AMP Threat Grid 设备
版本说明

版本 2.2

最后更新日期： 2017 年 3 月 6 日

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 信头压缩是加州大学伯克莱分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。版权所有。版权所有 © 1981，加州大学董事会。

无论在该手册中是否作出了其他担保，来自这些供应商的所有文档文件和软件都按“原样”提供且仍有可能存在缺陷。思科和上面所提及的提供商拒绝所有明示或暗示担保，包括（但不限于）适销性、特定用途适用性和无侵权担保，或者因买卖或使用以及商业惯例所引发的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标的列表，请访问此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。

包装内容物

用户文档

Threat Grid 设备的用户文档可从思科网站的“Threat Grid 设备安装和升级指南”页面获取：

http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html

安装更新

您必须先按照 AMP Threat Grid 设备产品文档页面上提供的《AMP Threat Grid 设备设置和配置指南》中所述完成初始设置和配置步骤，然后才能使用更高版本更新 Threat Grid 设备。

新设备：如果您的新设备出厂时安装了较低的版本，并且您希望安装更新，则必须先完成初始配置。请在所有设备配置完成之后再应用更新。

除非已安装许可，否则将不会下载设备更新；并且，如果尚未完全配置设备（包括数据库），则可能无法正确应用设备更新。

Threat Grid 设备更新是通过 OpAdmin 门户应用的。

更新是不可逆的：在升级到最新版本后，您无法再将其恢复到先前版本。

要测试更新，请提交一个样本进行分析。

内部版本号/发行版本查询表

内部版本号	版本	发布日期	备注
2016.05.20170303034712.1b205359.rel	2.2	2017 年 3 月 3 日	系统迁移、新门户 UI - “Mask”、可为处置服务配置多个 URL
2016.05.20170105200233.32f70432.rel	2.1.6	2017 年 1 月 7 日	为 OpAdmin/tgsh-dialog 提供 LDAP 身份验证支持
2016.05.20161121134140.489f130d.rel	2.1.5	2016 年 11 月 21 日	ElasticSearch5；CSA 性能修复
2016.05.20160905202824.f7792890.rel	2.1.4	2016 年 9 月 5 日	主要面向制造业
2016.05.20160811044721.6af0fa61.rel	2.1.3	2016 年 8 月 11 日	离线更新支持密钥，支持 M4 擦除
2016.05.20160715165510.baed88a3.rel	2.1.2	2016 年 7 月 15 日	
2016.05.20160706015125.b1fc50e5.rel-1	2.1.1	2016 年 7 月 6 日	
2016.05.20160621044600.092b23fc	2.1	2016 年 6 月 21 日	
2015.08.20160501161850.56631ccd	2.0.4	2016 年 5 月 1 日	2.1 更新的起点。您必须先升级到 2.0.4，然后才能更新为 2.1。
2015.08.20160315165529.599f2056	2.0.3	2016 年 3 月 15 日	引入 AMP 集成、CA 管理和分离 DNS
2015.08.20160217173404.ec264f73	2.0.2	2016 年 2 月 18 日	
2015.08.20160211192648.7e3d2e3a	2.0.1	2016 年 2 月 12 日	
2015.08.20160131061029.8b6bc1d6	v2.0	2016 年 2 月 11 日	强制从此版本更新为 2.0.1

内部版本号	版本	发布日期	备注
2014.10.20160115122111.1f09cb5f	v1.4.6	2016 年 1 月 27 日	2.0.4 更新的起点
2014.10.20151123133427.898f70c2	v1.4.5	2015 年 11 月 25 日	
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 +hotfix2		**注意：**版本 1.0+hotfix2 是强制更新，可对更新系统本身进行修复，使该系统无需拆分大文件即可对其进行处理。
2014.10.20141125162158.8afc5e2f	v1.0		

