Firepower 系统版本说明

版本 6.0
首次发布日期：2015 年 11 月 11 日
上次更新日期：2016 年 8 月 22 日

这些版本说明适用于版本 6.0 Firepower 系统。即使您熟悉更新过程，也请务必通读并理解这些版本说明。这些版本说明描述了受支持的平台、新增功能和更改的功能、管理平台受管设备的兼容性、已知问题和已解决的问题。它们还包含有关先决条件、警告以及具体安装说明的详细信息。

提示 要访问 Firepower 系统的完整文档，请访问 http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html，参阅文档规划图。

警告：您必须先安装 FireSIGHT 系统 6.0.0 版预安装软件包，然后才能更新至版本 6.0。有关详细信息，请参阅 *"FireSIGHT System Release Notes Version 6.0 Pre-Installation Package"*（FireSIGHT 系统 6.0 版预安装软件包的版本说明）。

有关详细信息，请参阅以下各节：

支持的平台和兼容性

支持的平台、最低原始版本和操作系统因版本不同而异。有关详情，请参阅：

支持的平台

您可以在下表中指定的平台上运行版本 6.0。有关最低 Firepower 系统版本要求，请参阅更新至版本 6.0 的 Firepower 版本要求，第 12 页。

注意：对于某些 Firepower 管理中心模型（之前称为 FireSIGHT 管理中心或 Defense Center），Firepower 版本 6.0 比之前的版本需要更多内存。具体来说，MC750 需要两个 4GB 双列直插式内存模块 (DIMM)。具有 6GB 内存的 MC1500 也同样需要更多内存。

表 1 版本 6.0 支持的平台

版本 6.0 支持的平台	版本 6.0 的功能	版本 6.0 的其他运行要求
Firepower 管理中心（MC750、MC1500、MC3500、MC2000 和 MC4000）	management	■ MC750 需要两个 4GB 双列直插式内存模块 (DIMM) ■ MC1500 需要至少 8GB 的内存
64 位 Firepower 管理中心虚拟设备	management	托管于： ■ VMware vSphere 虚拟机监控程序/VMware ESXi 5.1 ■ VMware vSphere 虚拟机监控程序/VMware ESXi 5.5 ■ VMware vCloud Director 5.1
Firepower 7000 系列和 8000 系列（7010、7020、7030、7050、7110、7115、7120、7125、8120、8130、8140、8250、8260、8270、8290、8350、8360、8370、8390、AMP7150、AMP8050、AMP8150、AMP8350、AMP8360、AMP8370、AMP8380 和 AMP8390）	受管设备	n/a
具备 FirePOWER 服务的思科 ASA（ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X、ASA 5512-X、ASA 5515-X、AS A5516-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X-SSP-10、ASA 5585-X-SSP-20、ASA 5585-X-SSP-40、ASA 5585-X-SSP-60）	受管设备	运行 ASA 版本 9.4(2) 或 9.5(2)
NGIPSv（虚拟受管设备）	受管设备	托管于： ■ VMware vSphere 虚拟机监控程序/VMware ESXi 5.1 ■ VMware vSphere 虚拟机监控程序/VMware ESXi 5.5 ■ VMware vCloud Director 5.1

管理平台受管设备的兼容性

管理功能因版本不同而异。下表详细说明了可用的管理平台以及这些平台可以管理的设备：

表 2 按管理平台划分的管理平台兼容性

支持的管理平台	您可以使用此管理平台管理哪些设备？
Firepower 管理中心（MC750、MC1500、MC3500、MC2000 和 MC4000）	以下至少运行版本 5.4.0.6 的所有设备： ■ Firepower 7000 系列和 8000 系列（7010、7020、7030、7050、7110、7115、7120、7125、8120、8130、8140、8250、8260、8270、8290、8350、8360、8370、8390、AMP7150、AMP8050、AMP8150、AMP8350、AMP8360、AMP8370、AMP8380 和 AMP8390） ■ NGIPSv（虚拟受管设备） ■ 具备 Firepower 服务的思科 ASA（ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X-SSP-10、ASA 5585-X-SSP-20、ASA 5585-X-SSP-40、ASA 5585-X-SSP-60） 以下运行版本 5.4.1.5 的设备： ■ 具备 Firepower 服务的思科 ASA（ASA 5506X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X 和 ASA 5516-X） 以下运行版本 6.0 的所有设备： ■ Firepower 7000 系列和 8000 系列（7010、7020、7030、7050、7110、7115、7120、7125、8120、8130、8140、8250、8260、8270、8290、8350、8360、8370、8390、AMP7150、AMP8050、AMP8150、AMP8350、AMP8360、AMP8370、AMP8380 和 AMP8390） ■ NGIPSv（虚拟受管设备） ■ 具备 FirePOWER 服务的思科 ASA（ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X、ASA 5516-X、ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X-SSP-10、ASA 5585-X-SSP-20、ASA 5585-X-SSP-40 和 ASA 5585-X-SSP-60）

表 2 按管理平台划分的管理平台兼容性（续）

支持的管理平台	您可以使用此管理平台管理哪些设备？
ASDM 版本 7.5(1.112)	以下运行版本 6.0 的所有设备： ■ 具备 FirePOWER 服务的 Cisco ASA（ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X、ASA 5516-X、ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X-SSP-10、ASA 5585-X-SSP-20、ASA 5585-X-SSP-40 和 ASA 5585-X-SSP-60）
64 位 Firepower 管理中心虚拟设备	以下至少运行版本 5.4.0.6 的所有设备： ■ Firepower 7000 系列和 8000 系列（7010、7020、7030、7050、7110、7115、7120、7125、8120、8130、8140、8250、8260、8270、8290、8350、8360、8370、8390、AMP7150、AMP8050、AMP8150、AMP8350、AMP8360、AMP8370、AMP8380 和 AMP8390） ■ NGIPSv（虚拟受管设备） ■ 具备 Firepower 服务的思科 ASA（ASA 5516-X、ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X-SSP-10、ASA 5585-X-SSP-20、ASA 5585-X-SSP-40、ASA 5585-X-SSP-60） 以下运行版本 5.4.1.5 的设备： ■ 具备 Firepower 服务的思科 ASA（ASA 5506X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X 和 ASA 5516-X） 以下运行版本 6.0 的所有设备： ■ Firepower 7000 系列和 8000 系列（7010、7020、7030、7050、7110、7115、7120、7125、8120、8130、8140、8250、8260、8270、8290、8350、8360、8370、8390、AMP7150、AMP8050、AMP8150、AMP8350、AMP8360、AMP8370、AMP8380 和 AMP8390） ■ NGIPSv（虚拟受管设备） ■ 具备 FirePOWER 服务的 Cisco ASA（ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X、ASA 5516-X、ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X-SSP-10、ASA 5585-X-SSP-20、ASA 5585-X-SSP-40 和 ASA 5585-X-SSP-60）

