Cisco Threat Grid Appliance Release Notes

Version: 2.7.2ag

Last Updated: 8/8/2019

Cisco Systems, Inc. www.cisco.com

All contents are Copyright © 2015-2019 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Contents

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 in the 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.

Build Number/Release Version Lookup Table

Build Number	Release Version	Release Date	Notes
2019.02.20190808T000800.srchash.b61789e86a09.rel	2.7.2ag	8/8/2019	Air-gapped appliances only.
2019.02.20190723T224935.srchash.bb8b40c2e248.rel	2.7.2	7/23/2019	Backup pruning fix; security and M5 mfg updates.
2019.02.20190703T201951.srchash.0f2b9bc45628.rel	2.7.1	7/3/2019	Network Simulation; Migrate ES indexes to version 6.
2019.02.20190601T155353.srchash.b67f91c65917.rel	2.7	6/1/2019	Refresh to 3.5.27; ES6; XFS; Wal-G; data drives wiped on reset.
2018.12.20190204T162246.srchash.cb9269c1357f.rel	2.6	2/4/2019	Hard retention limits
2018.08.20180914205342.474e26a8.rel	2.5	9/14/2018	Win10; sample deletion. Refresh to 3.5.11
2017.12.20180601200650.e0c052b0.rel	2.4.3.3	6/1/2018	Fix cluster initialization, prune ancient ES/PG migration support
2017.12.20180519011227.ed8a11e9.rel	2.4.3.2	5/19/2018	ClamAV update for CVE-2018-1000085. Bug fixes.
2017.12.20180501005218.4e3746f4.rel	2.4.3.1	5/1/2018	PG schema reporting for DDL error detection at update check
2017.12.20180427231427.e616a2f2.rel	2.4.3	4/27/2018	Remote Virtual Exit Localization; direct standalone-to-cluster migration
2017.12.20180302174440.097e2883.rel	2.4.2	3/2/2018	Clustering
2017.12.20180219033153.bb5e549b.rel	2.4.1	2/19/2018	Clustering support in OpAdmin. Refresh application to 3.4.59

Build Number	Release Version	Release Date	Notes
2017.12.20180130110951.ce6dd56e.rel	2.4.0.1	1/30/2018	Security update to ClamAV only
2017.12.20171214191003.4b7fea16.rel	2.4	12/14/2017	Clustering EFT. jp/kr contsubs. Refresh portal to 3.4.57.
2016.05.201711300223355.1c7bd023.rel	2.3.3	11/30/2017	Starting point for 2.4 upgrade
2016.05.20171007215506.0700e1db.rel	2.3.2	10/7/2017	ElasticSearch shard count reduction.
2016.05.20170828200941.e5eab0a6.rel	2.3.1	8/28/2017	Bug fixes.
2016.05.20170810212922.28c79852.rel	2.3	8/11/2017	Automates license download. Refreshes the portal software to 3.4.47.
2016.05.20170710175041.77c0b12f.rel	2.2.4	7/10/2017	This release introduces Backup functionality.
2016.05.20170519231807.db2f167e.rel	2.2.3	5/20/2017	This minor release allows new factory installations to be run without Windows XP.
2016.05.20170508195308.b8dc88ed.rel	2.2.2	5/8/2017	Minor release of changes to network configuration and operating-system components to support upcoming features.
2016.05.20170323020633.f82e66fe.rel	2.2.1	3/24/2017	Disables SSLv3, fixes a resource issue
2016.05.20170308211223.c92516ee.rel	2.2mfg	3/8/2017	Manufacturing-only changes. No customer impact. Not deployed via update server.

Build Number	Release Version	Release Date	Notes
2016.05.20170303034712.1b205359.rel	2.2	3/3/2017	System Migration, New Portal UI, “Mask”, Multiple URLS for Disposition Service
2016.05.20170105200233.32f70432.rel	2.1.6	1/7/2017	LDAP Authentication support for OpAdmin/tgsh-dialog
2016.05.20161121134140.489f130d.rel	2.1.5	11/21/2016	ElasticSearch5; CSA performance fix
2016.05.20160905202824.f7792890.rel	2.1.4	9/5/2016	Primarily of interest to Manufacturing
2016.05.20160811044721.6af0fa61.rel	2.1.3	8/11/2016	Offline update support key, M4 wipe support
2016.05.20160715165510.baed88a3.rel	2.1.2	7/15/2016	
2016.05.20160706015125.b1fc50e5.rel-1	2.1.1	7/6/2016	
2016.05.20160621044600.092b23fc	2.1	6/21/2016	
2015.08.20160501161850.56631ccd	2.0.4	5/1/2016	Starting point for the 2.1 update. You must be at 2.0.4 before you can update to 2.1.
2015.08.20160315165529.599f2056	2.0.3	3/15/2016	Introduces AMP integration, CA mgmt., and split DNS
2015.08.20160217173404.ec264f73	2.0.2	2/18/2016	
2015.08.20160211192648.7e3d2e3a	2.0.1	2/12/2016	
2015.08.20160131061029.8b6bc1d6	v2.0	2/11/2016	Force update to 2.0.1 from here
2014.10.20160115122111.1f09cb5f	v1.4.6	1/27/2016	Starting point for the 2.0.4 update
2014.10.20151123133427.898f70c2	v1.4.5	11/25/2015	
2014.10.20151116154826.9af96403	v1.4.4		

Build Number	Release Version	Release Date	Notes
2014.10.20151020111307.3f124cd2	v1.4.3		
2014.10.20150904134201.ef4843e7	v1.4.2		
2014.10.20150824161909.4ba773cb	v1.4.1		
2014.10.20150822201138.8934fa1d	v1.4		
2014.10.20150805134744.4ce05d84	v1.3		
2014.10.20150709144003.b4d4171c	v1.2.1		
2014.10.20150326161410.44cd33f3	v1.2		
2014.10.20150203155143+hotfix1.b06f7b4f	v1.1 +hotfix1		
2014.10.20150203155142.b06f7b4f	v1.1		
2014.10.20141125162160+hotfix2.8afc5e2f	v1.0 +hotfix2		**NOTE:** The 1.0+hotfix2 is a mandatory update that fixes the update system itself to be able to handle large files without breaking.
2014.10.20141125162158.8afc5e2f	v1.0		

Version 2.7.2ag

This release is identical to Threat Grid Appliance release 2.7.2, except insofar as it adds support for a more efficient and compact offline update media generation mechanism.

Version 2.7.2

This release fixes an issue that caused NFS backups to require excessive storage in releases 2.7.0 and 2.7.1; and adds the ability to enable access to opadmin over the clean interface (as an explicit toggle in the console).

Fixes and Updates

- Database base backups are now only retained until a new base backup has been successfully created.
- The console configuration interface now supports a `enable_clean_opadmin` option, disabled by default, which (after applying configuration and rebooting) enables access to the administrative interface at port 8443 on the assigned clean IP.

Security Updates

Updates redis for data corruption fixes, including CVE-2019-10192 and CVE-2019-10193.

Version 2.7.1

This release adds network simulation support for appliances, implements mitigations for some security issues, fixes a bug which could cause cluster setup to fail after doing a data reset on 2.7.0, implements a background migration for compatibility with future releases based on newer versions of Elasticsearch, and makes various smaller improvements.