版本 2.2

发布日期：2017 年 3 月 3 日

有关本文档和相关文档的 PDF 格式版本，请参阅以下链接指向《Threat Grid 设备安装和升级指南》：

http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html

强烈建议您阅读《AMP Threat Grid 设备迁移说明》和《数据保留说明》。

- 《AMP Threat Grid 设备迁移说明 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 设备数据保留说明》：

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

要求

必须先在 2.1.5/2.1.6 中完成 ElasticSearch 迁移，然后才能安装 2.2。

关于本版本

版本 2.2 会显著提高存储效率，使初始安装有版本 1.x 的系统上之前不可用的磁盘容量可用。

重要提示：

将来可以用这项最新功能对旧内容进行修剪（删除。尽管所有内容都会迁移，但可以不断删除比较旧的内容（特别是大量生成却极少使用的分区磁盘和网络工件）以确保持续运营。有关详细信息，请参阅上面链接的《*数据保留说明*》。

本版本的 Threat Grid 设备与 Threat Grid 云 3.4.37 版属于同等版本。（请注意，这并不意味着 *功能* 完全相等：如果功能所需的硬件、服务、第三方许可证或者其他内容或设施仅在云中可用，则相应功能在设备上仍然不可用）。

这也就是说，现在可以为设备配置几项以前只能在云中部署的第三方集成，其中包括 VirusTotal、OpenDNS 和 TitaniumCloud。不仅如此，设备还可以自动下载 ClamAV 签名的更新，从而提高对已知恶意软件的识别能力。

新功能

附带的应用版本具有许多新功能，其中包括：

- 支持为处置更新服务通知配置多个 URL。
- 以传统存档格式存储的内容已迁移为可提高解压效率并按数据类型加以区别存储的内容。
- 现在可以在设备上配置 VirusTotal、OpenDNS 和 TitaniumCloud 集成了。
- 可以每晚自动更新 ClamAV 签名。此功能默认启用，并可通过 OpAdmin 中新添加的“集成”页面禁用。
- 样本调用失败可以自动重试，从而降低有效整体失败率。
- 应用前端可将所有时间戳转换为正用来查看信息的浏览器的本地时区。因此，应用本身的非 UTC 时区将不再那么有用，并且也不再那么被人需要。
- *Mask* UI - Threat Grid 门户 3.4.37 版在 2.2 版本的设备上首次提供增强的 UI 功能。

  注意：*Mask* 取代了旧版的 *Face* 界面，但用户仍可选择在两个界面间来回切换。*Mask* 提供了许多增强功能，包括完全重新设计的分析报告。有关详细信息，请参阅该应用在线帮助页面上提供的《门户版本说明》。（在页面顶部的门户 UI 导航栏中，点击**帮助**按钮打开帮助主页。）

漏洞修复

- 起初安装了 1.x 版本的设备上因使用 MBR 分区表而不可访问的磁盘空间现在已分配和可访问。
- 现在，即使主要引导加载程序损坏或不可用，从 1.x 版本升级的系统也可调用恢复引导加载程序。

安全修复

- 已更新底层虚拟化技术以解决 VGA 驱动程序中潜在的缓冲区溢出问题。

2.1.6 版

发布日期：2017 年 1 月 5 日

版本 2.1.6 在 Threat Grid 设备的管理员界面中增加了 LDAP 身份验证和授权，还包括各种与未发布或即将发布功能相关的架构改进。

新功能

OpAdmin 和 TGSH 对话界面均可配置 LDAP 身份验证。请注意，此功能不会延伸到应用界面。

已知问题

磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

2.1.5 版

发布日期：2016 年 11 月 21 日

本版本显著改善了 CSA API 查询性能，从而提高了与思科 ESA 和 WSA 设备集成的可靠性和速度。本版本还升级了各种后端组件，以增强可靠性并适应未来的发展。

重要提示：请注意，CSA API 性能只有在完成迁移过程（本版本安装完毕后于后台运行）后才会获得改进；有关详细信息，请阅读本版本附带的技术说明（可从以下链接获取：