表 3 按受管设备划分的管理平台受管设备的兼容性

支持的受管设备	哪些平台可以用于管理此设备？
Firepower 7000 系列和 8000 系列（7010、7020、7030、7050、7110、7115、7120、7125、8120、8130、8140、8250、8260、8270、8290、8350、8360、8370、8390、AMP7150、AMP8050、AMP8150、AMP8350、AMP8360、AMP8370、AMP8380 和 AMP8390）	以下运行版本 6.0 的所有设备： ■ Firepower 管理中心（MC750、MC1500、MC3500、MC2000 和 MC4000） ■ 64 位 Firepower 管理中心虚拟设备
具备 FirePOWER 服务的思科 ASA（ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X、ASA 5512-X、ASA 5515-X、ASA 5516-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X-SSP-10、ASA 5585-X-SSP-20、ASA 5585-X-SSP-40、ASA 5585-X-SSP-60）	以下运行版本 6.0 的所有设备： ■ Firepower 管理中心（MC750、MC1500、MC3500、MC2000 和 MC4000） ■ 64 位 Firepower 管理中心虚拟设备 ■ ASDM（ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X、ASA 5516-X、ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X-SSP-10、ASA 5585-X-SSP-20、ASA 5585-X-SSP-40 及 ASA 5585-X-SSP-60）
NGIPSv（虚拟受管设备）	以下运行版本 6.0 的所有设备： ■ Firepower 管理中心（MC750、MC1500、MC3500、MC2000 和 MC4000） ■ 64 位虚拟 Firepower 管理中心

新功能

版本说明的这一节汇总了版本 6.0 Firepower 系统中的新功能和经过更新的功能：

- 新功能，第 5 页
- 更改的功能，第 7 页
- 更新的术语，第 7 页
- 更新的文档，第 8 页

新功能

版本 6.0 引入了以下功能：

扩展的威胁防护

基于 URL 和 DNS 的安全情报

提供了基于 URL 和域名系统 (DNS) 服务器的全新安全情报源，以提升现有的基于 IP 的安全情报功能。目前，基于 IP 的情报用于控制对已知恶意软件、网络钓鱼、命令与控制及僵尸站点的访问。旨在击败基于 IP 的情报（例如，快速通量 [fast flux]）的新攻击方法会滥用 DNS 负载均衡功能，试图隐藏恶意服务器的实际 IP 地址。虽然与这种攻击关联的 IP 地址频繁调进调出，但域名很少会发生变化。在应对这种攻击时，基于 URL 的情报会与基于 IP 的情报互补，并且基于 DNS 的情报将帮助识别与这些类型的攻击有关联的已知 DNS 服务器。使用这些新的情报源可以创建访问控制策略，并且新控制面板会提供可视性和分析功能。此外，基于 URL 和基于 DNS 的安全情报事件还将馈送到危害表现 (IoC) 关联功能中。这些新源通过来自思科 Talos 安全情报和研究团队的定期更新提供，而且与基于 IP 的安全情报功能类似，是基础产品的一部分，不需要单独许可。

DNS 检测与 Sinkhole

攻击者通过相同的方式使用 SSL 协议隐藏其活动，攻击者使用 DNS 协议也是出于相同的目的。出于这种原因，作为解决快速流量型攻击的另一种方式，Firepower 系统提供了拦截 DNS 流量请求的功能，以及基于策略设置采取适当的操作。DNS 策略允许请求已知的命令和控制、垃圾邮件、网络钓鱼等、要阻止的站点、返回未找到域 (Domain Not Found) 消息，或将流量定向至预配置的 Sinkhole。最后一个选项通过 Firepower 受管设备直接路由流量，并提供有关可能导致产生 IoC 警报的终端的信息。

增强的网络可视性与可控性

通过 ASDM 管理的具备 FirePOWER 服务的 Cisco ASA SSL 解密

现在，Cisco 下一代防火墙 (NGFW) 具备 FirePOWER 服务的 Cisco ASA 能够本地管理 SSL 通信，并且可在对流量进行攻击、应用和恶意软件检测之前解密流量。这与我们在 Cisco FirePOWER 下一代 IPS (NGIPS) 设备版本 5.4 中引入的功能相同。SSL 解密既可在被动模式下部署，也可在内联模式下部署，并支持基于 HTTPS 和 StartTLS 的应用（例如，SMTPS、POP3S、FTPS、IMAPS、TelnetS）。解密策略可以配置为对加密流量日志记录和处理施加精细控制，例如基于 URL 类别限制解密以应对隐私问题。此外，它还提供阻止自签名加密流量的功能，或在 SSL 版本、特定 Cipher Suite 和/或未经批准的移动设备上提供此功能。

支持 OpenAppID 定义的应用

OpenAppID 是 Cisco 专注于应用的开源检测语言，使用户能够在不依赖 NGFW 供应商的发布周期或规划图的情况下，为自定义、本地化和云应用创建、共享和实施新应用检测签名。在版本 6.0 中，用于识别和控制 3000 多个应用访问权限的 Firepower 应用检测引擎已得到增强，能识别 OpenAppID 定义的应用。Snort 是我们为将入侵检测游戏设为开源所做的一项努力，同样，OpenAppID 也是将应用检测游戏设为开源的一种方式。支持 OpenAppId 定义的应用表明 Cisco 致力于实现开源计划并向客户提供灵活性。

强制网络门户和主动身份验证

为了在将用户映射到 IP 地址及其关联的网络事件时提供更好的可视性，强制网络门户和主动身份验证功能可配置为当系统通过浏览器视窗发出提示时，要求用户输入其凭据。映射还允许策略基于用户或用户组。此功能可补充现有的 Sourcefire 用户代理 (SUA) 与 Active Directory 的集成，以应对非 Windows 环境、自带设备 (BYOD) 用户及访客问题。

注意：在运行 ASA 版本 9.5(2) 或更高版本时，具备 FirePOWER 服务的 Cisco ASA 仅支持强制网络门户和主动身份验证功能。

与思科身份服务引擎 (ISE) 集成

与 Cisco ISE 进行集成可使系统获得更多可用的用户身份数据，以用于分析和策略控制。通过订用 Cisco Platform Exchange Grid (pxGrid)，Firepower 管理中心可以下载更多用户数据、设备类型数据、设备位置数据和安全组标签（SGT - ISE 用来提供网络访问控制的方法）。除了提高对您网络中用户的可视性之外，此数据还是很有价值的情报，因为通过基于 SGT、设备类型或 ISE 提供的任意其他信息创建策略，它可以扩展您能提供的控制权限。

注意：在版本 6.0 中，您无法使用 ISE 自动隔离受感染的终端。此功能将加入到以后的版本中。

增强了针对高级持续性威胁的威胁防御能力

本地恶意软件检查

此功能能够直接在 Firepower 设备上识别常见的恶意软件，并减少在云中或在内部部署中发送文件进行动态分析（沙盒）的需求（请参阅“与 AMP Threat Grid 集成”）。使用高保真 ClamAV 签名，其 SHA-256 查找返回未知 (Unknown) 处理结果的文件将在 Firepower 设备上进行本地分析，以识别与恶意软件相关的常见特征，从而减少动态分析需求。

