Cisco Secure Workload Release Notes, Release 3.8.1.19

First Published: 2023-08-18

Introduction

This document describes the features, bug fixes and any behavior changes for the Cisco Secure Workload software patch release 3.8.1.19.

This patch is associated with the Cisco Secure Workload software major release 3.8.1.1, the details of which 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: 3.8.1.19

Date: August 18, 2023

New Features

Feature Name	Description
Ease-of-use	
Agent token	You can now generate a time-bound agent token on the Secure Workload UI to disable service protection on workloads.
Day 2 Operations	
Windows desktop license	The following versions consume Windows desktop license in Secure Workload: • Microsoft Windows10Enterprise2016LTSB • Microsoft Windows10EnterpriseLTSC2019 • Microsoft Windows10EnterpriseLTSC2021 • Microsoft Windows10ProforWorkstations • Microsoft Windows11 • Microsoft Windows11Pro • Microsoft Windows11Home • Microsoft Windows11Enterprise • Microsoft Windows11ProforWorkstations

Feature Name	Description
Cloud Native Workloads	
AWS cloud collector supports flow logs	Secure Workload AWS connector supports partitioning of VPC flow logs every hour or every 24 hours. This helps to capture information about the network traffic moving to and from network interfaces within the VPC.

Enhancements

- Software agents support:
  - Solaris 11.4 on SPARC architecture (No Forensic and Process Visibility).
  - Enforcement on Solaris 11.4 on x86_64 and SPARC architectures.
- In the Agent List page, a warning sign is now displayed for agents that no longer support current versions. The warning is displayed when the agent's version (M.M) is two steps or more behind the cluster's version, for example, 3.6.52 vs 3.8.1.
- Software agent TetSensor/TetSensor.exe binary can be used to inspect the content of the offline flow files.
- TCP flags are now displayed for dropped flows on AIX workloads in the Secure Workload Traffic page.
- Software agent profile reports kernel information for AIX, Linux, and Solaris workloads.
- With the help of APIs, you can now upload CMDB using a JSON payload.
- OpenShift daemonset agent supports RedHatEnterpriseCoreOSServer 4.10, 4.11, 4.12, and 4.13.
- Automatically approve all policies generated by policy discovery.
- Support 10,000 workloads (8RU) and 37,500 workloads (39RU) in full fidelity mode.
- AWS, Azure and FMC connectors are no longer in Beta, these connectors are now in production.
- The reporting dashboard now displays:
  - top 10 hosts based on flows
  - number of labels, scopes, and unused filters.
  - agents with software versions that is not current.
- GCP connector is enhanced with better workflow and therefore more intuitive and streamlined for managing the cloud resources.
- For the secure connector, you can enable alerts to know when the secure connector is down or unreachable.

Changes in Behavior

- When an active agent is removed from the Agent List page, the agent is stopped and the services are disabled.
- CVE information is now reported for Windows Server 2022 workloads.

Known Behaviors

See the Cisco Secure Workload major release 3.8.1.1 release notes.

Compatibility Information

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

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 37,500 (VM or bare-metal) Up to 75,000 (2x) when all the sensors are in conversation mode
Flow features per second	Up to 2 million

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

Configurable Option	Scale
Number of workloads	Up to 10,000 (VM or bare-metal) Up to 20,000 (2x) 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 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.

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.

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

Resolved Issues

Identifier	Headline
CSCwf78551	wss could crash causing frequent agent reconnections on very busy clusters
CSCwf40082	Standby Cluster Patch Update Changes CIMC Password in Cluster, But Not Changed in CIMC admin User
CSCwd93604	Druid segment load queue could go high on 3.7 due to 2GB+ segment size
CSCwd24084	Storcli showing all disks faulty but only one disk faulty in CIMC
CSCwf60529	SCCM Deployed Agents Might Fail Later Upgrades
CSCwf78123	[Linux] Continuous Policy deviation/Correction on newer platforms when iptables-legacy present
CSCwf37266	AIX enforcement rules do not properly match on subnets with leading zeros
CSCwf79178	Sensor process may crash on disconnect from cluster
CSCvz95023	FMC-CSW connector: CSW pushes ipv6 hop by hop if protocol is set to Any
CSCwf78486	SSL rate limiting causing issues on high volume clusters after upgrade to 3.8.1.1
CSCwf82059	Azure Connector Gather Labels: shows no data and errors with 404
CSCwf82361	Agent inactive alert check can cause false alerts
CSCwd86013	Enforcement Analysis Page - capability to filter out PERMITTED:REJECTED or REJECTED:PERMITTED
CSCwf65746	Cluster upgrade to 3.8.1.1, can cause enforcement status change to POLICIES_OUT_OF_SYNCH
CSCwe45637	ADM run generates a huge UDP port range 1100-10300, when policy generalization set "very aggressive"
CSCvv96844	Flows with incorrect consumer/provider ports for flows that are idle for more than 12m

Identifier	Headline
CSCwf78555	Noisy service status check for Internalk8sdns
CSCwf81934	Intermittent failures of OrchestratorInventoryManager

Open Issues

Identifier	Headline
CSCwd67224	AIX 7.x once enforcement is enabled, agent not able to connect to CSW Cluster due to fragmentation
CSCwb80213	vNIC is hung up on a baremetal server (eNIC version on BM should be upgraded)
CSCwb42177	Live and Enforcement policy analysis - hover over the table for scopes column and text chopped off

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