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

新功能

核心应用经过修改，支持版本高于 1.x 的 ElasticSearch。

除以前的 1.7.x 版本以外，还支持 ElasticSearch 版本 2.x 和 5.x（必须迁移到 2.0 后方可使用 5.0）。

PostgreSQL 已升级到版本 9.6.1。

瞬态故障后自动恢复的功能已延伸到更广泛的内部服务。

漏洞修复

对于在 clean 网络中通过 DHCP 成功检索地址时的延迟，现在可防止其在升级时阻止服务成功启动或重新配置。

放宽 ElasticSearch 超时，即使在升级到本地 5.0 前也能减少失败次数。

主要版本数据库升级现在比较不容易被错误标记为失败并回滚。

在 ElasticSearch 完成初始化之前，依赖 ElasticSearch 的应用组件无法再启动。

已知问题

磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

2.1.4 版

发布日期：2016 年 9 月 5 日

本版本解决了许多与硬件支持相关的问题，特别是为气隙式部署设备的软件更新提供支持时作为必备条件的那些问题。

新功能

监控和报告功能现在可用于 ElasticSearch 服务负载过大的场景。

漏洞修复

对失败服务自动重启的支持延伸到（在延迟后）失败频率足以将其暂时禁用的服务。

某些内部服务可能因 Redis 初始化延迟而无法启动的场景已得到解决。

存储设备名称或 ID 更改不会再阻止系统成功启动。

TG-5004-K9 和 TG-5504-K9 硬件现在完全支持系统擦除。

已知问题

磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

2.1.3 版

发布日期：2016 年 8 月 11 日

本版本解决了许多与硬件支持相关的问题，特别是为气隙式部署设备的软件更新提供支持时作为必备条件的那些问题。

新功能

监控和报告功能现在可用于 ElasticSearch 服务负载过大的场景。

漏洞修复

- 对失败服务自动重启的支持延伸到（在延迟后）失败频率足以将其暂时禁用的服务。
- 某些内部服务可能因 Redis 初始化延迟而无法启动的场景已得到解决。
- 存储设备名称或 ID 更改不会再阻止系统成功启动。
- TG-5004-K9 和 TG-5504-K9 硬件现在完全支持系统擦除。

已知问题

磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

2.1.2 版

发布日期：2016 年 7 月 15 日

本版本是漏洞修复次要版本。

漏洞修复

- 不正常关机不会再使系统处于 Redis 键/值存储阻止服务启动的状态。
- 已解决与 tg-tunnel 的 qemu 连接（对于使用此默认关闭功能的客户）的回归问题。
- 将系统修改为不再使用 tg-tunnel 现在是自动完成的过程。

已知问题

- 已知在采用某些特定 BIOS 版本的 TG-5004-K9 和 TG-5504-K9 硬件上，擦除支持会出现故障。此问题有望在该硬件发布前得到解决。
- 磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

2.1.1 版

发布日期：2016 年 7 月 6 日

本版本解决了单独的 clean-network DNS 支持方面的一些问题，修复了一个重要的安全漏洞，并提供了各种次要修复和改进。

新功能

- 用户可以通过修改有关潜在硬盘驱动器故障的 SMART 警告的可视性设置来解除这些警告，这将阻止就同一个错误发出任何进一步通知，除非错误的性质或状态有所更改。

漏洞修复

- 单独的 clean-network DNS 现在可以正常运行。
- 避免了重新配置后备份期间的假警告。

安全修复

- 已修复 CVE-2016-1443 漏洞。
- SSH 在恢复模式下不再默认启用。

已知问题

- 已知在采用某些特定 BIOS 版本的 TG-5004-K9 和 TG-5504-K9 硬件上，擦除支持会出现故障。预计在此硬件发布之前解决此问题。
- 磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

