Cisco Secure Workload Release Notes, Release 3.7.1.51

First Published: 2023-06-22

Last Modified: 2023-06-30

Introduction

This document describes the features, bug fixes and any behavior changes for the Cisco Secure Workload software patch release 3.7.1.51. 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.

As a best practice, it is recommended to patch a cluster to the latest available patch version before performing a major version upgrade. For more information, see Cisco Secure Workload Upgrade Guide.

Release Version and Date

Version: 3.7.1.51

Date: 22 June, 2023

New and Changed Information

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

Compatibility Information

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.

Enhancements

- Software agents processes flows carried through VLAN tagged frames.
- Enhanced the functionality to detect clients in the NetFlow and ASA Connectors' reported flows.
- Enhanced functionality to capture forensic events on SUSE Linux Enterprise Server (SLES) workloads using the software agents.
- On the Flow Search page, the TCP flags display the flows denied on the AIX workloads.
- The Workload Profile page now displays 2022 CVEs.

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 Virtual:

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).

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).

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

Identifier	Headline
CSCwe21841	Need to enable Degree model for Client server determination when both ports are well known.
CSCwf78123	[Linux] Continuous Policy deviation/Correction on newer platforms when iptables-legacy present.
CSCwe83822	Windows Agent Upgrade from 3.7.1.22 can fail MSI signature check.
CSCwf18991	AIX: DHCP broken when Catch-all is DENY.
CSCwf29111	Policy Analysis may incorrectly show rejected flow by Windows workload.
CSCwf29138	TetSen.exe process is faulting on Windows workloads.
CSCwf37266	AIX enforcement rules do not properly match on subnets with leading zeros.
CSCwf68114	NetScaler: External orchestrator annotations are missing cluster_name.
CSCwf78551	wss could crash causing frequent agent reconnections on very busy clusters.

Open Issues

Identifier	Headline
CSCwb80213	vNIC is hung up on a baremetal server, requires reboot of server to recover
CSCwf78123	[Linux] Continuous Policy deviation/Correction on newer platforms when iptables-legacy present.
CSCwb91717	Data for SW Status Upgrade chart for software agents in pending status is missing
CSCwb42177	Live and Enforcement policy analysis - hover over the table for scopes column and text chopped off
CSCwb39541	Change error message on Investigate Traffic queries that are timing out
CSCwc63711	Missing permissions for Azure segmentation
CSCwd67224	AIX 7.x once enforcement is enabled, agent not able to connect to CSW Cluster due to fragmentation
CSCwd60340	Agent Installer Script Downloaded From 3.6 Release Will Not Download Sensor from 3.7 Release

Identifier	Headline
CSCwd93604	Increase in druid load queue on clusters with very high flow ingestion rate

Note Click on the identifier to access Cisco's Bug Search Tool to see additional information about the issue.

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