文件属性分析

由于某些文件类型支持可用于隐藏恶意软件的嵌套内容，因此此功能提供文件本地分析功能，以确定隐藏其中的恶意软件的生存能力。例如，PDF 文件可包含嵌套在此文件中的不同文件类型。然后，系统会生成文件构成报告，用以识别此文件中是否包含嵌套数据、这些嵌套文件所代表的文件类型，以及每个嵌套文件包含恶意软件的几率。根据此信息，您可以选择是否发送文件进行动态分析。

与 AMP Threat Grid 集成

Cisco 于 2014 年 6 月收购了 ThreatGrid，并因此提高了我们帮助客户解决高级持续性威胁的能力，而且该技术也已完全集成到 Firepower v6.0 中。在使用我们的 **AMP for Firepower** 选项时，AMP Threat Grid 现在可以在云中提供沙盒功能。将会对照数亿条经过分析的其他恶意软件人为因素，对发送到云进行动态分析的文件进行安全分析并建立关联，以全面了解恶意软件攻击和活动及其分布的相关信息。利用详细报告可识别关键行为指标并确定威胁指数，以便更快地进行优先级排序并从高级攻击中恢复。

此外，我们大大扩展了支持自动动态分析的文件类型的范围，从仅支持可执行文件扩展到包括 PDF 和 Office 文档在内。

扩展管理功能

多域管理

为了处理以下运营商市场的问题，Firepower 管理中心现在可以创建多个管理域：必须管理单独的客户环境及进行过收购的企业（产生重叠的 IP 地址），或具有需要单独管理的地区业务部门的企业。这些域（最多 50 个）使单独管理环境成为可能，并通过基于角色的精细访问控制 (RBAC) 进行管理。每个域提供单独的事件数据、报告和网络映射。

策略层级和继承

为了支持多域管理并使策略管理更加高效，版本 6.0 提供了创建策略层级的功能。可以建立适用于所有管理环境的全局策略（例如，访问控制）。然后，可以在全局策略级别下建立策略层级，以代表不同的环境、不同的公司、不同的业务部门或不同的组织部分。其中每个策略环境都可以继承其上面层级的策略，从而实现更加一致、高效的策略管理。

扩展 ASDM 管理可用性

Cisco 自适应安全设备管理器 (ASDM) 是适用于 具备 FirePOWER 服务的 Cisco ASA 的本地管理功能。该功能已作为 Cisco ASA 5506-X、ASA 5508-X 和 ASA 5516-X 的组成部分引入这些设备中。通过 Firepower v6.0，ASDM 现在能够在其余 具备 FirePOWER 服务的 Cisco ASA 设备（ASA 5512-X/ASA 5515-X/ASA 5525-X/ASA 5545-X/ASA 5555-X/ASA 5585-X）上使用。

更改的功能

- 您无法在以下页面上比较策略：“NAT 策略”(NAT Policy) 页面、“平台设置”(Platform Settings) 页面和“SSL 策略”(SSL Policy) 页面。
- 版本 6.0 不支持使用 AMP 私有云进行 AMP for Firepower 签名查找。在版本 6.0 中，系统会自动向 AMP 公共云提交 SHA-256 签名。如果您有 AMP 私有云且正在从端点接收事件，则无需对配置进行任何其他更改，Firepower 管理中心版本 6.0 即可继续接收这些事件。
- 连接事件的系统日志消息现在可为以下字段填写信息：“HTTP 引荐来源”(HTTP Referrer)、“用户代理”(User Agent) 和“引用主机”(Referenced Host)。
- 版本 6.0 不支持发现事件运行状况监控。
- 您现在可以在运行 FirePOWER 服务的 ASA 模块上编辑“自动应用旁路 (AAB)”(Automatic Application Bypass [AAB]) 设置。

更新的术语

版本 6.0 中使用的术语可能与之前版本中使用的术语有所不同。有关详细信息，请参阅 *“Firepower Compatibility Guide”*（Firepower 兼容性指南）。

更新的文档

要访问 Firepower 系统的完整文档，请访问 http://www.cisco.com/c/en/us/td/docs/security/firesight/roadmap/firesight-roadmap.html，参阅文档规划图。在版本 6.0 中，以下文档进行了更新，以反映功能的新增和更改，并且解决报告的文档问题：

- *《Firepower 管理中心联机帮助》*
- *《ASA FirePOWER 模块联机帮助》*
- *《Firepower 管理中心配置指南》*
- *《Firepower 管理中心安装指南》*
- *《Firepower 系统虚拟安装指南》*
- *《Firepower 系统 eStreamer 集成指南》*
- *《Firepower 系统补救措施 API 指南》*
- *《Firepower 系统数据库访问指南》*
- *《Firepower 系统主机输入 API 指南》*
- *《适用于 VMware 的 Firepower NGIPSv 快速入门指南》*
- *《适用于 Vmware 的 Firepower NGIPSv 和 Firepower 管理中心快速入门指南》*
- *《思科 ASA FirePOWER 服务本地管理配置指南》*
- *《Firepower 7000 和 8000 系列安装指南》*

更新后的版本 6.0 文档包含以下错误：

- *《Firepower 管理中心配置指南》*没有反映以下方面：在多域部署中，当您创建 DNS 策略时，系统默认禁用 DNS 规则的子级白名单和 DNS 规则的子级黑名单。您可以通过编辑它们启用每条规则。(CSCuw62140)
- 在线帮助错误地表述了以下内容：如果您部署配置更改时启用了“在策略应用期间检查流量”(Inspect traffic during policy apply)，并且没有特定配置要求 Snort 重启，则默认入侵策略（而非当前部署的访问控制策略）会在策略部署期间检查流量。

注意：在线帮助内容可能与*《Firepower 管理中心配置指南》*内容不同。*《Firepower 管理中心配置指南》*内容的更新频率要高于在线帮助。

准备工作：重要更新和兼容性说明

在开始版本 6.0 的更新过程之前，您应熟悉更新过程中的系统行为，以及任何兼容性问题或者更新前后需要进行的配置更改。

警告：在更新至版本 6.0 之前，您必须先安装 FireSIGHT 系统 6.0.0 版预安装软件包。有关详细信息，请参阅 *“FireSIGHT System Release Notes Version 6.0 Pre-Installation Package”*（FireSIGHT 系统 6.0 版预安装软件包的版本说明）。

警告：Cisco 强烈建议您在维护时段或者中断对部署影响最小时执行更新。

有关详细信息，请参阅以下各节：

- 配置和事件备份准则，第 9 页
- 升级之前拆分 Firepower 管理中心高可用性，第 9 页
- 更新 MC750、MC1500 和管理中心虚拟设备的 Firepower 管理中心内存，第 9 页
- 将管理中心 HTTPS 证书升级到版本 6.0，第 10 页