版本 2.1

发布日期：2016 年 6 月 21 日

重要提示：此更新的最低版本是 v2.0.4。您必须先升级到版本 2.0.4，然后才能升级到版本 2.1。

本版本完全支持即将发布的硬件版本，整合了许多安全增强功能，并升级到 Threat Grid 门户产品的同期版本。

新功能

- 现在可将文件类型 `js`、`dot`、`dotx` 和 `dotm` 作为恶意文件通过处置更新服务提交到 FireAMP 私有云。
- 安全启动在即将发布的 TG-5004-K9 和 TG-5504-K9 硬件上运行时受到完全支持。
- 在所有硬件上，运行时禁用模块加载和 kexec 以减少基于内核的 Rootkit 的风险，并在调用操作系统内核和 initrd 签名前由引导加载程序对其进行验证。
- 可以隐藏与硬盘驱动器 SMART 警告相关的服务通知，使其只能在内容更改的情况下自动重新打开。
- 可以检测过长时间保持打开的数据库事务并将其作为服务通知予以报告，从而有助于在这种情况恶化到需要延长停机时间进行修复之前加以补救。

漏洞修复

- Glovebox 的可靠性显著提高。
- 在网络接口需要更长时间才能准备就绪的情况下，恢复模式下的网络可靠性得到提高。
- 来自 IPMI 的硬件错误相关服务通知可能会将已有警告数误报为 0。
- NTP 失败不会再导致在系统配置完成前发出服务通知。
- 启动后至少 10 分钟内无法记录因预期服务处于非活动状态而导致的失败，留出时间供各项服务正确完成初始化。

安全修复

- 已更新底层虚拟化技术以解决 VGA 驱动程序中潜在的缓冲区溢出问题。

已知问题

- 已知在采用某些特定 BIOS 版本的 TG-5004-K9 和 TG-5504-K9 硬件上，擦除支持会出现故障。预计在此硬件发布之前解决此问题。
- 磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

2.0.4 版

发布日期：2016 年 5 月 1 日

重要提示：此更新的最低版本是 v1.4.6。您必须先升级到版本 1.4.6 或更高版本，然后才能完成 2.0.4 更新。

本版本包括许多可靠性改进和漏洞修复。

请注意，启动时间可能会减慢，特别是对具有大量数据的设备而言；但是，这种启动时间的延长解决了几个可能会在启动后不久发生的故障。

新功能

- 为邮件警报建立的 SMTP 连接现在可以充分利用本地配置的证书颁发机构。
- 处置更新服务集成得到改进，并与 FireAMP 私有云版本 2.2.0 完全兼容。

漏洞修复

- 设备现在可更新处置索引，使其符合预期状态。这样即可修复几个可能由索引状态不一致或过时而导致的客户影响漏洞。
- 设备要等待 ElasticSearch 集群完全可用后才能启动相关服务。
- 增加了为 ElasticSearch 分配的内存量，也因此增加了 ElasticSearch 中可在不出错的情况下编入索引的最大可能数据量。
- 临时启动加载程序配置覆盖（例如从 1.x 升级到 2.x 期间实施的配置覆盖）已清除。因此，已解决可能导致以前从 1.x 版本升级的设备在使用恢复模式时显示升级模式菜单的情况。
- 已解决一个可能导致邮件警报失败的漏洞。

2.0.3 版

发布日期：2016 年 3 月 15 日

此版本引入一系列功能以支持 FireAMP 私有云设备集成。这些功能包括在 Clean 和 Dirty 接口之间拆分 DNS 的功能、CA 管理和 FireAMP 集成配置。

现在，生成的 SSL 证书令 CN 复制为 subjectAltName。这解决了与 SSL 客户端的不兼容性问题，即当存在至少一个 subjectAltName 时 SSL 客户端会忽略 CN 字段。如果使用此类工具，则可能需要重新生成之前由设备生成的任何证书。

