Cisco Secure Workload Release Notes Release 3.6.1.47

This document describes the new features, caveats, and limitations for Cisco Secure Workload software, release 3.6.1.4x

This document describes the features, bug fixes and any behavior changes for the Cisco Secure Workload software patch release 3.6.1.47. This patch is associated with the Cisco Secure Workload software major release 3.6.1.5. Details of the major release can be found here - https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_6_1_5.html.

Release Notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of this document:

https://www.cisco.com/c/en/us/support/security/tetration/products-release-notes-list.html

The following table shows the online change history for this document.

Table 1 Online History Change

Date	Description
Sep 12, 2022	Release 3.6.1.47 became available.

Contents

This document includes the following sections:

New and Changed Information

This section lists the new and changed features in this release and includes the following topics:

New Software Features

- No new software features in this patch release

Enhancements

- Software Agents now support Redhat Enterprise Server 9 on x86_64 and s390x architectures

Changes in Behavior

- No changes to software in this patch release

Caveats

This section contains lists of open and resolved caveats, as well as known behaviors.

Open Caveats

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

Table 2 Open Caveats

Bug ID	Description
CSCvz95962	Conversation Mode: Short lived non TCP flows in conversation mode can have client server flipped
CSCwa11427	Conversation Mode: 39RU cluster may not support 50k sensors when enforcement is enabled.
CSCvz95023	FMC-CSW orchestrator: CSW pushes ipv6 hop by hop if protocol is set to any
CSCvz99865	AWS Flow Logs: Policies Analysis with AWS Flow logs doesn't work.

Resolved Caveats

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

Table 3 Resolved Caveats

Bug ID	Description
CSCwb21235	namenode switchover script may fail to wait for namenode to start

CSCwb94594	Unable to perform a massive CSW agent deployment for their workloads
	Secure workload internal cluster orchestrator local dns may fail in very rare cases
CSCwc17237	Disabling network visibility also disables process/package visibility
CSCwc23159	RHEL 8.x enforcement agents don't display in Upgrade tab
CSCwc32016	Netflow sensor dropping received netflow data.
CSCwc59065	Enforcement Agent may restart when processing a policy with specific IPv6 ranges
CSCwc31985	Error decoding netflow datasets received from ACI with EOF errors
CSCwc77006	CSW 3.7 Upgrade may fail due to rsync version < 3.1.2 on orchestrators
CSCwc31977	Constant errors in decoding netflow packets from Netflow Connector.
CSCvy31758	Add Requirement to Import Working SSH Keys Before Upgrade
CSCwb76311	Windows agent installer powershell script does not provide option to install agent in custom path.
CSCwc29903	Agent installer script with user label update caveat
CSCwc79283	Agent on RHEL hosts would repeatedly appear in Agent Restarted anomaly
CSCwc68679	Disabling the Forensic feature does not stop logging events into audit logs
CSCvy04774	Match Condition Support for All Label Types
CSCwb72418	Policy Template import does not change Analyze Latest Policies button
CSCwb80090	Clock Drift Observed on Windows Server 2008 R2 with Cisco Secure Workload Agent
CSCwc14819	DNS external orchestrator goes into error state and is not able to get metadata from DNS servers configured with extremely large DNS zones.

Known Behaviors

- Refer to Cisco Secure Workload software major release 3.6.1.5 release notes - https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_6_1_5.html.

Compatibility Information

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

Usage Guidelines

- Refer to Cisco Secure Workload software major release 3.6.1.5 release notes - https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_6_1_5.html.

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 5 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 6 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 7 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 will always be based on whichever parameter reaches the limit first.

Related Documentation

The Cisco Secure Workload documentation can be accessed from the following websites:

Cisco Secure Workload Platform Datasheet: http://www.cisco.com/c/en/us/products/collateral/data-center-analytics/tetration-analytics/datasheet-c78-737256.html

Secure Workload Documentation: https://www.cisco.com/c/en/us/support/security/tetration/series.html#~tab-documents

Table 8 Installation 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). Document Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/hw/installation_guide/Cisco-Tetration-M5-Cluster-Hardware-Deployment-Guide.html
Cisco Secure Workload Virtual Deployment Guide	Describes the deployment of Cisco Secure Workload virtual appliances (formerly known as Tetration-V). Document Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Tetration_Analytics_Virtual_Appliance_Deployment_Guide.html
Cisco Secure Workload Upgrade Guide	Document Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/secure_workload/upgrade/appliance/cisco-secure-workload-upgrade-guide.html NOTE: As a best practice, it's always recommended to patch a cluster to the latest available patch version before performing a major version upgrade.

Latest Threat Data Sources	https://updates.tetrationcloud.com/