Release Notes for Cisco Threat Grid Appliance Version 2.12

First Published: 2020-11-10

Last Modified: 2021-04-08

Introduction

This document describes the new features, open issues, and closed issues in the following Cisco Threat Grid Appliance Versions:

- 2.12.0
- 2.12.0.1
- 2.12.0.1ag
- 2.12.1
- 2.12.2
- 2.12.3
- 2.12.3ag

It also includes the release notes and what's new for Cisco Threat Grid Portal software version 3.5.62.

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 2.12.3ag

- Release Date: April 8, 2021
- Build Number: 2020.04.20210408T003014.srchash.e0a6f81ee2b7.rel
- 2.12.3 plus fixes only relevant to airgap installation.

Version 2.12.3

- Release Date: March 27, 2021
- Build Number: 2020.04.20210327T023915.srchash.cd88b2c098bc.rel
- Backup fix, RADIUS fixes, ClamAV bump.

Version 2.12.2

- Release Date: February 9, 2021
- Build Number: 2020.04.20210209T215218.srchash.b91029c46829.rel
- SFP fix, sudo backport, sync-service migration fix.

Version 2.12.1ag

- Release Date: December 18, 2020
- Build Number: 2020.04.20201218T221855.srchash.4d2c8e5aec68.rel
- Same as v2.12.1 plus airgap installation fixes.

Version 2.12.1

- Release Date: December 17, 2020
- Build Number: 2020.04.20201217T221834.srchash.40ff39c7654f.rel
- Signed documents, Prometheus export.

Version 2.12.0.1ag

- Release Date: November 7, 2020
- Build Number: 2020.04.20201107T011654.srchash.a6a02730b42f.rel
- Same as v2.12.0.1 plus airgap installation fixes.

Version 2.12.0.1

- Release Date: November 5, 2020
- Build Number: 2020.04.20201105T010610.srchash.0f8ff86ad922.rel
- This release provides extensive enhancements to product security and robustness; Improves administrative functionality; Refresh to 3.5.62.

Version 2.12.0

- Release Date: October 23, 2020
- Build Number: 2020.04.20201023T235216.srchash.3b87775455e9.rel
- Internal release only.

Fixes and Updates

Version 2.12.3ag

This release is same as v2.12.3 plus airgap installation fixes.

Version 2.12.3

This release is focused on fixes.

Note Review the 2.12.0.1 and 2.12.1 release notes if upgrading to this release directly from 2.11.x.

- Resolved an issue where RADIUS authentication was not correctly enabled; this was a result of some architectural changes implemented in v2.12.0.
- ClamAV version has been updated.

- Resolved an issue where backup services with dependencies on NFS were not being scheduled to run as expected in some situations. Backup services are now being properly scheduled and run.
- Resolved an issue where checking for updates could cause a configuration file to be placed at an erroneous path and changes to configuration in the Admin UI would no longer be properly applied. The configuration file now always appears in the correct location.
- Resolved an issue that prohibited users from changing authentication modes in the Admin UI.

Version 2.12.2

This release is focused on fixes.

Note Review the 2.12.0.1 and 2.12.1 release notes if upgrading to this release directly from 2.11.x.

- As a side effect of boot security enhancements made in 2.12.0, the set of supported SFPs on appliance models with ixgbe-based network adapters was artificially restricted for earlier 2.12.x releases. This is now addressed, such that the list of supported SFPs matches that for 2.11.x.
- An updated version of sudo has been included to patch CVE-2021-3156.
- For new 2.12.x series appliance installations, some database migrations were not being run; this is now repaired. Installations restored from backups or upgraded appliances are unaffected.

Version 2.12.1ag

This release is same as v2.12.1 plus airgap installation fixes.

Version 2.12.1

This release adds feature improvements (with a focus on monitoring and ease-of-support) on top of the under-the-hood enhancements present in 2.12.0.x.

Note Review the 2.12.0.1 release notes if upgrading to this release directly from 2.11.x.

The following fixes and updates are included in this release:

- A feature is now available to allow engineering to provide (via customer support) signed, cleartext documents which run a selected command on an appliance and return its output to the user. This permits investigation and remediation of issues on airgapped appliances, and others used by customers who are unable to provide support staff with remote access, even when the specific investigatory steps required were not anticipated when software development was underway.
- Metrics generated by various services on the appliance are now exported in a format readable by Prometheus and compatible tools. This permits customers to attach appliances to their own (Prometheus-compatible) monitoring and metrics framework, and receive metrics describing the status of the underlying components within the appliance's software stack.

  Note that this functionality is considered beta and subject-to-change; customers using it should carefully review the release notes of future releases.