2.0.2 版

发布日期：2016 年 2 月 18 日

本漏洞修复专用版本解决了一个紧急安全问题。

安全更新

已修复 GNU C 库以修复 CVE-2015-7547 和 CVE-2015-1781 漏洞。

2.0.1 版

发布日期：2016 年 2 月 12 日

本漏洞修复专用版本更正了版本 2.0 中存在的一些问题。

漏洞修复

检查设备配额的调用不再根据该配额进行计数。

已解决一个可能偶尔导致设备在启动时挂起的问题。

已知问题

磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

版本 2.0

发布日期：2016 年 2 月 11 日

重要提示：从本版本起，强制更新为 2.0.1。

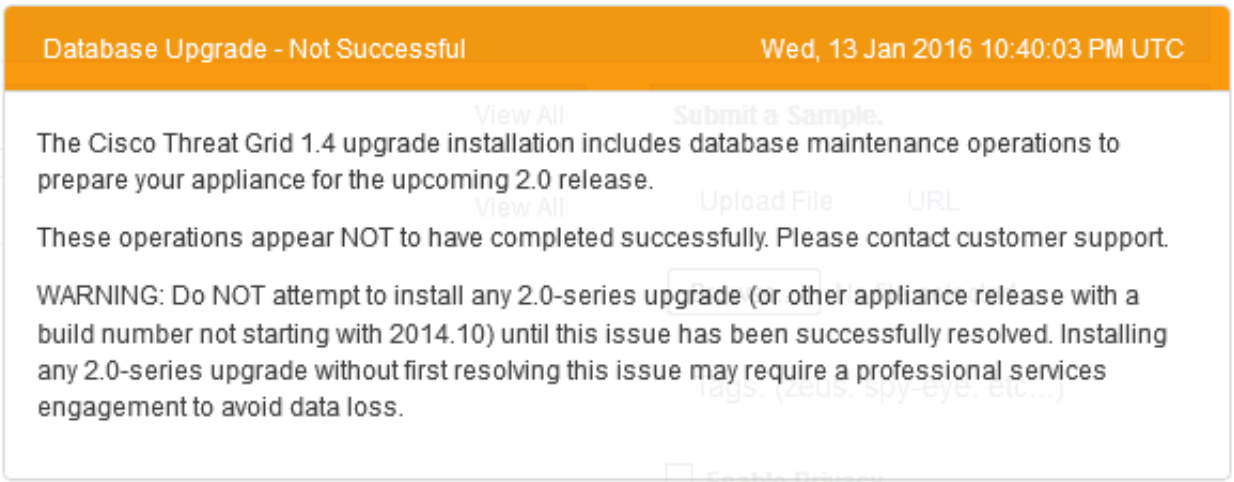
这是主要版本，基于更新的操作系统。它包括支持未来硬件版本的改进，并同 Threat Grid 云门户产品一样能够使用相同的软件。

请注意，由于 ElasticSearch 数据库容量较大，所以 2.0 版升级可能需要一些时间（最长可达数小时）。

首先，完成 1.4.6 升级，它是升级到 2.0 之前的中间步骤。

请勿中断升级过程，否则可能需要支持补救。如需查看正在进行的升级的状态，最佳办法是通过控制台访问。

在 1.4.6 升级完成之后、在继续进行 2.0 升级之前，请检查 Threat Grid 门户中的通知以验证是否出现了以下错误：



数据库升级失败通知

*“数据库升级 - 失败”*消息意味着新设备运行的是低于预期的 PostgreSQL 版本，并且自动数据库迁移过程已失败。

如果您没有看到错误通知，则可以继续执行 2.0 升级。

2.0 升级所需的时间

请注意，由于 ElasticSearch 数据库容量较大，所以 2.0 版升级可能需要一些时间（最长可达数小时）。

请勿中断升级过程，否则可能需要支持补救。如需查看正在进行的升级的状态，最佳办法是通过控制台访问。

另外，还包括以下 Threat Grid 设备特定的更新：

新功能

- 现在已支持 Windows 7 64 位虚拟机。
- 现在，系统会自动轮换并删除客户支持发起的跟踪，从而延长运行时间，而不会有耗尽可用空间的风险。
- 内部配置备份更加全面彻底，即使两个 SSD 同时发生故障，仍可使设备恢复运行，而不会造成主要数据丢失。