Fixes and Updates

- Network simulation is now available on appliances, resolving a known limitation in 2.7.0.
- The exit section of the appliance-configuration UI now has an additional mode wherein only locally-simulated network is available to VMs. With this option administratively selected, API and UI users cannot select any option which would send network traffic from VMs to destinations outside of the local appliance.
- Background Elasticsearch index migration to ES6-native indexes is enabled as of this release. This migration must successfully complete before any version of the Threat Grid Appliance which requires Elasticsearch 7.0 or newer is installed.
- Misspelling a configuration option name in the command-line configuration tool is now handled with a more meaningful error message.
- An issue which could cause clusters which had their configuration modified by support (rather than being installed and configured strictly through supported UI processes) to fail when upgraded to 2.7.0 has been resolved.
- Facilities for querying status or manually triggering execution of scheduled background jobs has been improved.

Known Issues

Elasticsearch index migration may cause substantial delays in the NFS backup process, causing warnings related to same. These warnings should be disregarded while service notices indicate that index migration is actively ongoing, and raised with support only should the index migration process fail to make progress over an extended period.

Security Updates

- Mitigate CVE-2019-11477, CVE-2019-11478 and CVE-2019-11479 by disabling TCP selective acknowledgment support, and dropping packets requesting a maximum segment size below 300 bytes.
- Mitigate CVE-2019-7608 by disabling Kibana Timelion support.
- Patch bzip2 to incorporate fix for CVE-2019-12900.

Version 2.7

This release updates core Threat Grid software to follow the cloud 3.5.27 release, moves to Elasticsearch 6.5, and makes several enhancements to appliance-specific tools and infrastructure.

Fixes and Updates

- The scope of sample deletion functionality has been extended to include artifacts, matching behavior of the cloud product.
- The data reset process is now more comprehensive; while the wipe process (in the recovery bootloader menu) is still required for a firm guarantee of destruction of all customer-related data, the reset process now clears operating-system logs and other state which was previously left in place.

  A successfully reset appliance will have a new randomly-generated password displayed on its console (identical to behavior in newly-installed state).

  Note that this improved process now reboots multiple times, and can be invoked from recovery mode (as opposed to the prior process, which could only be successfully invoked when booted into regular-operation).
- TLSv1.0 and TLSv1.1 are disabled on the admin interface, and disabled by default for the main application. If one of these protocols is required for integration compatibility purposes, they can be reenabled (for the main application only) from tgsh.
- Elasticsearch 6.5.4 is used for the core Threat Grid application's searchable datastore. Note that there will be a background migration required to update historical indexes before any future release supporting only Elasticsearch 7.x can be installed without data loss; please pay attention to future versions' release notes.
- Hostname: Appliances now use their serial number as their hostname, for better interoperability with some NFSv4 servers.
- Appliances initially manufactured with this release or later will use XFS as their primary filesystem. This change does not impact preexisting devices, except as otherwise described.
- If appliances have their data reset, their datastore will change over to XFS. This improves forward compatibility and provides OS-level support for I/O usage monitoring on a per-service basis.
- WAL-E is no longer maintained, so it is replaced with WAL-G for PostgreSQL backup/restore. Existing WAL-E archives will remain compatible and restoring large backups should take significantly less time for PostgreSQL.
- The list of IP addresses used for customer support connections should DNS resolution not be correctly operating when support mode is enabled is updated to accurately reflect the servers used in production at this time.
- Configuring a SSH public key for access to the appliance now disables password-based authentication via SSH, making SSH authentication methods one-or-the-other but not both. (After a successful SSH connection using key-based authentication, tgsh-dialog will prompt for a password, such that both tokens are required).

- Network configuration in recovery mode now mirrors the full system: All interfaces are brought up; firewall rules and policy routing restricting which processes can communicate on which interfaces are in-play; etc. (Note that support mode traffic on port 19791 is allow-listed across all three interfaces).
- The tools used to display system-monitoring graphs are updated in this release. Historical system-monitoring data is not preserved through this migration.

Known Issues

Network simulation support is not yet supported on the appliance, contrary to upstream 3.5.27 documentation.

Other Notes

The data reset process now requires sufficient storage to contain all content necessary for a fresh install on the system's SSDs; only after presence and validity of this content has been ensured is any preexisting data deleted. It is conceivable that systems (particularly first-generation hardware), which have been in use for an extended period, may not have sufficient space immediately available; customer support can assist if needed.

Version 2.6

Released 2/4/2019

This release updates core Threat Grid software to follow the cloud 3.5.19 release, and includes under-the-hood enhancements to allow a shorter release cycle going forward.

Fixes and Updates

- A configuration option is available to make retention-period limits strictly enforced (not storing artifacts from analysis for more than 15 days, even if storage availability would permit a longer period). This is disabled by default.
- Microsoft Office is now included on the optional Japanese and Korean VM images.
- An issue which could cause a configuration failure when migrating a standalone node to be the initial node of a cluster has been addressed.
- An issue which could cause `tgsh` commands (that ran a pager, modified service status, or adjusted the local timezone) to fail, has been addressed.
- A scenario in which Elasticsearch could end up in a loop (due to a watchdog timeout insufficient to permit inconsistent indices to be repaired/recovered on startup), has been addressed.

Version 2.5

Released 9/14/2018

This release updates core Threat Grid software to follow the cloud 3.5 series.

This is the first appliance release to include support for Windows 10.

Installing this update will modify account names for ESA/CSA devices integrated with this appliance (as the prior names could leak sensitive information). Any issues encountered in this process will be reported under the title "Device Name Migration". No changes to your ESA or CSA devices should be necessary. Please contact customer support with any questions.

Fixes and Updates

- Windows 10 VM support has been added.
- Sample deletion support is now available on appliances. (Note that deleting samples which were originally uploaded prior to installing this release may not remove copies of the sample stored elsewhere on the appliance; however, these additional copies are subject to the retention rules documented for "Disk Artifacts" in *Threat Grid Appliance Data Retention Notes* and will eventually age out as new content is added.)
- VM storage format has been modified to improve storage and update efficiency going forward.
- Tools used to generate system-monitoring graphs have been updated; expect any direct URLs to change.
- Disabling NFS is now better-supported on an appliance which has already completed configuration.
- Attached USB storage devices can no longer generate spurious SMART hardware status warnings.
- IP fragmentation settings have been modified to mitigate any denial-of-service attacks using CVE-2018-5391. (Note that these attacks would need to be launched from a customer network, not by sandboxed malware, to be effective).
- The entire system is now built with a more recent version of gcc, enabling full retpoline support in the kernel.
- Corrupt redis stores are automatically remediated even if clustering is not enabled, fixing a regression introduced in 2.4.0.

Version 2.4.3.3

Released 6/1/2018

This point release addresses an issue in the database initialization process when creating a new cluster from scratch (new clusters initialized from a backup created by a standalone appliance are not affected); and removes some unused software libraries.

Fixes and Updates

- This is a proactive remediation -- customers who already initialized a cluster with a blank database will receive a service notice with the text "Database encoding is not set correctly", and should contact customer support to schedule a retroactive fix.
- Customers who are not preparing to create an appliance cluster do not need to install this update.
- **Data Migration from Pre-2.2 Releases No Longer Supported:**

  Note that due to the removal of unused code, appliances which never had the ElasticSearch 5 migration run successfully (at the end of the 2.1 series) no longer ship with tools that permit customer support to perform this migration after-the-fact.

  Similarly, systems for which PostgreSQL was never updated to 9.6 (which similarly took place prior to 2.2.0), no longer ship with tools permitting this update to be done belatedly.

  Systems without these migrations complete would not have worked correctly with any 2.3 or 2.4 release, and would have displayed a service notice when running 2.1.6 directing the user to permit migrations to complete or contact customer support prior to performing any further update. Always ensure that a system is in generally good working order before applying an update, unless given specific contrary advice from release notes or customer support.

