Cisco Secure Workload Release Notes, Release 3.8.1.53

First Published: 2024-06-19

Last Modified: 2024-06-18

Introduction

This document describes the features, bug fixes, and behavior changes, if any, in Cisco Secure Workload software patch 3.8.1.53. This patch is associated with Cisco Secure Workload software release 3.8.1.1, the details of which are available here.

As best practice, we recommend that you 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 Information

Release Version: 3.8.1.53

Published Date: June 19, 2024

Enhancements for Release 3.8.1.53

- You can now prevent older versions of software agents from registering with the cluster or being installed using the installer script. This is controlled with a configuration under the platform cluster configuration. This enhancement ensures that only new versions of software agents can be installed and prevents the installation of agents with deprecated versions.
- Client detection for dropped TCP flows reported by Cisco Secure Firewall has been improved.
- Client detection for flows reported by AnyConnect has been improved.
- Consumer or Provider detection has been improved for flows when visibility fidelity is set to conversation.

Changes in Behavior

- Ingest Virtual Appliances now accept more than one instance of each connector type.
- The Forensic Memory Usage alert is now monitoring the current memory usage correctly. Earlier, it was following the maximum memory (max_rss) used.
- Memory and CPU usage anomalies in Software Agents Health page are now raised based on when they deviate from the corresponding quota values configured in the Agent Config Profiles. Before they were incorrectly following the corresponding alerts thresholds configurations.
- The Stats graph in **Workload Profile** > **Stats** now accurately displays the current memory usage for Host Visibility and Forensics' **Memory Overhead**, resolving the issue of showing peak memory usage.

- The default value for the **Memory Quota Limit** for Process Visibility and Forensics in Agent Config Profile is increased to 512 MB.
- API Key for Agent Installer roles is now authorized to execute OpenAPI endpoint “GET /openapi/v1/sensors”.
- Agent anomaly type is now included in the OpenAPI endpoint “GET /openapi/v1/sensors” response content.

Resolved and Open Issues

The resolved 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. There is no open issues available here.

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

Identifier	Headline
CSCwj74525	Windows Agent may restart with a memory read violation
CSCwi10313	Agent installed on Solaris Sparc failing to register to Secure Workload Cluster
CSCwi10329	Agent installed on Solaris Sparc is running but not reporting machine info or flows
CSCwi46792	[AnyConnect Connector] Use new flow direction features of AnyConnect to determine IP correctly
CSCwj74155	Windows workload may become unresponsive due to Secure Workload agent crashâ¨
CSCwi41825	False positive Agent CPU usage anomaly
CSCwi10513	Agent installed on Solaris Sparc is unable to monitor ipmpX devices with IPNET frames
CSCwj66511	High CPU usage and restart of tet-sensor process on Linux workloads
CSCwi49642	Enforcement registration fails for Solaris Agent
CSCwh91667	[3.8] Forensics/vulnerability data missing or stale for enforced workloads with catch all Deny
CSCwi92311	Cleanup special files when offline flows feature is disabled

Related Resources

Table 1: 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.

Additional Information for Secure Workload

Information	Description
Compatibility Information	For information about supported operating systems, external systems, and connectors for Secure Workload agents, see the Compatibility Matrix.
Known Behaviors	For more information on the known behaviors, see Cisco Secure Workload Release Notes, 3.9.1.1.
Scalability Limits	For information about the scalability limits of Cisco Secure Workload (39-RU) and Cisco Secure Workload M (8-RU) platforms, see Cisco Secure Workload Platform Data Sheet..

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