漏洞修复

- 即使邮件服务器使用空方法列表通告身份验证（尤其是 Microsoft Exchange），未经身份验证的 SMTP 也能正确工作。
- 现在，夜间更新下载期间相关故障的服务通知也可正确发送。

安全修复

- 有关帐户创建或 CSA 设备（即 ESA/WSA 等）注册的应用级别通知会发送到为通知提示所配置的第一个邮件地址。如果未配置任何地址，则不会发送通知。（以往的版本会将这些通知发送到 admin@test，这可能会导致数据泄露。）
- OpenSSL 已更新到版本 1.0.2f。

已知问题

磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

未来版本可能会修改决定 I/O 使用的方法以规避此问题。

1.4.6 版

发布日期：2016 年 1 月 27 日

版本 1.4.6 会安装升级到版本 2.0 过程中使用的工具。

新功能

版本 1.4.6 的设备可以升级到版本 2.0。

1.4.5 版

2015 年 11 月 25 日

现在，擦除设备功能可以在版本 1.4.4 随附的演示设备上使用。有关详细信息，请参阅《Threat Grid 设备管理员指南》中的“擦除设备”一节。

1.4.4 版

本版本修复了一个影响许可证验证的严重问题，并解决了一个阻止向用户显示夜间更新检查期间所发生错误的漏洞。

重要信息：如果从 1.4 之前的版本进行升级，请确保阅读下文版本 1.4 的版本说明。

漏洞修复

- 许可证验证不再试图重建内部只读数据库（这可能会导致许可证因无效而被错误拒绝）。
- 现在，夜间更新检查期间发生的错误可以正确地向用户显示。

1.4.3 版

本版本包括对底层虚拟化基础设施的少量安全更新，并添加一个用户可访问的机制以擦除设备的磁盘（以供卸载或将租借的硬件返回到 Cisco Demo Loan Program）。

新功能

- **擦除：**新的启动菜单选项将允许您擦除 Threat Grid 设备的磁盘。请注意，在执行此操作后，设备将不再运行，无需返回思科进行重新镜像。

安全更新

- 潜在的拒绝服务无法再使用专门设计的以太网数据包使正在运行的样本挂起。

已知问题

- 在极少数情况下，已知 Windows XP 上的 VM 分析会发生故障。当出现这种情况时，样本分析的屏幕会显示为黑屏。此故障与单个样本无关；如果发生这种情况，建议重新提交样本（或转用 Windows 7）。

1.4.2 版

本版本更新了产品中使用的底层虚拟化技术，并附带若干较小但重要的漏洞修复。

重要信息：如果从 1.4 之前的版本进行升级，请确保阅读下文版本 1.4 的版本说明。

漏洞修复

- Flash (SWF) 文档现在可以正确激活。
- 与“Glovebox”工具中运行的实时样本分析进行交互的支持现在已与 Firefox 40 中的新安全默认值兼容。
- 通过“重新生成”(Regenerate) 按钮生成的 SSL 证书可为某些软件和工具接受，但之前会被拒绝。
- Windows 7 虚拟机在执行期间不再会挂起。

已知问题

- 在极少数情况下，已知 Windows XP 上的 VM 分析会发生故障。当出现这种情况时，样本分析的屏幕会显示为黑屏。此故障与单个样本无关；如果发生这种情况，建议重新提交样本（或转用 Windows 7）。

1.4.1 版

本版本更新了产品中包含的 Windows 7 镜像，不再显示 Microsoft Office 激活对话框。

从 1.4 之前的版本升级

重要提示：如果从 1.4 之前的版本进行升级，请确保阅读下文版本 1.4 的版本说明。

漏洞修复

- 在使用 Windows 7 分析 Microsoft Office 文档时，不再显示 Microsoft Office 激活对话框。
- 使用客户支持工具分析引导过程中的系统行为不再导致出现服务通知（当这些工具不再活动时）。