Version 2.4.3.2

Released 5/19/2018

This point release includes one security update and two bug fixes.

Fixes and Updates

- ClamAV is updated, addressing CVE-2018-1000085.
- Enhances the update mechanism to allow repair of a condition where the `win7-x64` virtual machine could be unavailable.

  This condition only impacts systems which were previously updated to 2.4.1 or later.

  An update download must complete successfully after 2.4.3.2's installation, followed by a reboot, to apply this fix.
- A software fault could prevent samples from being run until after at least one update check was performed following the installation of 2.4.3 or later. This is now corrected.

If updating from a pre-2.4.3 release, see also the 2.4.3 and the 2.4.3.1 release notes.

Version 2.4.3.1

Released 5/1/2018

Additionally, 2.4.3.1 adds diagnostic reporting of database schema anomalies. No customer data is reported to the update server as part of this -- all reporting is metadata (DDL) only, intended to ensure reliability of future upgrades.

Version 2.4.3

Released 4/27/2018

This feature updates core Threat Grid software, adds support for promotion of standalone appliances to the initial node of a cluster without an intervening reset process, and adds a customer accessible remote exit mechanism (replacing the limited-availability "tg-tunnel" mechanism that preceded it). Customers using tg-tunnel should read these notes carefully before applying this update, and contact customer support with any questions.

Fixes and Updates

- A new version of the core Threat Grid software is used, which corresponds to cloud portal release 3.4.65.

  Note that feature availability may differ between cloud and appliance software. Differences in the APIs are noted in the relevant sections of the API documents. Differences in the UI are described in the portal online help: Help > Introduction to Threat Grid > Threat Grid Cloud and Appliances Comparison.

- Standalone appliances with data backed up to NFS no longer require a database reset and restore-from-backup to become the initial node of a new cluster.

- Remote exit support is available. If activated (this feature is on by default only for appliances previously configured to use tg-tunnel), this tunnels traffic from malware VMs to a Cisco datacenter, and from there to an exit location.

  Note that new keys to use with this service are retrieved when software updates are downloaded (even if no update is available). This means that at least one update check must take place before this service can be used; that an appliance with an expired license may not be able to retrieve new keys, and thus may lose access to this service; and that appliances which only install updates via the offline update mechanism may not use this service.

- The manner in which virtual machines are stored has been changed to reduce the minimum possible amount of data transfer needed when small changes to VMs are deployed.

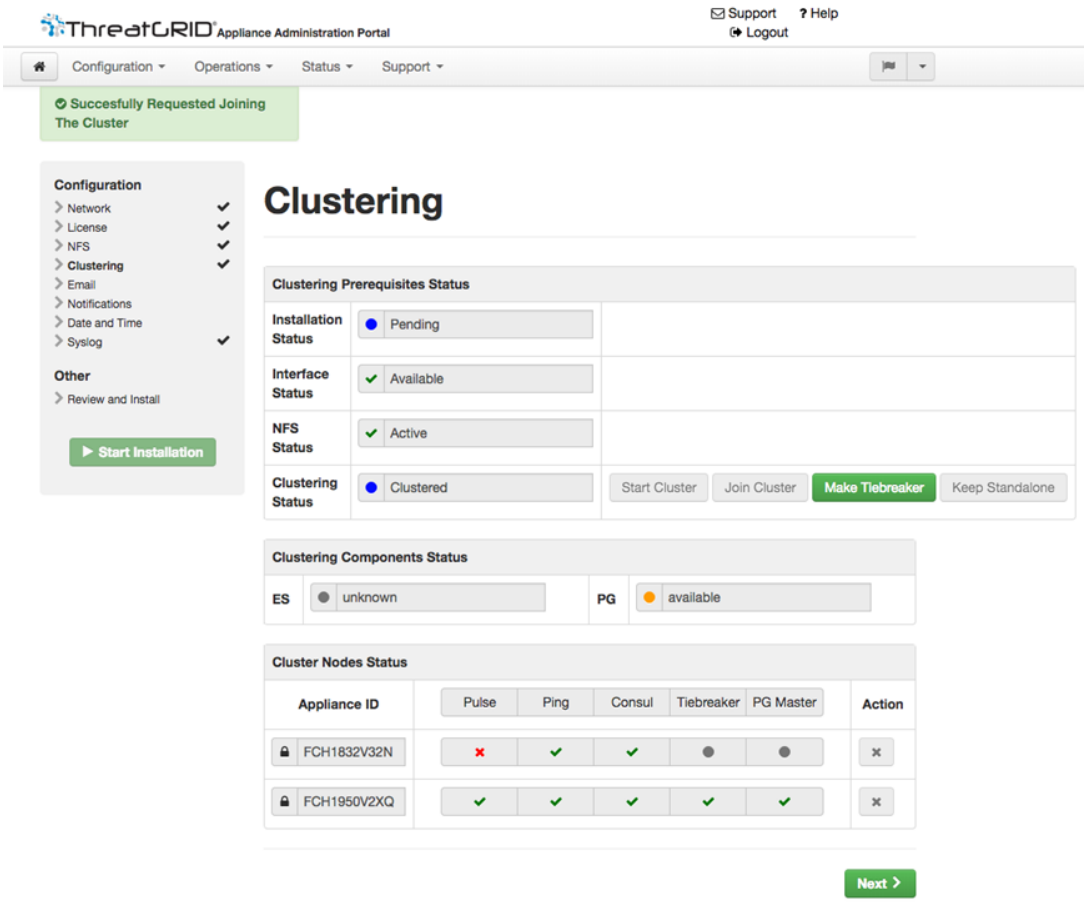
Version 2.4.2

Released 3/2/2018

This is the first release in which appliance clustering is generally available as a feature. Various setup and workflow improvements have been made since 2.4.1, which was the final release in which clustering was still considered to be an early field trial feature only.

Fixes and Updates

- Safety features are added to prevent a single datastore from being mounted for read/write access with the same key by multiple Threat Grid appliances, except when those appliances are members of the same cluster.
- Clustering no longer requires a license indicating participation in an early field trial.
- Resolves a scenario in which monitoring on clusters could be sporadically unable to determine Elasticsearch cluster health after extended uptime.
- NFS settings may no longer be updated when actively mounted. An unmount option is available in the OpAdmin administrative interface when a node is not part of a cluster.
- Resolves an issue that could cause failed negotiations for customers who are tunneling outbound traffic through Threat Grid data centers.
- The new Clustering configuration page:



Version 2.4.1

Released 2/19/2018

This release updates the core Threat Grid software, and introduces configuration UI for appliance cluster setup and maintenance.

This release also fixes a bug that could permit an appliance to enter a state where it could not run new sample analysis operations until rebooting, makes numerous stability improvements to clustering support, and folds in security updates previously only available in the 2.4.0.1 interim release.

Fixes and Updates

- A new version of the core Threat Grid software is used, which corresponds to cloud portal release 3.4.59; notably, this includes enhancements to the sample report. For details see the release notes available in the portal online help (*Help > Release Notes*).

  (Note that feature availability may differ between Threat Grid cloud and appliance software. For more information, see the documentation. Differences are noted in the relevant sections of the API documents. Differences in the UI are described in the portal online help: *Help > Introduction to Threat Grid > Threat Grid Cloud and Appliances Comparison*.)

- The "supervisor" component failing could leave large amounts of ramdisk storage allocated if numerous virtual machines were running at the time, preventing further analysis operations from taking place until the appliance was rebooted. This is now resolved.

- Numerous stability improvements have been made to clustering support.

