AMP Threat Grid 设备
版本说明

版本 2.1

最后更新时间： 2016 年 2 月 15 日

目录

重要说明

2.0 升级可能需要数小时

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。

从 1.4 之前的版本升级

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 的版本说明的相关部分。

版本 1.0+hotfix2 更新是强制更新

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。

内部版本号/版本查询表

内部版本号	版本	发布日期
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
2014.10.20160115122111.1f09cb5f	v1.4.6	2016 年 1 月 27 日
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 必需	
2014.10.20141125162158.8afc5e2f	v1.0	

版本 2.0.1

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

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）。

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。

版本 1.4.6

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。

版本 1.4.5

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。

版本 1.4.4

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。

版本 1.4.3

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）。

版本 1.4.2

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）。

版本 1.4.1

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。

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

- 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。

版本 1.2.1

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。