- For appliances which were initially installed prior to release 2.4 (or which have loaded backups created by systems originally installed with such a release), daily Elastic Search indices will be "rolled up" into monthly ones. This prevents a failure mode where an appliance could be rendered inoperable if the number of file descriptors required to open all indices exceeded the number available.
- Freezer storage is now pruned by bucket size, not only file count. This means that storage utilization for samples and related content will not exceed the amounts described in the data retention documentation; but also means that the retention period may be lower than that described in said documentation, if samples or derived content have an average size larger than those described.
- A detailed description of the PostgreSQL database replication state (for clusters) is now available via the GraphQL interface to the Admin UI.
- After completing first-time configuration, an appliance now tries to immediately start all services needed for regular operation rather than requiring a reboot before the system can be used.
- When the appliance is configured to permit only remote exits, a service notice is now created should those exits be unavailable.
- Pressing Enter on the keyboard in the Admin UI now is directed to any modal dialog displayed, rather than the form under it.
- New remote-exit and cloud-search endpoint configuration pushed by the update server can no longer cause service disruption when applied (unless users have made configuration changes manually that would require a service restart in the Admin UI, and then saved but did not apply them).
- Race conditions involving boot-time network configuration are resolved, including one which could prevent DNS resolution from being configured.
- When configuration steps with an associated service are rerun during a manually-triggered reconfiguration, their logs now go to the journal entry for the service backing that configuration step in addition to the log for the reconfiguration job.
- Cisco license agreements for on-premise and cloud offers are now combined into a single license: the "End User License Agreement" (EULA), which Threat Grid appliance users are required to accept the first time they log in to the appliance after the 2.12.1 update.

Version 2.12.0.1ag

This release is same as v2.12.0.1 plus airgap installation fixes.

Version 2.12.0.1

This release makes extensive changes to enhance security and robustness of the product. It also adds user-visible enhancements to administrative functionality, and upgrades the version of the core Threat Grid software included to correspond with version 3.5.62 of the cloud product.

The following fixes and updates are included in this release:

- On each reboot, the appliance is reset to a completely pristine software loadout (with code signatures checked at runtime). Configuration operations that previously happened only during a two-reboot reconfiguration cycle now happen as part of every boot cycle. This means that:
    - The reconfigure with-reinstall operation is made redundant.
    - Installing upgrades is now faster. The old upgrade process included these steps:

- Activate the single-user-mode upgrade process to be run on next boot.
- Reboot into single-user mode, configured to install the new packages.
- Install new software in single-user package-installation mode.
- Reboot into single-user mode configuration mode.
- Reconfigure the appliance in single-user configuration mode.
- Reboot into full operation mode.
- The new software is now running normally.

The new upgrade process is as follows and only involves a single reboot:

- Activate the new software to provide the root filesystem on next boot.
- Reboot into new software.
- Configuration happens as part of the regular boot process.
- The new software is now running normally.

- The GNU GRUB bootloader is completely removed from the Threat Grid Appliance software stack. The prior configuration did not allow unsigned configuration files to be loaded (and was not vulnerable to CVE-2020-10713), whereas the new boot mechanism entirely removes GRUB.
- Logs, active configuration, and other customer-owned data are now stored almost exclusively on the RAID 5 data array, rather than being distributed between data and OS drives. The remaining appliance-specific content stored on OS drives is limited to information required for correct operation of recovery mode should the data drives not be mountable, and has limited privacy impact if disclosed.
- Because less content is stored on the OS array with this release, early appliances (with smaller OS drives) are less likely to need to delete VM images other than the mandatory default image during a data reset (thus the need to download updates online before those deleted VM images become available again).
- Support for using the clean interface for NTP time synchronization (as opposed to the default use of dirty for this purpose) is now available.
- The Admin UI includes the following enhancements:
  - Allows generated SSL certificates (but not keys) to be downloaded by the user, reintroducing legacy functionality which was dropped during the rewrite.
  - Provides a friendlier notification for the user when the server is unavailable during an explicitly user-triggered reboot.
  - Displays color-coded certificate validity to match the categories used by service notices.
  - Provides a backup status page that displays the most recent time at which complete, non-incremental (where applicable) backups of PostgreSQL, Elasticsearch, and sandcastle freezer data were successfully completed.
- Some configuration operations in tgsh which were not properly supported (such as options to modify admin email, glovebox URL, SMTP configuration, etc) have been removed.

- Wipe operations (to render a system inoperable until remanufacturing and permanently destroy all data contained, for use before return of hardware to the Demo Loan Program) are no longer activated from the bootloader menu, but rather via a command invocation within recovery-mode `tgsh`. This should not be mistaken with usage for the reset operation (which leaves a system operable with an empty database, but does not provide the same guarantees as to forensic non-recoverability), which has not changed.
- Configuration files for the Threat Grid application are now generated in a fully repeatable manner, rather than by the applying deltas to prior configuration. This change reduces the number of ways an appliance's history or upgrade path can modify its current behavior, which will result in more consistent and supportable behavior. In consequence, some configuration changes can no longer be performed by customer support. In particular, customers who have had support modify the default VM selection on their behalf must make this change in the Threat Grid application for their selected default to be honored going forward.
- Automated detection and remediation is available if the DHCP leases assigned to VM guests are not reclaimed after a guest has exited. This issue has previously been observed when network connectivity to the network exit in use has been lost, and is thus only known to occur with remote exit support enabled.

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 Release 3.5.62

First released to Threat Grid Cloud portal on July 30, 2020.

Fixes and Updates

This release only includes behavioral indicator changes:

- 11 New Behavioral Indicators
- 11 Modified Behavioral Indicators