in this release.

Compatibility Information

- Agent packages for Windows 8.1 have been removed as OS is no longer supported.

For detailed compatibility information, please refer to Platform Information on Cisco.com.

Known Behaviors

See the Cisco Secure Workload major release 3.7.1.5 release notes.

New Software, New Hardware and Deprecated Features

New Software Features

There are no new software features in this release.

New Hardware Features

There are no new hardware features in this release.

Deprecated Features

There are no deprecated features in this release.

Enhancements

- User first and last names can be up to 40 characters.
- When filtering, the Contains operator is listed first.

Changes in Behavior

- On the UI, under label management, the label usage count now includes only direct usages.
- Flow learned inventories are not displayed on the **Scopes and Inventory** page. This will have no impact on policy discovery, policy analysis, and enforcement.

Verified Scalability Limits

The following tables provide the scalability limits for Cisco Secure Workload (39-RU), Cisco Secure Workload M (8-RU), and Cisco Secure Workload Cloud:

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

Configurable Option	Scale
Number of workloads	Up to 25,000 (VM or bare-metal). Up to 50,000 (2x) when all the sensors are in conversation mode.
Flow features per second	Up to 2 million.
Number of hardware agent enabled Cisco Nexus 9000 series switches	Up to 100 (deprecated).

Note Supported scale will always be based on which ever parameter reaches the limit first.

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

Configurable Option	Scale
Number of workloads	Up to 5,000 (VM or bare-metal). Up to 10,000 (2x) when all the sensors are in conversation mode.
Flow features per second	Up to 500,000.
Number of hardware agent enabled Cisco Nexus 9000 series switches	Up to 100 (deprecated).

Note Supported scale will always be based on which ever parameter reaches the limit first.

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.
Number of hardware agent enabled Cisco Nexus 9000 series switches	Not supported.

Note Supported scale is based on whichever parameter reaches the limit first.

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.

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

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

Resolved Issues

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

Identifier	Headline
CSCwe16875	Now honoring FMC limit of 50 ports per access rule. Policy with more than 50 ports will be split into multiple access rules.
CSCwf78123	[Linux] Continuous Policy deviation/Correction on newer platforms when iptables-legacy present.
CSCwe74218	Read Only CSW User Can Create and Delete User Labels with OpenAPI.
CSCwe21801	Need to have cases-insensitive comparison of LDAP attributes fetched from connectors.
CSCwe32392	High number of Ldap queries from Secure Workload Anyconnect Connector.
CSCwe20941	Ldap loader queries ldap twice per poll interval.

Identifier	Headline
CSCwc97458	Workload CVE Vulnerability Detection Logic Reports Many False Positives.
CSCwd68433	ADM incorrectly removed approved policies.
CSCwd64311	ADM submits with Default Config button clicked not setting some flags.
CSCwe47738	Workspace Last Update Time Changes to Current Time when Clicked Manage Policies.
CSCwe27066	Anyconnect connector - the controller crashed: Not able to export flow data.
CSCwd85744	Workload package removal does not reflect in UI.
CSCwf03825	AIX agent installer does not recognize ipfilter version greater than ipfilter v5.3.0.7
CSCwe38118	Batch indexer crash looping trying to use multivalue for orchestrator_system/cluster.
CSCwe02419	Enabling CSW alerts may not apply configuration to connectors on edge appliance.
CSCwe38457	Upgrade to 3.7 may cause druid disks to fill up.

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
CSCwd67224	AIX 7.x once enforcement is enabled, agent not able to connect to CSW Cluster due to fragmentation.
CSCwf78123	[Linux] Continuous Policy deviation/Correction on newer platforms when iptables-legacy present.
CSCwd60340	Agent Installer Script Downloaded From 3.6 Release Will Not Download Sensor from 3.7 Release.
CSCwb39541	Change error message on Investigate Traffic queries that are timing out.
CSCwb91717	Data for SW Status Upgrade chart for software agents in pending status is missing.
CSCwb80213	vNIC is hung up on a baremetal server (eNIC version on BM should be upgraded).
CSCwc63711	Missing permissions for Azure segmentation.
CSCwd93604	Increase in druid load queue on clusters with very high flow ingestion rate.
CSCwe83822	Windows Agent Upgrade from 3.7.1.22 can fail MSI signature check.
CSCwb42177	Live and Enforcement policy analysis - hover over the table for scopes column and text chopped off.
CSCwf37266	AIX enforcement rules do not properly match on subnets with leading zeros.
CSCwf18991	AIX: DHCP broken when Catch-all is DENY.

Related Documentation

Document	Description
Cisco Secure Workload Cluster Deployment Guide	Describes the physical configuration, site preparation, and cabling of a single- and dual-rack installation for Cisco Secure Workload (39-RU) platform and Cisco Secure Workload M (8-RU). Cisco Tetration (Secure Workload) M5 Cluster Hardware Deployment Guide
Cisco Secure Workload Virtual Deployment Guide	Describes the deployment of Cisco Secure Workload virtual appliances (formerly known as Tetration-V). Cisco Secure Workload Virtual (Tetration-V) Deployment Guide
Cisco Secure Workload Platform Datasheet	Cisco Secure Workload Platform Datasheet
Secure Workload Documentation	Secure Workload Documentation
Latest Threat Data Sources	Cisco Secure Workload

Contact Cisco

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