版本 1.4

本版本集中解决了预备升级到即将发布的 2.0 版本所需的存储格式更改问题。

重要信息：

对于 1.0 系列软件同捆的具有大量数据库内容的设备，可能需要比平时更长的时间来应用此次升级。

对于与版本 1.2 之前的（已使用数月的）软件同捆的设备，我们建议您允许应用本次升级的时间为 90 分钟。

对于从 1.0 以下版本（非思科品牌的）设备转移样本数据的设备，升级过程可能会需要更长时间；如果有任何问题，请联系客户支持。

新功能

- 升级所有设备上的数据库存储以使用与标准上游数据库版本兼容的 PostgreSQL 9.4。

- 已向 tgsh-dialog 重新添加“应用”(APPLY) 按钮，并具有新的功能：按照与系统更新后相同的方式自动配置并更新任务。可用来修复更新尝试中止后仍具有不一致状态的系统。

- 已添加一种机制，客户支持通过该机制可选择用于其他思科设备触发作业的默认虚拟机。

漏洞修复

- 如果系统写入性能被降级，新虚拟机镜像的更新不再容易出现失败的情况。

- 从控制台调用的更新作业在 Opadmin 中不再易被错误地视为失败。

- 更新过程中不再创建服务通知。

- 已修复生成自某些 Microsoft Office 文档类型的不正确的文件扩展名。

版本 1.3

本版本添加了相当数量的设备特定功能，包括：远程系统日志支持、系统级别问题的邮件提示和性能图表的可用性。本版本贴近稍新版本的 ThreatGRID 服务，实现对集成思科 FireSIGHT 管理中心产品的支持。本版本还包含设备特定的漏洞修复。

请注意，如果配置远程系统日志，则请对出站流量使用 clean 接口。有关详细信息，请参阅已更新的 1.3 版管理文档。

新功能

- 可以配置通过邮件发送的通知在系统监控事件上触发。

- 已向管理界面的 SSL 配置页面添加按钮以生成新的自签 SSL 证书。

-.随时间推移的 CPU、I/O 和内存使用量的图表现在在管理界面中可用。

- 操作系统级别的网络接口名称现在会与其用于文档中的逻辑名称（“clean”、“dirty”、“admin”）匹配。

- 支持热插拔网络接口；无需在启动时插入接口以使其稍后可用，而在发生热插拔事件时需要刷新 DHCP 的接口将会如此。（需要 SFP 的接口仍需在启动时安装这些 SFP）。

- 失败的服务会自动重启。

- 失败的服务会在应用中生成服务通知。

- NTP 同步时的失败尝试会在应用中生成服务通知。

- 过多的数据库检查点积压工作会产生用户可见的警告。

- 已为空闲空间事件添加服务通知。

- 已向有关升级可用性的服务通知添加版本说明内容。

漏洞修复

- 具有超过 /24 高位的网络掩码不再被过早裁剪。

安全更新

- 修复 qemu 已禁止通过 CD-ROM 驱动器执行的漏洞；请参阅 CVE-2015-5154。
- 通过应用调试界面升级本地权限的可能性得到降低。

其他说明

- 已更新 EULA 条款。

1.2.1 版

这会更新 ThreatGRID 设备基于来自更新版本的云服务的软件。关键功能是支持集成其他思科设备 -- 包括 ESA 和 WSA 设备。

本版本中没有修改任何设备特定代码或基础设施。

新功能

- 支持思科沙盒 API

安全更新

- 修复 qemu 以禁用软盘控制器模拟，从而避免 CVE-2015-3456

版本 1.2

本版本改善与其他思科产品的集成，精简软件更新过程，并添加硬件监控支持。

新功能

- 软件更新检查现在会在每天夜间在后台自动发生。

- 当软件更新可用时，Threat Grid 应用内会有通知。

已修复的漏洞

- 软件更新在慢速连接上不再超时。

- 关机或重启时正在处理的样本不再丢失或以副本形式插入。应用 1.2 版更新后，样本处理会在达到适当的停止点之前延迟关机。设备重新启动后会继续样本处理。（以往，样本处理可能会导致系统关闭出现更长的延迟，并且会导致样本丢失。）