配置和事件备份准则

在您开始更新之前，Cisco 强烈建议删除或移动设备上的所有备份文件，然后将当前的事件和配置数据备份到外部位置。

使用 Firepower 管理中心备份自己及其管理的设备的事件和配置数据。有关备份和恢复功能的详细信息，请参阅 *"Firepower Management Center Configuration Guide"*（Firepower 管理中心配置指南）。

版本 6.0 不支持使用 AMP 私有云进行 AMP for Firepower 签名查找。在版本 6.0 中，系统会自动向 AMP 公共云提交 SHA-256 签名。如果您有 AMP 私有云且正在从端点接收事件，则无需对配置进行任何其他更改，Firepower 管理中心版本 6.0 即可继续接收这些事件。

注意：Firepower 管理中心会清除来自以前的更新的本地存储备份。要保留存档的备份，请将备份存储到外部。

升级之前拆分 Firepower 管理中心高可用性

版本 6.0 不支持高可用性对中的 Firepower 管理中心。要在高可用性环境中更新 Firepower 管理中心，您必须拆分高可用性对并单独更新每个 Firepower 管理中心。要更新至版本 6.0，您必须拆分高可用性对。

更新 MC750、MC1500 和管理中心虚拟设备的 Firepower 管理中心内存

对于某些 Firepower 管理中心模型（之前称为 FireSIGHT 管理中心或 Defense Center），Firepower 版本 6.0 比之前的版本需要更多内存。具体来说，MC750 需要两个 4GB 双列直插式内存模块 (DIMM)。具有 6GB 内存的 MC1500 也同样需要更多内存。

由于内存增加是由 Cisco 产品需求引起的，因此 Cisco 正在向拥有这些模型的客户提供内存升级套件。有权在符合条件的 MC750 或 MC1500 Firepower 管理中心模块上运行版本 6.0 的客户可以免费订购上述套件。

有关订购内存套件的详细信息，请参阅 http://www.cisco.com/c/en/us/support/docs/field-notices/640/fn64077.html。有关收到套件后如何更换内存的说明，请参阅 *"Firepower Management Center Installation Guide"*（Firepower 管理中心安装指南）中的"Memory Upgrade Instructions for Firepower Management Centers"（Firepower 管理中心内存升级说明）。

此外，管理中心虚拟设备更新至版本 6.0 最少需要 8GB 内存。

将管理中心 HTTPS 证书升级到版本 6.0

目前版本 6.0 不支持在 Firepower 管理中心上使用采用 `RSASSA-PSS` 签名算法的证书。如果您使用此类证书将 Firepower 管理中心更新到版本 6.0，或者在版本 6.0 中添加此类证书，则系统将不允许您登录管理中心 Web 界面，并且会生成无法授权访问。如果依然无法访问此设备，请与系统管理员联系 (`Unable to authorize access. If you continue to have difficulty accessing this device, please contact the system administrator`) 这一错误。

在更新之前，使用 `sha1WithRSAEncryption` 或 `sha256WithRSAEncryption` 算法生成并安装 HTTPS 证书，然后重启 Firepower 管理中心，或者使用默认的 Firepower 管理中心证书，然后重启设备。

同样地，如果 Firepower 管理中心使用的证书是借助大于 2048 位的公共服务器密钥生成的，则更新至版本 6.0 后，您将无法登录管理中心 Web 界面。

如果您使用大于 2048 位的公共服务器密钥无法登录管理中心 Web 界面，则可通过以下方法来替换使用更大的公共密钥创建的证书：生成服务器证书请求 (CSR)，然后使用此请求将生成的证书应用到 Firepower 管理中心。安装新证书后，重启设备。

注意：有关在 5.4.x 版本的设备中正确生成证书的信息，请参阅 5.4.1 版本的 *"FireSIGHT System User Guide"*（FireSIGHT 系统用户指南）中的"Using Custom HTTPS Certificates"（使用自定义 HTTPS 证书）。

如果您在更新至版本 6.0 或在上传证书后无法访问 Web 界面，请与支持部门联系。

更新期间的流量和检查

更新过程会重新启动受管设备，并且还可能重启 Snort 过程。根据设备的配置和部署方式，以下功能可能会受到影响：

- 流量检查，包括应用感知和控制、用户控制、URL 过滤、安全情报、入侵检测和防御以及连接日志记录
- 流量，包括交换、路由、NAT、VPN 及相关功能
- 链路状态

请注意，当您更新 8000 系列集群或堆栈对时，系统会每次更新一台设备，以避免流量中断。当您更新集群具备 FirePOWER 服务的 Cisco ASA 设备时，系统会每次更新一台设备，这样可让更新在更新第二台设备之前完成。

下表说明了 Snort 重启会如何影响流量检查。同理，也可预测产品更新可能会影响流量。

Link State

在已启用**旁路 (Bypass)** 的 7000 系列和 8000 系列 内联部署中，网络流量会在更新过程中的两个点中断：

- 更新过程开始时，在链路关闭和打开（摆动），以及网卡切换到硬件旁路时，流量会短暂中断。硬件旁路期间不会检查流量。
- 更新完成后，在链路摆动以及网卡退出旁路时，流量会再次短暂中断。端点重新连接，并与传感器接口重新建立链路后，将会再次检查流量。

NGIPSv 设备、具备 FirePOWER 服务的 Cisco ASA、Firepower 8000 系列设备上的非旁路网络模块、71xx 子系列设备上的 SFP 收发器或运行 Firepower 威胁防御的 ASA Firepower 模块**不**支持可配置**旁路 (Bypass)** 选项。

表 4 网络流量中断

在此受管设备模型上...	配置为...	在重启过程中，流量会...
7000 系列、8000 系列和 NGIPSv	启用或禁用了 **Failsafe** 的内联模式或内联点击模式	不检查就通过（如果禁用 **Failsafe**，并且 Snort 处于繁忙而非关闭状态，则一些数据包可能会丢弃）
	被动	不中断且不检查
7000 系列和8000 系列	已路由、已交换或透明	已删除
具备 FirePOWER 服务的 Cisco ASA	已路由或透明，且出故障时自动打开（**允许流量**）	不检查就通过
	已路由或透明，且出故障时自动关闭（**关闭流量**）	已删除

交换和路由

Firepower 7000 系列和 8000 系列受管设备在更新过程中，**不会**执行交换、路由、NAT、VPN 或相关功能。如果您将设备配置为仅执行交换和路由，则网络流量在更新过程中会被阻止。

更新过程中的审计日志记录

在更新具有 Web 界面的设备时，系统完成其更新前任务之后，简化的更新界面页面会显示。直到更新过程完成和设备重新启动之后，对设备的登录尝试才会反映在审核日志中。

更新版本 6.0 的时间和磁盘空间要求

下表提供了版本 6.0 更新的磁盘空间和时间准则。请注意，使用 Firepower 管理中心更新受管设备时，Firepower 管理中心需要其 `/Volume` 分区有额外的磁盘空间。

