Release Notes for Cisco Secure Malware Analytics Appliance (formerly Threat Grid Appliance) Version 2.19

First Published: 2023-02-01

Last Modified: 2024-09-24

Introduction

This document describes the Release Notes, and Known Issues in Cisco Secure Malware Analytics (formerly Threat Grid) Appliance Version 2.19.0

User Documentation

The following Secure Malware Analytics (formerly Threat Grid) appliance user documentation is available:

Secure Malware Analytics Appliance User Documentation

Appliance user documentation is available on the Secure Malware Analytics appliance Install and Upgrade Guides page on the Cisco website.

Note Newer documentation is being made available from the Secure Malware Analytics appliance Products and Support page.

Backup FAQ

Please see the Backup Notes and FAQ for technical information and instructions.

Clustering Overview and FAQ

Please see the Clustering Overview and FAQ for additional information.

Installing Updates

Before you can update the Secure Malware Analytics (formerly Threat Grid) appliance with newer versions, you must have completed the initial setup and configuration steps as described in the Appliance Setup and Configuration Guide, which are available on the Secure Malware Analytics Appliance Install and Upgrade Guides page on the Cisco website.

New Appliances: If you have a new Appliance that shipped with an older version and wish to install updates, you must complete the initial configuration first. **Do Not** apply the updates until all Appliance configuration is done.

Appliance updates will not download unless the license is installed, and may not apply correctly if the Appliance has not been fully configured, including the database.

Secure Malware Analytics Appliance updates are applied through the Admin UI Portal.

Updates are one-directional: you cannot revert to a previous version after you upgrade to a more recent version.

To test the update, submit a sample for analysis.

Fixes and Updates

Version 2.19.4

- **Enhanced Policy Routing**: Improvements to policy routing to ensure smoother network traffic management.
- **New Firmware Update Tool**: A firmware update tool has been added, specifically designed for the M5 and M6 generations of the appliance. Refer to the admin guide for detailed instructions on how to use this new feature.

Version 2.19.3

This release adds a variety of fixes and enhancements.

- Implemented components update to provide fix against http2 rapid reset attacks. Relevant CVEs: CVE-2024-27983 CVE-2024-27919 CVE-2024-2758 CVE-2024-2653 CVE-2023-45288 CVE-2024-28182 CVE-2024-27316 CVE-2024-31309 CVE-2024-30255 CVE-2024-24549.
- Fixed 250 MB file submission timeout.
- Fixed exception when clicking on sample from an empty recent submission.
- Fixed report generation exception.
- Adjusted system parameters to reduce occurence of vm_reported_error due to resource contention.
- Fixed migration from standalone to cluster.

Version 2.19.2

This release addresses a problem preventing UCS M6 hardware appliance from successfully performing the destroy-data.

Version 2.19.1

This release resolves an out-of-space condition affecting upgrades to future versions on older generations of hardware, and removes some incorrect service notices on the UCS M6.

After upgrading, the appliance will take longer than usual to boot because a migration is being applied. Please allow the appliance 30 minutes to complete the migration.

Version 2.19.0

This release updates the core application software and includes a variety of other fixes and enhancements.

- The core application software has been updated to match cloud version 3.5.129.
- Fixes minor issues that could lead to spurious error messages during the boot and configuration process.
- Fixes an issue where downloading of support snapshots fails if it takes longer than a minute.
- Ping via the clean and dirty interface is now allowed in tgsh.
- Kibana (used in the admin portal's dashboard) has been replaced with Grafana.
- Security and bug fixes

Known Issues

- Firmware updates may sometimes fail to apply during the update process itself. Should this happen, these updates will be retried during the reboot process following any successful reconfiguration run.