- 系统启动时不再发生“502 错误的网关”(502 Bad Gateway) 的错误。

- NTP（网络时间协议）同步现在能正确地发生。

- 生成的 SSL 证书序列号现在在所有设备上为唯一。**注意：**本次修复仅影响首次安装 1.2 或更高版本的系统。

- 在处理数量相对较少的样本后导致设备耗尽磁盘空间的存储错误配置已被修复。

- 审计日志现在能正确地显示客户端 IP 地址。

- SSH 密钥配置页面上的文本能正确地反映这是为 threatgrid 用户而非 root 配置密钥。

- 生成的邮件中的密码重置链接现在是正确的了。

安全更新

- 管理界面的会话 cookie 在 Threat Grid 设备间不再可移植。

- OpenSSL 经过升级以包含上游修复。

其他改进

- 在首次安装 1.2 或更高版本的设备上，PostgreSQL 数据库会使用与上游 PostgreSQL 和相关项目（例如 EnterpriseDB）二进制兼容的存储格式。

已知问题

- 在可以运行 Windows 7 作业之前，需要做出以下用户介入行为：

1. 以管理员身份在 clean 接口上登录主 ThreatGRID 应用控制台。2. 点击右上角**欢迎管理员 (Welcome Admin)** 以访问下拉菜单。3. 点击**管理组织 (Manage Orgs)**。4. 点击**初始组织 (Initial Organization)**。5. 在**额外 VMS (Additional VMS)** 字段中，输入 **win7**。6. 点击**更新 (Update)**。

在完成这个之后，当提交样本时，在**高级选项 (Advanced Options)** 下，

用户可以选择 **win7**。

- 许可解析对文本文件格式敏感。许可证必须保存在 UNIX 文本文件中 - 各行由 CR 而非 CRLF 分隔。

版本 1.1 在线修正 1

在线修正 1 与 1.1 相同，但同时修复了一个影响慢速连接上更新下载可靠性的漏洞。

版本 1.1

本版本向 Threat Grid 设备添加了若干新功能（包括 Window 7 支持），并已修复若干漏洞。

新功能

- 已添加 Windows 7 支持。

- 邮件可通过连接在设备 **Clean** 网络上的邮件服务器发送，而不是仅允许使用通过 **Dirty**（即恶意软件）可访问的邮件服务器。

- 支持直接从设备将快照上传给 Threat Grid 支持。

- 支持在将快照提交给 Threat Grid 支持之前对其进行查看。

- 可从字符 (curses) 界面应用更新，而不仅仅通过基于 Web 的管理界面 (**OpAdmin**) 应用更新。

- 可从恢复模式成功修改系统密码。

- 需要重启生效的管理更改变得更少。

- 已对 GUI 配置工作流添加更多客户端的 Javascript 验证。

已修复的漏洞

- 已解决各类出站邮件配置问题。

- 管理界面内的通知现在可以正确显示。

- 配置 UI 中长期运行的作业的状态现在以最低延迟传输。

- 已修复某种情况下管理界面拒绝启动的问题。

- 配置 GUI 不能总是准确反映是否需要重启以使配置更改生效。此问题已修复。

- 已从 tgsh-dialog（基于 curses）管理界面删除不支持的菜单项目。

安全更新

- 已更新具有已知漏洞的上游程序包（ntpd、bash、openssl）。

- 配置备份不再全局可读。

1.0+hotfix2 更新 - 强制更新

1.0+hotfix2 是**强制更新**，用于修复更新系统本身，使其无需拆分大文件即可进行处理。