警告：在更新过程中的任何时候都不得重新开始更新或重新启动设备。Cisco 提供的时间预估仅供参考，实际更新时间因设备型号、部署和配置而异。请注意，在更新的预先检查部分和重新启动后，系统可能会呈非活动状态；这是预期的行为。

更新的重新启动部分 包括数据库检查。如果在数据库检查过程中发现错误，更新需要更长时间才能完成。与数据库交互的系统后台守护程序，在数据库检查和修复期间不会运行。

注意：设备的当前版本与发行版本（版本 6.0）越接近，更新所需的时间就越少。

如果遇到更新进度方面的问题，请联系支持部门。

表 5 时间和磁盘空间要求

设备	/上的空间	/Volume 上的空间	管理器中的 /Volume 上的空间	Time
Firepower 管理中心（MC750、MC1500、MC3500、MC2000 和 MC4000）	16 MB	8022 MB	1.5 GB	58 分钟
64 位 Firepower 管理中心虚拟设备	16 MB	8022 MB	1.5 GB	因硬件而异
7000 系列和 8000 系列设备（7010、7020、7030、7050、7110、7115、7120、7125、8120、8130、8140、8250、8260、8270、8290、8350、8360、8370、8390、AMP7150、AMP8050、AMP8150、AMP8350、AMP8360、AMP8370、AMP8380 和 AMP8390）	16 MB	6496 MB	1.2 GB	94 分钟
具备 FirePOWER 服务的思科 ASA（ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X、ASA 5516-XASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X-SSP-10、ASA 5585-X-SSP-20、ASA 5585-X-SSP-40 和 ASA 5585-X-SSP-60）	32 MB	7644 MB	1.2 GB	41 分钟
NGIPSv（虚拟受管设备）	17 MB	6046 MB	1.2 GB	因硬件而异

更新至版本 6.0 的 Firepower 版本要求

要更新至 Firepower 系统版本 6.0，设备必须至少运行下表中指定的版本。有关最低操作系统要求和管理平台受管设备兼容性的信息，请参阅支持的平台和兼容性，第 1 页。

注意：如果您想使用 Firepower 管理中心将其受管设备更新至版本 6.0，则该管理中心必须至少运行版本 6.0。

表 6 版本 6.0 支持的平台

平台	更新至版本 6.0 所需的最低版本
Firepower 管理中心（MC750、MC1500、MC3500、MC2000 和 MC4000）	5.4.1 版
64 位 Firepower 管理中心虚拟设备	5.4.1 版
Firepower 7000 系列和 8000 系列（7010、7020、7030、7050、7110、7115、7120、7125、8120、8130、8140、8250、8260、8270、8290、8350、8360、8370、8390、AMP7150、AMP8050、AMP8150、AMP8350、AMP8360、AMP8370、AMP8380 和 AMP8390）	版本 5.4.0.6
具备 FirePOWER 服务的思科 ASA（ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X、ASA 5516-X）	5.4.1 版
具备 FirePOWER 服务的思科 ASA（ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X-SSP-10、ASA 5585-X-SSP-20、ASA 5585-X-SSP-40 和 ASA 5585-X-SSP-60）	版本 5.4.0.6
NGIPSv（虚拟受管设备）	版本 5.4.0.6

版本 6.0 中的 Web 浏览器和屏幕分辨率兼容性

请注意以下内容，以优化使用 Web 界面的体验。

网络浏览器兼容性

用于 Firepower 系统的版本 6.0 网络界面在下表所列的浏览器上进行过测试。

注意：如果您使用 Microsoft Internet Explorer 11 浏览器，则必须通过**工具 (Tools) > Internet 选项 (Internet Options) > 安全 (Security) > 自定义级别 (Custom level)** 禁用 Internet Explorer 设置中的**当将文件上载到服务器时包括本地目录路径 (Include local directory path when uploading files to server)** 选项。

表 7 受支持的网络浏览器

浏览器	需要启用的选项和设置
Chrome 46	JavaScript、Cookie
Firefox 41	JavaScript、Cookie、安全套接字层 (SSL) v3
Microsoft Internet Explorer 10 和 11	JavaScript、Cookie、安全套接字层 (SSL) v3、128 位加密、**活动脚本**安全设置、兼容性视图、将**检查存储网页的较新版本**设置为**自动**

屏幕分辨率兼容性

Cisco 建议，至少选择 1280 像素宽的屏幕分辨率。用户界面兼容低分辨率，但高分辨率可优化显示效果。

版本 6.0 中的集成产品兼容性

以下集成产品所需版本因 Firepower 系统版本而异：

- 思科身份服务引擎 (ISE)
- 思科 AMP Threat Grid
- 思科 Firepower 系统用户代理

有关详细信息，请参阅 *“Firepower System Compatibility Guide”*（Firepower 系统兼容性指南）。

安装更新

在开始更新之前，您必须通读和理解这些版本说明，特别是支持的平台和兼容性，第 1 页和准备工作：重要更新和兼容性说明，第 8 页。

有关最低 Firepower 系统版本要求，请参阅更新至版本 6.0 的 Firepower 版本要求，第 12 页。要更新您的设备，请参阅以下概述的准则和操作步骤：

- 更新 Firepower 管理中心，第 15 页
- 更新受管设备和 ASA FirePOWER 模块，第 16 页

警告：请不要在更新期间重新启动或关闭设备，直至看到登录提示。系统在更新的预先检查部分可能呈非活动状态。这是预期的行为，不需要您重新启动或关闭设备。

注意：对于某些 Firepower 管理中心模型（之前称为 FireSIGHT 管理中心或 Defense Center），Firepower 版本 6.0 比之前的版本需要更多内存。具体来说，MC750 需要两个 4GB 双列直插式内存模块 (DIMM)。具有 6GB 内存的 MC1500 也同样需要更多内存。有关详细信息，请参阅更新 MC750、MC1500 和管理中心虚拟设备的 Firepower 管理中心内存，第 9 页和 *“Firepower Management Center Installation Guide”*（Firepower 管理中心安装指南）。

警告：如果系统的受管设备运行的是版本 5.4.0.5 或更早版本，则将系统更新至版本 6.0 可能会导致流量中断和系统问题。在更新至版本 6.0 之前，您必须先将受管设备更新至版本 5.4.0.6 或更高版本。

何时执行更新

由于更新过程可能会影响流量检查、流量和链路状态，Cisco **强烈**建议您在维护时段或者在中断对部署影响最小的时间执行更新。

安装方法

在更新至版本 6.0 之前，您必须先安装 FireSIGHT 系统 6.0.0 版预安装软件包。有关详细信息，请参阅 *"FireSIGHT System Release Notes Version 6.0.0 Pre-Installation Package"*（FireSIGHT 系统 6.0.0 版预安装软件包的版本说明）。