- Clustering status is exposed in the OpAdmin UI. Customers participating in the clustering EFT can build a cluster from a standalone node; add a new appliance with an empty database to an existing cluster; see cluster status; determine whether a cluster is fault-tolerant; remove dead nodes; and see and (where possible) control which nodes are holding roles which may incur service interruption during failover or transition events.

Known Issues

- Clustering: If a system is improperly removed and wiped, without using the "Remove" option in the UI to inform other nodes of its removal, then databases mirroring to it may fail if the system is re-added.

- NFS/Clustering Safety:

  — Safety features are not yet active to prevent users from attempting to share a single NFS datastore: across multiple non-clustered appliances, between a cluster and one or more non-clustered appliances, or between multiple distinct clusters.

  — Only install encryption keys associated with a pre-existing backup store as explicitly directed by documentation or customer support.

- NFS: The Administrative (OpAdmin) UI does not currently prohibit making changes to the NFS configuration after the configuration has been activated. Making such changes is an unsupported operation, particularly when a node is a member of a cluster, and taking this action will have unspecified consequences up to and including data loss.

Security Updates

The security fixes introduced in the interim release 2.4.0.1 are carried through and included in this regular release.

Version 2.4.0.1

Released 1/30/2018

This interim release updates ClamAV to 0.99.3. Installing this update promptly is strongly encouraged.

Fixes and Updates

- A file descriptor leak which could prevent virus definitions from being updated is addressed.

Security Updates

Addresses exposure to the following:

- CVE-2017-12374
- CVE-2017-12375
- CVE-2017-12376
- CVE-2017-12377
- CVE-2017-12378
- CVE-2017-12379
- CVE-2017-12380

Version 2.4

Released 12/14/2017

This release updates core Threat Grid software; adds support for optional VMs (including ones containing separately-licensed 3rd-party software) that are available for download as updates; and introduces limited-availability clustering support as a pre-release feature for customers participating in early field trials.

Fixes and Updates

- A new version of the core Threat Grid software is used, which corresponds to cloud portal release 3.4.57. (Feature availability may differ between cloud and appliance software; see documentation).
- VM distribution uses a new, more bandwidth-efficient mechanism, which avoids downloading content that is shared between multiple VMs more than once, and allows different VMs to be distributed to different customers. Note: This mechanism is also present in a 2.3.x release being generated specifically to support update to 2.4.0.
- A new VM, "win7-x64-2", is available to all customers.
- A new VM, "win7-x64-kr", is available for download by customers whose license indicates purchase of a license to run Hancom Office on their Threat Grid appliance. Other optional VMs (with further 3rd-party licensed software of locale-specific interest or use), may be available in the near future.
- Clustering: Pre-release support for building a cluster of multiple appliances is introduced. This requires additional hardware, and is presently only available for customers who are eligible for, and have opted into, an early field trial.

Version 2.3.3

Released 11/302017

This release introduces a more efficient update system. The new update system will download only the components that changed between subsequent virtual machine releases, and will avoid downloading shared software components between multiple virtual machines more than once.

Required:

This release **must** be installed before the upcoming Threat Grid Appliance 2.4.0 release can be downloaded.

Fixes and Updates

- VM distribution uses a new mechanism that increases bandwidth efficiency. It avoids downloading content that is shared between multiple VMs more than once, and allows different VMs to be distributed to different customers.

Version 2.3.2

Released 10/7/2017

This release addresses a high-priority search issue when running version 2.2 or later. Search functionality and related APIs could fail when search evaluates data that has been added on more than a certain number of dates. (Note that dates are only included in the calculation if they contain indexed data, i.e., data from at least one sample analysis.)

Fixes and Updates

- Indexes used for search are migrated in a manner which improves efficiency and increases (by a factor of 5) the number of days of search data which can be queried. (Future updates will raise this limit further.)
- Licenses retrieved over the network no longer have a NUL character on the end. (This did not impact validity or usability of such licenses.)
- Various updates were introduced to support upcoming, unreleased functionality.

Version 2.3.1

Released 8/28/2017

This release addresses some issues in the 2.3.0 release impacting appliances updated from prior releases.

Fixes and Updates

- An issue which could prevent data added in 2.1.4 or earlier from being present in some search results is resolved.
- An issue which could prevent appliances initially installed with software version 1.2.x and upgraded directly to 1.4.x from being able to successfully apply the 2.3.0 update is resolved.
- The organizational administration page again correctly shows per-org rate limit configuration, rather than presenting organizational-level licensing configuration only applicable to the cloud product.

Version 2.3

Released 8/11/2017

This release updates core Threat Grid software; removes VMs which are no longer actively tested and supported by the cloud product; moves to a higher-performance network implementation for customers not tunneling malware traffic; implements a honeypot for SMTP traffic; and blocks outbound SSH from malware (matching behavior of the cloud service in this manner). It also introduces automatic license retrieval: If an appliance is Internet-connected, it can attempt to retrieve a license (or a replacement for an expired license) via network. Note that automated retrieval is at present only available for licenses sold or renewed after the release of this software (2017-08-11).

While use of IPv4LL (169.254.0.0/16) address ranges was never tested and supported, these are now *explicitly unsupported*, and must not be used.

Fixes and Updates

- A new version of the core Threat Grid software is used, which corresponds to cloud portal release 3.4.47. (Feature availability may differ between cloud and appliance software; see the portal Release Notes located in the UI Help for details.)
- Only VMs which are actively tested and maintained as part of the cloud product are present: Windows XP is removed, even from appliances where they were previously grandfathered in. Windows 7 is now 64-bit only.
- Samples submitted to `winxp` or `win7-x86` VMs are still available. Note that any scripts or clients which hardcoded `winxp` should be changed.
- Except where tunneling is in use, outbound network traffic from malware is using a higher-performance mechanism for egress from the virtual machine. This allows outbound unencrypted SMTP to be sandboxed local to the appliance.
- Outbound SSH from sandboxed VMs is now blocked.
- A situation where NTP could fail to sync due to failed DNS lookup for the time server is mooted: The NTP service will periodically restart if it has no peers.

Version 2.2.4

Released 7/10/2017

This release introduces a backup feature:

Threat Grid appliances now support encrypted backups to NFS-backed storage; initialization of data from such storage; and reset to an empty-database state into which such a backup can be loaded.

(Note that reset is different from the wipe process used to allow an appliance to be shipped off customer premises without information leakage. The wipe process appropriate for that purpose already exists in the recovery bootloader, but is NOT suitable for preparing a system to restore a backup; reset is for backup preparation.)

Extended documentation regarding the backup functionality is available, and we strongly encourage consulting it prior to use. Please see the Backup Notes and FAQ for technical information and instructions.

Fixes and Updates

- Backup to, and restore from, a customer-provided NFSv4 store is now supported.
- A limited data-reset operation is now available for preparing a system to restore a backup. (The reset operation applies to database content, but unlike the secure wipe option available in recovery mode, will not make an appliance permanently unusable.)
- Fixes a regression introduced in 2.2.2, which could prevent network traffic from routing to the local network (other than the gateway) when DHCP is in use, or when network interfaces are hotplugged or reconfigured after boot.

Version 2.2.3

Released 5/19/2017

Threat Grid appliances manufactured on or after 2017-07-01 (July 1, 2017), will no longer include licensing or distribution of Windows XP, in compliance with Microsoft requirements. This minor release allows new factory installations to be run without Windows XP.

Installing this release will not remove Windows XP from an appliance where it was previously available.

This also fixes some issues which could cause a successful update check to be reported as failed in OpAdmin when the clean interface did not have an associated DNS server configured. Note that if the "Run Update" button is displayed, an update can be safely attempted, *even if* the "Update Check Error" notice is present.

