Release Notes for Cisco Threat Grid Appliance Version 2.9

First Published: 2019-12-12

Last Modified: 2019-12-17

Introduction

This document describes the new features, open issues, and closed issues in Cisco Threat Grid Appliance Version 2.9.

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 2.9mfg

Release Date: December 17, 2019

Build Number: 2019.09.20191217T061826.srchash.ee4e1ec4f2c7.rel

This release differs from Version 2.9 only by providing a MFG NFS fix that differentiates host names during installation.

Version 2.9

Release Date: December 12, 2019

Build Number: 2019.09.20191212T010702.srchash.6195db15f97a.rel

This release updates core Threat Grid software to follow the cloud 3.5.39 release; allows the admin interface to be disabled (when disabled, non-clustered appliances can operate correctly with only the clean and dirty ports connected); improves robustness when used with unreliable NFS servers, and includes various other improvements.

Fixes and Updates

The following fixes and updates are included in Version 2.9:

- The core Threat Grid application is updated to release 3.5.39. Note that this update synchronizes the scoring threshold for samples to be considered malicious with current cloud behavior at 90 versus the prior 95.
- Backup maintenance of VM images has been decoupled from the online-update process, preventing failures in the reset of systems which have been updated via an airgap ISO rather than online download.
- A scenario wherein an invalid remote-syslog configuration could render a system unable to be configured without customer-support assistance has been resolved.
- The encryption layer used for NFS storage is patched to avoid crashes when spurious ESTALE results are received from the server. Note that these errors may still cause data corruption, and it is strongly encouraged that any customer encountering them investigate the cause on the NFS server's side.
- The password for the admin user of the primary Threat Grid interface is now initialized from the user-provided password set when first logging into the administrative web UI.
- Disabling the physical admin port is now allowed. When disabled, non-clustered appliances can operate correctly with only the clean and dirty ports connected, and the admin UI will be presented on port 8443 of the clean interface. If the port is not disabled, unplugging the admin port results in a non-functional (or at best, a partially-functional) appliance.
- Default self-signed certificate generation has been modified to generate certificates which are accepted by MacOS 10.15 (Catalina).

- A rare scenario wherein RAID array hardware-health checks could hang is detected and alerted on.
- The underlying mechanism used to collect per-service status metrics is substantially reworked.
- An issue that could prevent a cluster which has been out-of-sync for an extended time from successfully resynchronizing is resolved.
- An issue that could prevent failed services that are only active in clustered configurations from being restarted on failure has been addressed.

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.