使用 Firepower 管理中心的网络界面执行更新。先更新 Firepower 管理中心，然后用它更新其管理的设备。

安装顺序

先更新 Firepower 管理中心，再更新其管理的设备。

在成对的 Firepower 管理中心上安装更新

版本 6.0 不支持在高可用性对中更新 Firepower 管理中心。要在高可用性环境中更新 Firepower 管理中心，您必须拆分高可用性对并单独更新每个 Firepower 管理中心。要更新至版本 6.0，您必须拆分高可用性对。

在集群设备上安装更新

在集群设备（在 版本 6.0、7000 系列或 8000 系列设备中或高可用性对中的设备堆栈中）上安装更新时，系统会逐一在每台设备上进行更新。更新开始时，系统会逐一将更新应用至每台设备。

在堆叠设备上安装更新

在堆叠设备上安装更新时，系统同时进行更新。更新完成后，每台设备都会恢复正常运行。请注意：

- 如果主设备先于所有辅助设备完成更新，则在所有设备完成更新之前，堆栈会以受限的混合版本状态运行。
- 如果主设备晚于所有辅助设备完成更新，堆栈会在主设备完成更新后恢复正常运行。

安装后

在 Firepower 管理中心或受管设备上执行更新后，**必须**重新部署配置。部署可能会导致流量和处理的短时间暂停，还可能会导致一些数据包未经检查就通过。有关详细信息，请参阅 *"Firepower Management Center Configuration Guide"*（Firepower 管理中心配置指南）。

您还应执行多个额外的更新后步骤，以确保设备能正常运行。其中包括：

- 验证更新是否已成功
- 确保部署中的所有设备都能够成功通信
- 更新至版本 6.0 的最新补丁（如有），以利用最新的增强功能和安全修复程序
- 或者，更新入侵规则和漏洞数据库 (VDB)，并重新部署配置
- 根据新功能，第 5 页中的信息进行任何必要的配置更改

以下各节不仅包括有关执行更新的详细说明，还包括有关完成任何更新后步骤的详细说明。确保完成所有列出的任务。

更新 Firepower 管理中心

警告：在更新至版本 6.0 之前，您必须先安装 FireSIGHT 系统 6.0.0 版预安装软件包。有关详细信息，请参阅 *"FireSIGHT System Release Notes Version 6.0.0 Pre-Installation Package"*（FireSIGHT 系统 6.0.0 版预安装软件包的版本说明）。

使用本节中的操作步骤更新 Firepower 管理中心，包括虚拟 Firepower 管理中心。要更新版本 6.0，需要重启 Firepower 管理中心。

警告：在您更新 Firepower 管理中心之前，请将配置重新部署到任何受管设备。否则，受管设备的更新可能会失败。

警告：请不要在更新期间重新启动或关闭设备，直至看到登录提示。系统在更新的预先检查部分可能呈非活动状态。这是预期的行为，不需要您重新启动或关闭设备。

注意：将 Firepower 管理中心更新至版本 6.0，会从设备中移除现有的卸载程序。

要更新 Firepower 管理中心，请执行以下操作：

步骤 1 阅读这些版本说明，并完成任何必要的更新前任务。

注意： 更新之前，您需要拆分 Firepower 管理中心高可用性对，还可能需要在 MC750、MC1500 或 Firepower 管理中心虚拟设备上安装更多内存。如果您的 Firepower 管理中心所使用的自定义 HTTPS 证书采用 `RSASSA-PSS` 签名算法或使用超过 2048 位的公共密钥生成，则您可能还需要生成并上传新证书，否则更新后您将无法访问 Firepower 管理中心上的用户界面。有关详细信息，请参阅准备工作：重要更新和兼容性说明，第 8 页。

步骤 2 从支持站点下载更新：

- 对于 Firepower 管理中心和 Firepower 管理中心虚拟设备：

  `Sourcefire_3D_Defense_Center_S3_Upgrade-6.0.0-1005.sh`

注意：直接从支持站点下载更新。如果通过邮件传输更新文件，可能会损坏该文件。

步骤 3 选择 **System > Updates**，然后在 **Product Updates** 选项卡中点击 **Upload Update**，将更新上传到 Firepower 管理中心。浏览到更新并点击 **Upload**。

更新将会上传到 Firepower 管理中心。网络界面会显示您上传的更新的类型、其版本号以及生成更新的日期和时间。

步骤 4 确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

步骤 5 查看任务队列 (**System > Monitoring > Task Status**)，确保没有正在进行的任务。

必须等到所有长时间运行的任务都完成后，才能开始更新。系统更新完成后，为减少混乱，请删除来自"消息中心"(Message Center) 的关于上述任务的消息。

步骤 6 选择 **System > Updates**。

系统将显示 Product Updates 选项卡。

步骤 7 点击上传的更新旁边的安装图标。

系统将显示 Install Update 页面。

步骤 8 选择 Firepower 管理中心并点击 **Install**。确认要安装更新并重新启动 Firepower 管理中心。

更新过程将会开始。可以开始在任务队列 (**System > Monitoring > Task Status**) 中监控更新进度。但是，在 Firepower 管理中心完成其必要的更新前检查后，系统会注销您的登录。当您重新登录时，系统会显示 Upgrade Status 页面。Upgrade Status 页面会显示进度条，提供当前正在运行的脚本的相关详细信息。

如果更新由于任何原因而失败，该页面会显示错误消息，其中指明失败的时间和日期、更新失败时正在运行的脚本，并提供有关如何联系支持部门的说明。请**不要**重新开始更新。

警告：如果更新出现任何其他问题（例如，手动刷新 Update Status 页面后，几分钟都没有显示进度），请不要重新开始更新，而应联系支持部门。

更新完成后，Firepower 管理中心会显示成功消息，并重新启动。

步骤 9 在更新完成后，应清除浏览器缓存，并强制要求浏览器重新加载。否则，用户界面可能会出现意外行为。

步骤 10 登录至 Firepower 管理中心。

步骤 11 审阅并接受《最终用户许可协议 (EULA)》。请注意，如果不接受 EULA，您将从设备注销。

步骤 12 选择 **Help > About**，确认软件版本是否已正确列出：版本 6.0。另请注意 Firepower 管理中心上的入侵规则更新和 VDB 的版本。您随后会需要这些信息。