Important Note

If upgrading from a pre-2.2 release, please read the Appliance 2.2 release notes:

http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-release- notes-v2-2.pdf

Fixes and Updates

- The "Document Created an Executable File" indicator can no longer be triggered when the executable created is whitelisted. (
- Monitoring and logging services (kiries and syslog-ng) now start properly when no clean-network DNS server is configured. (
- A successful update check is now correctly reported as such in OpAdmin even if notifications regarding that check could not be sent. (
- In accordance with Microsoft licensing requirements, this version of the Threat Grid Appliance is capable of being installed without Windows XP.

Security Updates

OpenSSL is revved to 1.0.2k.

Version 2.2.2

Released 5/8/2017

This minor release makes changes to network configuration and operating-system components in support of features which will be added in upcoming releases. It fixes a bug in support mode which could cause all future connections to support servers to fail after a connection without a successful TLS handshake (until the service was restarted), and a bug which could prevent new antivirus signatures from being downloaded and installed.

Important Note

Please read the Appliance 2.2 release notes (http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-release-notes-v2-2.pdf) if upgrading from a pre-2.2 release.

Bug Fixes

- Support mode is no longer rendered inoperable after an interrupted TLS handshake.
- An issue which could prevent new antivirus signatures from being downloaded is fixed.
- Orphaned intake queue elements are now cleaned up automatically.

Enhancements

If DNS servers are both provided on the clean interface via DHCP and configured for that same interface via OpAdmin, both will be used.

Version 2.2.1

Released 3/24/2017

IMPORTANT NOTE

Note that 2.2.x MUST NOT BE INSTALLED if the ElasticSearch migration introduced in version 2.1.5 and still available and functioning in 2.1.6 is incomplete. Please contact customer support with any questions:

support@threatgrid.com

This minor release fixes a performance issue in 2.2 that could become severe over time. It partially mitigates the impact of installing 2.2 without allowing the ElasticSearch migration in 2.1.5 and 2.1.6 to fully complete. This release also removes long-deprecated support for SSLv3; and ensures that JVM-based services can successfully recover from out-of-memory conditions.

If upgrading from a pre-2.2 release please read the Appliance 2.2 Release Notes located at:

http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-release-notes-v2-2.pdf

New Features

The appliance can now recover from having had a 2.2-series release installed without allowing the ES5 migration in 2.1.5 and 2.1.6 to fully complete.

NOTE THAT THIS IS A PARTIAL MITIGATION.

Whereas in releases 2.1.5 and 2.1.6 this migration process has no impact whatsoever on integrity and availability, in 2.2.x, new content added to an index while that index is being migrated may be **LOST** at the completion of the migration process for that index. Therefore, we **strongly** recommend that 2.2.x not be installed until **after** the ElasticSearch migration in 2.1.5 or 2.1.6 has completed in full.

Bug Fixes

Analysis processes handling specific kinds of network events no longer use excessive amounts of time and memory or crash the analysis service.

Security Fixes

SSLv3 is no longer required, and this long-deprecated protocol is now disabled.

Version 2.2mfg

Released 3/8/2017

Manufacturing-only changes. No customer impact. Not deployed via update server.

Version 2.2

Released 3/3/2017

REQUIREMENT

The ElasticSearch migration **must be completed** in 2.1.5/2.1.6 before installing 2.2.

Documentation

Reviewing the AMP Threat Grid Appliance Migration Note and Data Retention Note is **strongly** recommended.

- AMP Threat Grid Appliance Migration Note v2.2:

http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-migration-note-v2-2.pdf

- AMP Threat Grid Appliance Data Retention Note:

http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-data-retention-v2-2.pdf

About This Release

Release 2.2 greatly increases storage efficiency to make disk capacity available that had not been usable on systems initially installed with 1.x releases.

IMPORTANT NOTE:

This last feature implements pruning - removal - of old content in the future. While all content is migrated, older content – especially carved disk and network artifacts that are produced in extremely high volume and only rarely used – may be removed on an ongoing basis to ensure continued operation. See the *Data Retention Note* linked above for details.

With this release, the Threat Grid Appliance is at version parity with Threat Grid Cloud release 3.4.37. (Note that this does not imply complete *feature* parity: Features requiring hardware, services, 3rd-party licenses or other content or facilities only available on the cloud may remain unavailable on the appliance).

That said, several 3rd-party detection and enrichment service integrations which were previously cloud-only can now be configured for the appliance; this includes VirusTotal, OpenDNS and TitaniumCloud. Moreover, the appliance can automatically download updates to ClamAV signatures daily, improving recognition of known malware.

New Features

The application version shipped has numerous new features, including:

- Support for configuring multiple URLs for Disposition Update service notifications.
- Content that is stored in the traditional archival format is migrated to one which allows more efficient decompression and per-datatype storage differentiation.
- VirusTotal, OpenDNS and TitaniumCloud integrations can now be configured on the appliance.
- ClamAV signatures can be automatically updated on a daily basis. This is enabled by default, and can be disabled from the newly-added Integrations page in OpAdmin.

- Failed sample invocations can be automatically retried, thereby reducing the effective overall failure rate.
- The application frontend converts all timestamps into the viewing browser's local timezone. In consequence, non-UTC timezones for the appliance itself are no longer needed, and will no longer be honored.
- *Mask* UI- Version 3.4.37 of the Threat Grid Portal features a UI enhancement seen on the appliance for the first time with release 2.2.

NOTE: *Mask* replaces the legacy *Face* interface, although users are still given the option to switch back and forth. *Mask* includes numerous enhancements, including a complete redesign of the Analysis Report. For more information please see the Portal Release Notes, which are available from the application's online help page. (From the portal's UI navigation bar at the top of the page, click the **Help** button to open the main help page.)

Bug Fixes

- Disk space that was inaccessible on appliances initially installed with 1.x releases, due to the use of MBR partition tables, is now allocated and accessible.
- Systems upgraded from 1.x releases now can invoke the recovery bootloader even if the primary bootloader is corrupt or unavailable.

Security Fixes

- Updates the underlying virtualization technology to address a potential buffer overflow in the VGA driver.

Version 2.1.6

Released 1/5/2017

The 2.1.6 release adds LDAP authentication and authorization to the Threat Grid Appliance administrator's interface, and also includes various architectural improvements related to unreleased/upcoming features.

New Features

Both OpAdmin and the TGSH Dialog interface may be configured for LDAP authentication. Note that this does not extend to the application interface.

Known Issues

Disk I/O throughput graphs contain only reads and writes to the operating system's dedicated filesystem, rather than to customer-owned data. This frequently means that no I/O is shown at all, as the system is built to minimize interaction with the root filesystem after startup is complete.

Version 2.1.5

Released 11/21/2016

This release greatly improves CSA API query performance, improving robustness and speed of integration with Cisco ESA and WSA devices. It also upgrades various backend components for robustness and future-proofing.

Important Note: Note that CSA API performance improvements are seen only after a migration process which runs in the background after the release is installed has completed; please read the tech note accompanying this release for details, available at this link:

http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-migration-note-v2-1-5.pdf.

New Features

The core application has been modified to support ElasticSearch versions newer than 1.x.

ElasticSearch versions 2.x and 5.x are both supported (migration to 2.0 is mandatory before 5.0 can be used), in addition to the prior 1.7.x release.

PostgreSQL is upgraded to version 9.6.1.

Automated recovery following transient failures is extended to a wider array of internal services.

Bug Fixes

Prevent delays in the clean network successfully retrieving an address via DHCP from preventing successful service startup or reconfiguration on upgrade.

