Release Notes for Cisco Threat Grid Appliance Version 2.14

First Published: 2021-08-05

Last Modified: 2021-08-19

Introduction

This document describes the new features, open issues, and closed issues in Cisco Threat Grid Appliance Version 2.14.

It also includes the Release Notes and What's New for Cisco Threat Grid Portal software version 3.5.85.

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 Information

Version 2.14.0

- Release Date: August 5, 2021
- Build Number: 2021.06.20210805T173332.srchash.f274d94a9b65.rel
- Refreshes to 3.5.85, includes Modern browser support.

Fixes and Updates

Version 2.14.0

This release includes the following fixes and updates:

- The core application software has been updated to match cloud version 3.5.85. Notably, this is the first appliance release to offer a VM image with modern browser support.
- For customers who have licensed the optional Japanese/Korean VM images, these images are now based on Windows 10 rather than Windows 7.
- The recovery image is now more robustly installed; its bootloader and the system image this bootloader invokes are installed on both OS and data drive arrays.
- A new user-invokable service is added to allow pcap captures of network traffic to/from the appliance to be saved to NFS.
- An issue that could prevent customers who used remote exit support before this feature was a standard part of the product from switching away from remote-exit-only mode has been resolved.
- The Admin UI now provides a warning when remote exit support is being selected but no remote exit configuration has been downloaded. This issue primarily impacts airgapped customers and brand new installs, as remote exit configuration is downloaded while checking for updates.
- HTTP Strict Transport Security headers for the core application have been enabled.
- Resolves a race condition that could cause some filesystem images with application components to not be activated at boot time, resulting in VMs being unavailable or other feature limitations until the next reboot. The system will now recover and mount the filesystems if this condition occurs.
- An issue that prevented service notifications from being created when no successful database backup had yet been completed has been resolved.

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.

Threat Grid Portal Release Notes and What's New

This section includes the release notes and what's new for Cisco Threat Grid Portal.

Threat Grid Portal Release 3.5.85

First released to Threat Grid Cloud portal on June 17, 2021.

Fixes and Updates

- Glovebox - This release adds a button to the running **Submissions** page that allows you to launch the Glovebox virtual machine in a new window during analysis.

  To open the Glovebox VM during sample analysis, click the **Open Glovebox Virtual Machine** button located at the bottom of the details section on the **Submissions** page. A new browser window opens with the contents of the sample. If the sample submission is a URL, the webpage will be launched within the Glovebox VM.

- XLM Support - XLM is a macro that is embedded inside the XLS file type. It uses functions such as AVERAGE or SUM in common usage. In malicious form, it can also import data from outside sources and execute files. Threat Grid has seen a large number of malicious documents using these macros, which avoid the common detection of VBA macros. With this release Threat Grid now has the ability to parse XLM macros stored within Excel files.

Behavioral Indicators

- 8 New Behavioral Indicators.
- 13 Modified Behavioral Indicators.

What's New

For detailed information about what's new in Threat Grid Portal release 3.5.85, see the online Help.