步骤 13 确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

步骤 14 如果支持站点上的可用规则更新比 Firepower 管理中心上的规则要新，请导入较新的规则。此时请勿自动应用已导入的规则。

有关规则更新的详细信息，请参阅*《Firepower 管理中心配置指南》*。

步骤 15 如果支持站点上的可用 VDB 比 Firepower 管理中心上的 VDB 要新，请安装最新的 VDB。

安装 VDB 更新会导致流量和处理的短时间暂停，还可能会导致一些数据包未经检查地通过。有关详细信息，请参阅*《Firepower 管理中心配置指南》*。

步骤 16 将配置重新部署到所有受管设备。

部署可能会导致流量和处理的短时间暂停，还可能会导致一些数据包未经检查就通过。有关详细信息，请参阅*《Firepower 管理中心配置指南》*。

步骤 17 如果支持站点提供了版本 6.0 的补丁，请按照该版本所述，应用最新的补丁。

必须更新至最新补丁才可利用最新增强功能和安全修复程序。

更新受管设备和 ASA FirePOWER 模块

在将Firepower 管理中心更新至版本 6.0 后，可以使用它们来更新其管理的设备。

警告：如果系统的受管设备运行的是版本 5.4.0.5 或更早版本，则将系统更新至版本 6.0 可能会导致流量中断和系统问题。在更新至版本 6.0 之前，您必须先将受管设备更新至版本 5.4.0.6 或更高版本。

您必须使用运行版本 6.0 的 Firepower 管理中心来更新任何没有自己的 Web 界面的受管设备。对于在 ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X 或 ASA 5516-X 上运行的 ASA FirePOWER 模块，您可以使用 Firepower 管理中心模块更新模块，或者连接到 ASA 设备并通过 ASDM 使用本地管理更新 ASA FirePOWER 模块。有关详细信息，请参阅*《具备 FirePOWER 服务的 Cisco ASA 本地管理版本说明》*。

更新受管设备分两步进行。首先，从支持站点下载更新，并将其上传到管理 Firepower 管理中心。接着，安装软件。可一次对多台设备进行更新，但这些设备必须都使用同一个更新文件。

对于版本 6.0 更新，所有设备都会重新启动。在更新过程中，7000 系列和 8000 系列设备**不会**执行流量检查、交换、路由、NAT、VPN 或相关功能。更新过程还可能会影响流量和链路状态，具体取决于设备的配置和部署。有关详细信息，请参阅更新期间的流量和检查，第 10 页。

警告：在更新受管设备之前，请使用其管理 Firepower 管理中心，以将您的配置重新部署至受管设备。否则，受管设备的更新可能会失败。

警告：请不要在更新期间重新启动或关闭设备，直至看到登录提示。系统在更新的预先检查部分可能呈非活动状态；这是预期的行为，不需要您重新启动或关闭设备。

要更新受管设备和 ASA FirePOWER 模块，请执行以下操作：

步骤 1 阅读这些版本说明，并完成任何必要的更新前任务。

有关详细信息，请参阅准备工作：重要更新和兼容性说明，第 8 页。

在集群设备上安装更新

在集群设备（在版本 6.0、7000 系列或 8000 系列设备中或高可用性对中的设备堆栈中）上安装更新时，系统会逐一在每台设备上进行更新。更新开始时，系统会逐一将更新应用至每台设备。

在堆叠设备上安装更新

在堆叠设备上安装更新时，系统同时进行更新。更新完成后，每台设备都会恢复正常运行。请注意：

- 如果主设备先于所有辅助设备完成更新，则在所有设备完成更新之前，堆栈会以受限的混合版本状态运行。
- 如果主设备晚于所有辅助设备完成更新，堆栈会在主设备完成更新后恢复正常运行。

安装后

在 Firepower 管理中心或受管设备上执行更新后，**必须**重新部署配置。部署可能会导致流量和处理的短时间暂停，还可能会导致一些数据包未经检查就通过。有关详细信息，请参阅 *"Firepower Management Center Configuration Guide"*（Firepower 管理中心配置指南）。

您还应执行多个额外的更新后步骤，以确保设备能正常运行。其中包括：

- 验证更新是否已成功
- 确保部署中的所有设备都能够成功通信
- 更新至版本 6.0 的最新补丁（如有），以利用最新的增强功能和安全修复程序
- 或者，更新入侵规则和漏洞数据库 (VDB)，并重新部署配置
- 根据新功能，第 5 页中的信息进行任何必要的配置更改

以下各节不仅包括有关执行更新的详细说明，还包括有关完成任何更新后步骤的详细说明。确保完成所有列出的任务。

更新 Firepower 管理中心

警告：在更新至版本 6.0 之前，您必须先安装 FireSIGHT 系统 6.0.0 版预安装软件包。有关详细信息，请参阅 *"FireSIGHT System Release Notes Version 6.0.0 Pre-Installation Package"*（FireSIGHT 系统 6.0.0 版预安装软件包的版本说明）。

