Threat Grid Appliance Release Notes

Version: 2.3

Last Updated: 8/11/2017

Cisco Systems, Inc. www.cisco.com

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Cover photo Copyright © 2016 Mary C. Ecsedy. All rights reserved. Used with permission.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Contents

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

User Documentation

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

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Build Number/Release Version Lookup Table

Build Number	Release Version	Release Date	Notes
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.
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

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Build Number	Release Version	Release Date	Notes
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		
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		**NOTE:** The 1.0+hotfix2 is a mandatory update that fixes

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Build Number	Release Version	Release Date	Notes
	+hotfix2		the update system itself to be able to handle large files without breaking.
2014.10.20141125162158.8afc5e2f	v1.0		

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Version 2.2mfg

Released 3/8/2017

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

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- 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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.
- Secure Boot is fully supported when running on the upcoming TG-5004-K9 and TG-5504-K9 hardware.
- 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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

- 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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Version 2.0

Released 2/11/2016

Important Note: Force update to 2.0.1 from here.

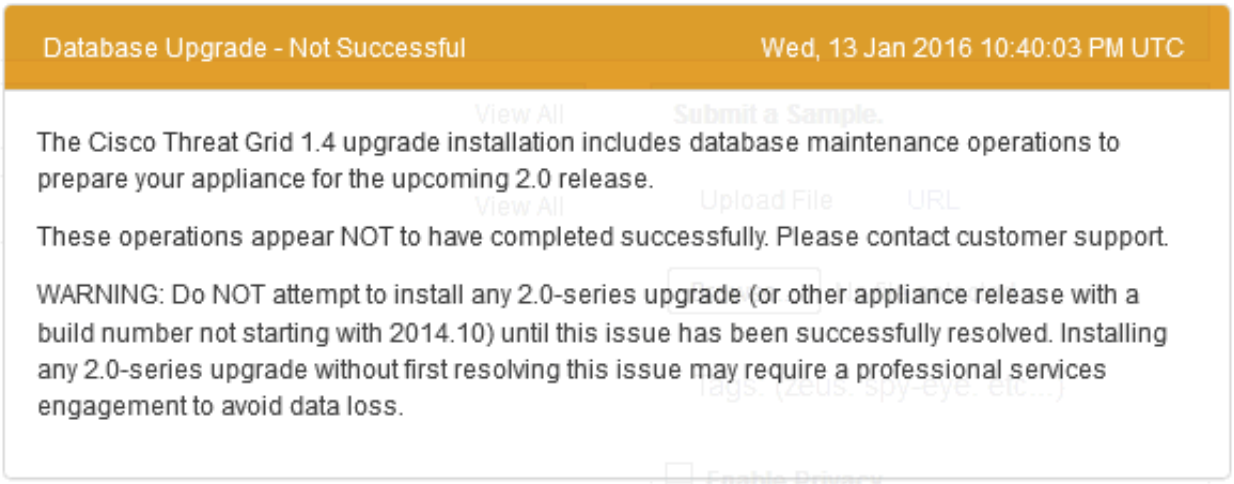
This is a major release, built upon an updated operating system. It includes enhancements that will support future hardware releases, and is able to use the same software as the Threat Grid Cloud Portal product.

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:

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Other Notes

- EULA terms updated.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

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.

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.