Relax timeouts for ElasticSearch, to reduce the number of failures even before upgrading to native-5.0.

Major-version database upgrades are now less vulnerable to being incorrectly marked as failed and rolled back.

Application components which rely on ElasticSearch can no longer be started before ElasticSearch has completed initialization.

Known Issues

Disk I/O throughput graphs contain only reads and writes to the operating system's dedicated filesystem, rather than to customer-owned data. This frequently means that no I/O is shown at all, as the system is built to minimize interaction with the root filesystem after startup is complete.

Version 2.1.4

Released 9/5/2016

This release resolves numerous issues related to hardware support, particularly those issues that are prerequisites to providing support for software updates to air-gapped appliances.

New Features

Monitoring and reporting is now available for scenarios where the ElasticSearch service is under excessive load.

Bug Fixes

Support for automatically restarting failed services is extended (after a delay) to services which have failed with enough frequency to be temporarily disabled.

A scenario where some internal services could fail to start due to a delay in redis initialization has been addressed.

Storage device name or ID changes no longer prevent the system from booting successfully.

System wipe is now fully supported on TG-5004-K9 and TG-5504-K9 hardware.

Known Issues

Disk I/O throughput graphs contain only reads and writes to the operating system's dedicated filesystem, rather than to customer-owned data. This frequently means that no I/O is shown at all, as the system is built to minimize interaction with the root filesystem after startup is complete.

Version 2.1.3

Released 8/11/2016

This release resolves numerous issues related to hardware support, particularly those issues that are prerequisites to providing support for software updates to airgapped appliances.

New Features

Monitoring and reporting is now available for scenarios where the ElasticSearch service is under excessive load.

Bug Fixes

- Support for automatically restarting failed services is extended (after a delay) to services which have failed with enough frequency to be temporarily disabled.
- A scenario where some internal services could fail to start due to a delay in redis initialization has been addressed.
- Storage device name or ID changes no longer prevent the system from booting successfully.
- System wipe is now fully supported on TG-5004-K9 and TG-5504-K9 hardware.

Known Issues

Disk I/O throughput graphs contain only reads and writes to the operating system's dedicated filesystem, rather than to customer-owned data. This frequently means that no I/O is shown at all, as the system is built to minimize interaction with the root filesystem after startup is complete.

Version 2.1.2

Released 7/15/2016

This is a minor bugfix release.

Bug Fixes

- An unclean shutdown can no longer leave the system in a state where the redis key/value store blocks service startup.
- A regression in qemu connectivity to tg-tunnel (for customers using this off-by-default feature) has been resolved.
- Modifying a system to no longer use tg-tunnel is now an automated process.

Known Issues

- Wipe support is known to be broken on TG-5004-K9 and TG-5504-K9 hardware with some specific BIOS releases. This is expected to be resolved prior to this hardware's release.
- Disk I/O throughput graphs contain only reads and writes to the operating system's dedicated filesystem, rather than to customer-owned data. This frequently means that no I/O is shown at all, as the system is built to minimize interaction with the root filesystem after startup is complete.

Version 2.1.1

Released 7/6/2016

This release addresses some issues in separate clean-network DNS support, resolves an important security bug, and provides various minor fixes and improvements.

New Features

- SMART warnings regarding potential hard drive failures can be silenced by the user by modifying their visibility setting, which will prevent any further notices of the same error until and unless the nature or status of the error changes.

Bug Fixes

- Separate clean-network DNS now functions correctly.
- A spurious warning during post-reconfiguration backup is avoided.

Security Fixes

- CVE-2016-1443 is addressed.
- SSH is no longer enabled by default in recovery mode.

Known Issues

- Wipe support is known to be broken on TG-5004-K9 and TG-5504-K9 hardware with some specific BIOS releases. This is expected to be resolved prior to this hardware's release.
- Disk I/O throughput graphs contain only reads and writes to the operating system's dedicated filesystem, rather than to customer-owned data. This frequently means that no I/O is shown at all, as the system is built to minimize interaction with the root filesystem after startup is complete.

Version 2.1

Released 6/21/2016

Important Note: The starting point for this update is v2.0.4. You must be at version 2.0.4 before you can upgrade to version 2.1.

This release fully supports upcoming hardware revisions, incorporates numerous security enhancements, and moves to a contemporary release of the Threat Grid Portal product.

New Features

- File types `js`, `dot`, `dotx`, and `dotm` can now be submitted as malicious to FireAMP Private Cloud via the Disposition Update Service.
- On all hardware, module loading and kexec are disabled at runtime to reduce exposure to kernel-based rootkits, and signatures of the operating system kernel and initrd are validated by the bootloader before invocation.
- Service notices related to hard drive SMART warnings can be hidden in such a way that they can only be automatically re-opened if their contents change.
- Database transactions that are left open for excessive periods of time are detected and reported as service notices, which supports remediation before the scenario has become so severe as to require extended downtime to repair.

Bug Fixes

- Glovebox reliability is greatly improved.
- Network reliability is improved in recovery mode in scenarios where a network interface requires an extended amount of time to become ready.
- Service notices related to hardware errors from IPMI could incorrectly claim that the number of warnings active was 0.
- NTP failures no longer cause service notices to be raised before system configuration has been completed.
- Failures due to expected services not being active cannot be logged until at least 10 minutes after boot, allowing time for services to initialize properly.

Security Fixes

- The underlying virtualization technology is updated to address a potential buffer overflow in the VGA driver.

Known Issues

- Wipe support is known to be broken on TG-5004-K9 and TG-5504-K9 hardware with some specific BIOS releases. This is expected to be resolved prior to this hardware's release.
- Disk I/O throughput graphs contain only reads and writes to the operating system's dedicated filesystem, rather than to customer-owned data. This frequently means that no I/O is shown at all, as the system is built to minimize interaction with the root filesystem after startup is complete.

Version 2.0.4

Released 5/1/2016

Important Note: The starting point for this update is v1.4.6. You must be at version 1.4.6 or newer before you can complete the 2.0.4 update.

This release includes numerous reliability improvements and bugfixes.

Note that boot times may be slower, particularly for appliances with a large amount of data; however, this increase in boot time resolves several failures which could happen shortly after boot.

New Features

- SMTP connections made for email alerting now can take advantage of locally configured certificate authorities.
- Disposition Update Service integration has been improved, and is fully compatible with FireAMP Private Cloud release 2.2.0.

Bug Fixes

- The appliance now updates the disposition indexes so they match their intended state. This fixes several customer-impacting bugs, which could be caused by an inconsistent or out-of-date index state.
- The appliance waits for the ElasticSearch cluster to be fully available before starting dependent services.
- The amount of memory allocated for ElasticSearch, and thus the maximum possible amount of data which can be indexed in ElasticSearch without error, has been increased.
- Temporary bootloader configuration overrides, such as those put in place during the upgrade from 1.x to 2.x, are cleared. In consequence, a scenario which could cause an appliance previously upgraded from a 1.x release to present an upgrade-mode menu when recovery mode is in use has been resolved.
- A bug which could cause email alerting to fail has been resolved.

Version 2.0.3

Released 3/15/2016

This point release introduces a number of features to support FireAMP Private Cloud device integrations. These include the ability to split DNS between the Clean and Dirty interfaces, CA Management, and FireAMP Integration Configuration.

Generated SSL certificates now have the CN duplicated as a subjectAltName. This addresses an incompatibility with SSL clients which ignore the CN field when at least one subjectAltName is present. It may be necessary to regenerate any previously appliance-generated certificates if using such tools.

