Release Notes for Cisco Threat Grid Appliance Version 2.8

First Published: 2019-10-01

Last Modified: 2019-11-08

Introduction

This document describes the new features, open issues, and closed issues in Cisco Threat Grid Appliance Version 2.8.

User Documentation

The following Threat Grid Appliance user documentation is available:

Threat Grid Appliance User Documentation

Threat Grid Appliance user documentation is available on the Threat Grid Appliance Install and Upgrade Guides page on the Cisco website.

Note Newer documentation is being made available from the Threat Grid 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 Threat Grid Appliance with newer versions, you must have completed the initial setup and configuration steps as described inthe AMP Threat Grid Appliance Setup and Configuration Guide, which are available on the Threat Grid 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.

Threat Grid Appliance updates are applied through the OpAdmin 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.

Version 2.8ag

Release Date: November 8, 2019

Build Number: 2019.07.20191108T182546.srchash.3a75349f9864.rel

This release differs from Version 2.8 only by permitting custom airgap update media to be generated with a fallback license to use if no valid license is currently installed.

Version 2.8

Release Date: Oct 1, 2019

Build Number: 2019.07.20191001T173332.srchash.6fc11c8fe8c6.rel

This release updates core Threat Grid software to follow the cloud 3.5.35 release; substantially reworks how software updates are applied; adds functionality to reset the software loadout to a known state **without** clearing installed data; and incorporates various other enhancements and fixes.

Important **INSTALLING THIS UPDATE UPGRADES BIOS AND CIMC FIRMWARE. DO NOT REBOOT OR POWER OFF THE SYSTEM WHILE THIS IS TAKING PLACE.**

Fixes and Updates

The following fixes and updates are included in Version 2.8:

- The core Threat Grid application is updated to release 3.5.35.
- The URL endpoint used for OpenDNS integration has been updated to reflect changes in the cloud environment.
- Cloud Search Federation is available. Should a cloud endpoint be configured (on the integrations page in the administrative interface), the application UI will provide an option to rerun a search query against the Threat Grid Cloud.
- Software updates are now applied by installing entire system images, rather than updating individual packages. This prevents drift between installed systems and the base image, makes update downloads smaller, and makes airgap update media easier to generate (and thus available sooner after a release's online availability).
- Graphs related to legacy services which no longer exist in current software releases are removed.
- Service restarts needed for the old_tls_enabled setting to take effect now take place automatically when configuration is applied.
- Installing this release of the Threat Grid Appliance software will update your system firmware as follows:

- TG5xx0 hardware is updated to BIOS 3.0(4b) and CIMC 3.0(4m) TG5xx4 hardware is updated to BIOS 4.0(2d) and CIMC 4.0(2h)

This firmware update will take place at the end of the normal software upgrade process, while the appliance is unavailable. This may take over 30 minutes, during which the chassis and appliance should NOT be powered-off or restarted.

- Network configuration in recovery mode is now functional even if the primary system cannot be mounted or configured.
- Added Stolon Keeper timeout to avoid possible hang on shutdown.
- Inability to check the active database encoding no longer triggers the same high-severity error intended for cases when an incorrect database encoding is in use.
- SSH authentication-phase timeout is revised to 60 seconds.
- The CLI configuration tool now has the option to configure a session idle timeout, honored in both opadmin and face.

Known Issues

- Like its immediate predecessor, this release creates backup copies of the VM images on the RAID-1 storage array, to be used in the event of a reset following a bulk-storage failure. Early Cisco Threat Grid Appliance models (based on the UCS C220-M3 platform) have less storage than later models, and are more likely than other units to have less than 25% of disk space remaining available on the RAID-1 filesystem after installing this release, which will trigger a service notice.

  For later model hardware, being at less than 25% remaining storage on the RAID-1 array after installing this release is abnormal and may be raised to customer support.
- 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. A future release may provide a service notice when this has occurred.

Security Updates

The BIOS and CIMC updates listed above contain a substantial amount of security-related content. Refer to Cisco UCS documentation for the above-mentioned BIOS and CIMC firmware releases for details.