Version 2.0.2

Released 2/18/2016

This bugfix-only release addresses an urgent security issue.

Security Updates

The GNU C library is patched to address CVE-2015-7547 and CVE-2015-1781.

Version 2.0.1

Released 2/12/2016

This bugfix-only release corrects some issues present in 2.0.

Bug Fixes

Calls to check a device's quota are no longer counted against that quota.

An issue that could occasionally cause an appliance to hang at boot time has been solved.

Known Issues

Disk I/O throughput graphs contain only reads and writes to the operating system's dedicated filesystem, rather than to customer-owned data. This frequently means that no I/O is shown at all, as the system is built to minimize interaction with the root filesystem after startup is complete.

Version 2.0

Released 2/11/2016

Important Note: Force update to 2.0.1 from here.

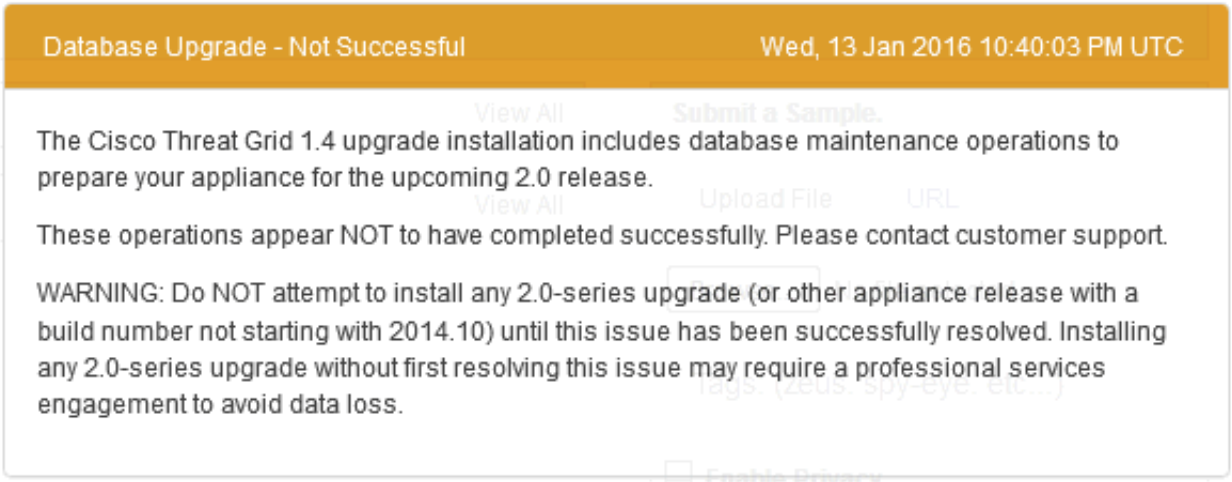
This is a major release, built upon an updated operating system. It includes enhancements that will support future hardware releases, and is able to use the same software as the Threat Grid Cloud Portal product.

Please note that the 2.0 upgrade can take some time, up to several hours, with a large ElasticSearch database.

First, complete the 1.4.6 upgrade, which is the immediate step before 2.0.

DO NOT interrupt the upgrade before it is completed, as doing so may require support remediation. The best method for checking on the status of an ongoing upgrade is via console access.

After the 1.4.6 upgrade is complete, and before continuing on to the 2.0 upgrade, check the notices in the Threat Grid Portal to verify whether or not the following error has occurred:



Database Upgrade Not Successful Notice

A "*Database Upgrade - Not Successful*" message means that a new appliance is running an older version of PostgreSQL than it's supposed to, and the automatic database migration process has failed.

If you do not see the error notice, then you may proceed with the 2.0 upgrade.

Time Required for 2.0 Upgrade

Please note that the 2.0 upgrade can take some time - up to several hours - with a large ElasticSearch database.

DO NOT interrupt the upgrade before it is completed, as doing so may require support remediation. The best method for checking on the status of an ongoing upgrade is via console access.

The following Threat Grid Appliance-specific updates are also included:

New Features

- Windows 7 64-bit VMs are now supported.
- Traces that are initiated by customer support are now automatically rotated and deleted, so they can be run for longer periods of time without the risk of exhausting available space.
- Internal configuration backups are more exhaustive, allowing an appliance to be recovered without major data loss even should both SSDs fail.

Bug Fixes

- Unauthenticated SMTP works correctly even with mail servers that advertise authentication with an empty method list (particularly, Microsoft Exchange).
- Service notices regarding failures during the nightly updates download are now delivered properly.

Security Fixes

- Application-level notices regarding account creation or CSA device (i.e., ESA/WSA/etc.) registration are sent to the first email address that has been configured for notice alerts. If no address is configured, the notices will not be sent. (Previous release versions sent these notices to admin@test.threatgrid.com, which could potentially result in data leakage.)
- OpenSSL is updated to version 1.0.2f.

Known Issues

Disk I/O throughput graphs contain only reads and writes to the operating system's dedicated filesystem, rather than to customer-owned data. This frequently means that no I/O is shown at all, as the system is built to minimize interaction with the root filesystem after startup is complete.

Future releases may modify the way I/O usage is determined to work around this issue.

Version 1.4.6

Released 1/27/2016

Release 1.4.6 installs tools used during the upgrade to 2.0.

New Features

Appliances at release 1.4.6 are eligible for upgrade to the 2.0 release.

Version 1.4.5

11/25/2015

The Wipe Appliance feature is now functional on demo appliances that were shipped with 1.4.4. For more information, please see the "Wipe Appliance" section in the Threat Grid Appliance Administrator's Guide.

Version 1.4.4

This release fixes a critical issue impacting license validation, and addresses a bug which was preventing errors in the nightly update check from being presented to the user.

IMPORTANT: If upgrading from a release prior to 1.4, be sure to read the release notes for version 1.4, below.

Bug Fixes

- License validation no longer attempts to rebuild an internal read-only database (which could result in licenses being falsely rejected as invalid).

- Errors in the nightly update check are now correctly displayed to the user.

Version 1.4.3

This release includes minor security updates for the underlying virtualization infrastructure, and adds a user-accessible mechanism to wipe an appliance's disks (for decommissioning or return of borrowed hardware to the Cisco Demo Loan Program).

New Features

- **Wipe:** A new boot menu option is available that will allow you to wipe the disks on a Threat Grid Appliance. Note that after performing this operation, the appliance will no longer operate without being returned to Cisco for reimaging.

Security Updates

- A potential denial-of-service using crafted Ethernet packets to cause running samples to hang is no longer possible.

Known Issues

- In rare circumstances, VM analysis on Windows XP has been known to fail. Video for the sample analysis will show a black screen when this occurs. This failure is independent of the individual sample; if this occurs, resubmitting the sample (or switching to Windows 7) is suggested.

Version 1.4.2

This release updates the underlying virtualization technology used in the product, and bundles several small but important bug-fixes.

IMPORTANT: If upgrading from a release prior to 1.4, be sure to read the release notes for version 1.4, below.

Bug Fixes

- Flash (SWF) documents are now correctly activated.

- Support for interacting with live sample analysis runs in the "Glovebox" tool is now compatible with new security defaults in Firefox 40.

- The "Regenerate" button generates SSL certificates acceptable to some software and tools which previously rejected them.

- Windows 7 virtual machines are no longer prone to hanging during execution.

Known Issues

- In rare circumstances, VM analysis on Windows XP has been known to fail. Video for the sample analysis will show a black screen when this occurs. This failure is independent of the individual sample; if this occurs, resubmitting the sample (or switching to Windows 7) is suggested.

Version 1.4.1

This release updates the Windows 7 image incorporated in the product, suppressing the Microsoft Office activation dialog.

Upgrading from a Release Prior to 1.4

Important Note: If upgrading from a release prior to 1.4, be sure to read the release notes for version 1.4, below.

Bug Fixes

- When analyzing Microsoft Office documents using Windows 7, the Microsoft Office activation dialog is no longer displayed.

- Use of customer support tools for analysis of system behavior early in the boot process no longer results in a service notice when these tools are no longer active.

Version 1.4

This release is focused on storage-format changes that are necessary to prepare for upgrade to the upcoming 2.0 release.

IMPORTANT:

For appliances that were initially shipped with 1.0-series software, with a large amount of database content, this upgrade may require a longer-than-usual maintenance window to apply.

For appliances that initially shipped with a software release prior to 1.2, which have been in use for several months, we suggest that you allow 90 minutes for the upgrade to be applied.

For appliances that had sample data transferred from a pre-1.0 (non-Cisco-branded) device, the upgrade process may take even longer; please contact customer support with any questions.

New Features

- Upgrades database storage on all appliances to use a build of PostgreSQL 9.4 compatible with standard upstream database releases.

- Re-added APPLY button to tgsh-dialog, with a new function: Completes self-configuration and update tasks in the same manner as performed after a system update. May be used to repair a system that has been left in an inconsistent state after an aborted update attempt.

- Added a mechanism by which customer support may select the default virtual machine used for jobs triggered by other Cisco devices.

Bug Fixes

- Updates with new virtual machine images are no longer prone to failure if system write performance is degraded.

- Update jobs that are invoked from the console are no longer prone to being incorrectly described as failed in Opadmin.

- Service notices are no longer created during the upgrade process.

- Incorrect filename extensions that were being generated for some Microsoft Office document types have been fixed.

Version 1.3

This release adds a significant number of appliance-specific features, including: remote syslog support; email alerting of system-level issues; and availability of performance graphs. This release moves to a slightly newer version of the ThreatGRID service implementing support for integration with Cisco FireSIGHT Management Center products. The release also incorporates appliance-specific bug fixes.

Note that remote syslogs -- if configured -- use the clean interface for outbound traffic. Please see the updated administrative documentation for 1.3 for more information.

New Features

- Emailed notices can be configured to trigger on system monitoring events.

- Button added to the SSL configuration page of the administrative interface generate new self-signed SSL certificates.

- Graphs for CPU, I/O, and memory usage over time are available in the administrative interface.

- Network interface names at the operating system level now match their logical names ("clean", "dirty", "admin") as used in the documentation.

- Hotplugging network interfaces is supported; an interface need not be plugged in at boot time to be able to function later, and interfaces which require DHCP refresh on hotplug events will do so. (Interfaces requiring SFPs still must have those SFPs installed at boot).

- Failed services are automatically restarted.

- Failed services generate service notices in the application.

- Failed attempts at NTP synchronization generate service notices in the application.

- Excessive database checkpoint backlog causes a user-visible warning.

- Added a service notice for free space events.

- Added release note contents to service notices regarding upgrade availability.

Bug Fixes

- Netmasks with high bits beyond /24 are no longer truncated prematurely.

Security Updates

- Patches qemu to disable exploits via CD-ROM driver; see CVE-2015-5154.

- Opportunities for local privilege escalations via application debugging interfaces mitigated.

Other Notes

- EULA terms updated.

Version 1.2.1

This updates the ThreatGRID appliance to be based on software from a newer version of the cloud service. Key among features added is support for integration with other Cisco appliances -- including ESA and WSA appliances.

No appliance-specific code or infrastructure is modified in this release.

New Features

- Support for the Cisco Sandboxing API

Security Updates

- Patches qemu to disable floppy controller emulation, avoiding CVE-2015-3456

Version 1.2

This point release improves integration with other Cisco products, streamlines the software update process, and adds hardware monitoring support.

New Features

- Checks for software updates now happen automatically in the background on a nightly basis.

- Notice is now provided inside the Threat Grid application when a software update is available.

Bugs Fixed

- Software updates no longer time out on slow connections.

- Samples that are being processed at the time of a shutdown or a reboot are no longer lost or inserted as duplicates. After the 1.2 update is applied, sample processing delays shutdown until the process has reached an appropriate stopping point. Sample processing resumes once the appliance has booted back up. (Previously, sample processing could result in a much longer delay in system shutdown as well as the loss of samples.)

- "502 Bad Gateway" errors no longer occur while the appliance is booting up.

- NTP (Network Time Protocol) synchronization now occurs correctly.

- Generated SSL certificate serial numbers are now unique across all apppliances. **NOTE:** This fix only impacts systems that were first installed with version 1.2 or newer.

- A storage misconfiguration that was causing appliances to run out of disk space after processing a relatively low number of samples has been fixed.

- Audit logs now corrrectly show the client IP address.

- Text on the SSH key configuration page correctly reflects that this configures keys for the threatgrid user, not root.

- Password reset links in generated emails are now correct.

Security Updates

- Session cookies for the administrative interface are no longer portable across Threat Grid appliances.

- OpenSSL is upgraded to incorporate upstream fixes.

Other Improvements

- On appliances that are first installed with version 1.2 or newer, the PostgreSQL database uses a storage format binary-compatible with upstream PostgreSQL and related projects such as EnterpriseDB.

Known Issues

- Before Windows 7 jobs can be run, the following user intervention is required:

1. Log into the primary ThreatGRID application console on the clean interface) as the admin user. 2. Click **Welcome Admin** in the top right-hand corner to access the drop-down menu. 3. Click **Manage Orgs**. 4. Click **Initial Organization**. 5. In the **Additional VMS** field, enter **win7**. 6. Click **Update**.

After this has been done, when submitting a sample, under **Advanced Options**,

the user can select **win7**.

- Licensing parsing is sensitive to text file format. Licenses must be stored in UNIX text files -- with lines delimited by CR rather than CRLF.

Version 1.1 Hotfix 1

Hotfix 1 is identical to 1.1, but also fixes a bug that impacts update download reliability over slow connections.

Version 1.1

This point release adds several new features to the Threat Grid appliance (including Window 7 support), and fixes several bugs.

New Features

- Windows 7 support has been added.

- Email can be sent via mail servers connected on the appliance's **Clean** network, rather than allowing only mail servers accessible via the **Dirty** (i.e., malware) interface to be used.

- Support snapshots can be submitted to Threat Grid Support directly from the appliance.

- Support snapshots can be viewed prior to submission to Threat Grid Support.

- Updates can be applied from the textual (curses) interface, as opposed to the web-based administrative interface (**OpAdmin**) only.

- The system password can be successfully modified from recovery mode.

- Fewer administrative changes require a reboot to become effective.

- Added more client-side Javascript validation for GUI configuration workflow.

Bugs Fixed

- Various issues with outbound email configuration have been resolved.

- Notices inside the administrative interface are displayed correctly.

- Status of long-running jobs in the configuration UI is now streamed with minimal latency.

- Fixed a case where the administrative interface could refuse to start.

- The configuration GUI did not always accurately reflect whether a reboot was needed for configuration changes to take effect. This has been fixed.

- Removed unsupported menu items from the tgsh-dialog (curses-based) administrative interface.

Security Updates

- Updated upstream packages with known vulnerabilities (ntpd, bash, openssl).

- Configuration backups are no longer stored world-readable.

1.0+hotfix2 Update - Mandatory

The 1.0+hotfix2 is a **mandatory update** that fixes the update system itself to be able to handle large files without breaking.