使用本节中的操作步骤更新 Firepower 管理中心，包括虚拟 Firepower 管理中心。要更新版本 6.0，需要重启 Firepower 管理中心。

警告：在您更新 Firepower 管理中心之前，请将配置重新部署到任何受管设备。否则，受管设备的更新可能会失败。

已解决的问题

您可以使用思科漏洞搜索工具 (https://tools.cisco.com/bugsearch/) 查看此版本中已解决的缺陷。需要登录思科帐户。

以下问题在版本 6.0 中已得到解决：

- 安全问题解决了跨站请求伪造 (CSRF) 漏洞。
- 安全问题解决了已经过身份验证的用户可以使用路径遍历访问系统文件的漏洞。
- 安全问题解决了多个跨站脚本 (XSS) 漏洞，包括 CVE-2015-0737、CVE-2015-4270 和 CVE-2015-6353 中描述的漏洞。
- 安全问题解决了多个跨站脚本 (XSS) 和 任意 HTML 注入漏洞问题，包括 CVE-2015-0707 中描述的漏洞。
- 安全问题解决了 MYSQL、DNS、NTP 和 OpenSSL 中的多个漏洞问题（如 CVE-2010-3614、CVE-2014-3569、CVE-2014-3570、CVE-2014-3572、CVE-2014-6568、CVE-2014-9293、CVE-2014-9294、CVE-2014-9295、CVE-2014-9296、CVE-2014-9297、CVE-2014-9298、CVE-2015-0205、CVE-2015-0287、CVE-2015-0292、CVE-2015-0374、CVE-2015-0381、CVE-2015-0382、CVE-2015-0385、CVE-2015-0391、CVE-2015-0409、CVE-2015-0411、CVE-2015-0432、CVE-2015-0498、CVE-2015-0505、CVE-2015-0506、CVE-2015-0507、CVE-2015-0511、CVE-2015-1798、CVE-2015-1799、CVE-2015-1499、CVE-2015-2566、CVE-2015-2567、CVE-2015-3405 和 CVE-2015-3676 所述）。
- 安全问题解决了在 MYSQL、Linux、GNU C Library、NTP、XML、OpenSSL 和其他第三方中生成拒绝服务的多个漏洞问题（如 CVE-2009-0696、CVE-2011-1155、CVE-2012-0876、CVE-2012-2807、CVE-2012-287、CVE-2012-3509、CVE-2012-3400、CVE-2012-3480、CVE-2012-5134、CVE-2013-0242、CVE-2013-1914、CVE-2013-4332、CVE-2013-4458、CVE-2014-3512、CVE-2014-3571、CVE-2014-3660、CVE-2014-6040、CVE-2014-8502、CVE-2015-0206、CVE-2015-0286、CVE-2015-0288、CVE-2015-0293、CVE-2015-1473、CVE-2015-1781 和 CVE-2015-1819 所述）。
- 安全问题解决了允许未经身份验证的远程攻击者利用或覆盖功能的多个任意脚本注入漏洞漏洞（如 CVE-2008-3075、CVE-2008-4101、CVE-2010-2252、CVE-2010-4494、CVE-2010-4651、CVE-2011-2716、CVE-2011-3102、CVE-2014-047、CVE-2014-4877、CVE-2014-5119、CVE-2014-7817、CVE-2015-1472 和 CVE-2015-6307 所述）。
- 安全问题解决了 HTTP 连接处理中允许用户重定向到恶意网站的多个漏洞（如 CVE-2012-1033 和 CVE-2015-0706 所述）。
- 安全问题解决了允许未经身份验证的远程攻击者在受影响的系统上披露敏感信息的多个漏洞，包括 CVE-2011-1098 和 CVE-2015-3153 中描述的漏洞。
- 安全问题解决了 SSLv3 中导致客户端连接受到外部攻击的多个漏洞（如 CVE-2014-3556 所述）。
- 安全问题解决了多个参数操纵和错误配置漏洞，包括 CVE-2009-0025、CVE-2009-4022 和 CVE-2015-0773 中描述的漏洞。
- 安全问题解决了导致受管设备在处理流量时出现微引擎故障的多个漏洞，包括 CVE-2015-6307 中描述的漏洞。
- 解决了当设备处理的流量不足时，系统无法生成完整的性能图表的问题。(108348/CSCze87001)
- 解决了入侵性能图表错误地报告已收到的数据包最小数量而不是实际收到数量的问题。(124331/CSCze87003)
- 解决了部署策略标识号大于 4096 的策略失败的问题。(134385/CSCze89030)
- 解决了可能已人为限制活动的动态 NAT 转换数量的问题。(134561/CSCze87078)
- 解决了在某些情况下，Firepower 7000 系列和 8000 系列设备的前面板 LCD 信息显示屏将某些软件错误显示为硬件错误的问题。(140386/CSCze91939)
- 解决了系统不显示失败的登录尝试次数的问题。(140400/CSCze87152)
- 改进了数据修剪。(141894/CSCze92576)

- 改进了 Firepower 7000 系列和 8000 系列设备的链接状态传播响应能力 (143860/CSCze87386)
- 解决了当您禁用使用入侵策略的访问控制规则或其他任何规则中都未使用的变量集，并尝试部署该策略时，部署失败的问题。(143872/CSCze87308)
- 改进了 URL 过滤。（144198/CSCze94590、144199/CSCze94758、144685/CSCze94805）
- 解决了当更新失败并且您尝试再次更新时，某些驱动器在安装过程中无法正确安装的问题。(144553/CSCze95696)
- 改进了报告。(145102/CSCze95656)
- 解决了“发现统计”(Discovery Statistics) 页面的以下统计摘要行不包括任何活动的问题：**全部活动 (Total Events)**、**前一小时的全部活动 (Total Events Last Hour)** 或**前一天的全部活动 (Total Events Last Day)**。(145153/CSCze95751)
- 改进了 Firepower 7000 系列和 8000 系列设备的故障排除功能。(145187/CSCze95510)
- 解决了从系统中删除 URL 过滤许可证导致云连接中断的问题。(144578/CSCze95183)
- 更正了内存使用状况监控器使用的计算方法，从而防止虚假警报。(144593/CSCze94840)
- 解决了 Firepower 7000 系列设备上的被动接口错误报告出口安全区和接口的问题。(144624/CSCze95206)
- 解决了当在“对象管理”(Object Management) 页面上编辑接口安全区时，堆叠设备配置在实际上并非最新配置的情况下显示为最新的问题。(144626/CSCze94847)
- 解决了当部署到 Firepower 7000 系列或 8000 系列设备的集群或设备堆栈时，如果在应用最新策略之前集群或堆叠设备包含过期的策略，则系统只部署到主要设备的问题。(144646/CSCze95167)
- 解决了在创建 HTML 报告时，Web 浏览器将报告错误地显示为二进制数据的问题。（144737/CSCze95180、144738/CSCze95205）
- 解决了已解密的 SSL 会话将连接日志中的 URL 显示为 http:// 而不是 https:// 的问题。(144785/CSCze95781)
- 解决了当创建与默认变量名称相同但大写情况不同的自定义网络变量时，系统错误地认为自定义变量和默认变量是相同的，并阻止您删除该自定义变量的问题。(44788/CSCze96160)
- 解决了系统将 DNS 流量作为 OpenVPN、QQ 和 Viber 流量来对待的问题。(144789/CSCze96154)
- 解决了当导入引用已共享层的策略时，导入策略失败的问题。(144946/CSCze96151)
- 改进了磁盘空间利用率。(145012/CSCze95309)
- 改进了 Firepower 7000 系列和 8000 系列设备中硬件加速的可靠性。（145035/CSCze95433、145509/CSCze95994、CSCus68624、CSCut53335 和 CSCut80043）
- 解决了如果在查看规则文档的同时在入侵规则编辑器上编辑本地规则，系统显示已生成的事件数据的当前本地规则配置，而不是触发它的规则配置的问题。(145118/CSCze95346)
- 解决了在将**前一小时 (Last Hour)** 设为时间范围，生成入侵事件性能图表时，系统错误地生成空白图表的问题。(145237/CSCze95774)
- 解决了当在 Firepower 管理中心上启用了远程存储并创建了预设的邮件警报响应时，预设的邮件警报禁用远程存储，并且远程存储备份失败的问题。(145288/CSCze95993)
- 解决了当尝试查看危害表现 (IoC) 的第一个或最后一个事件时，系统找不到该事件的问题。(145486/CSCze95786)
- 解决了 40GB 光纤网络模块流量统计错误地将其他 40GB 端口上的流量计入日志的问题。(145515/CSCze95830)
- 解决了当您网络上的用户在地址栏中输入包含大写字母的 URL 时，包含 Web 应用条件的访问控制规则与流量不匹配的问题。(CSCur37364)

- 解决了文件轨迹页面因子类型无效而无法加载的问题。(CSCur38623)
- 解决了在某些情况下，无法检索 URL 类别或 URL 声誉信息的问题。(CSCur38971)
- 解决了如果在删除流量配置文件前未将其禁用，则已删除的配置文件继续使用原本不应使用的资源的问题。(CSCur48345)
- 解决了当您创建了自定义工作流程并尝试打开入侵事件的数据包视图时，系统在数据包视图中打开错误的入侵事件的问题。(CSCur48743)
- 解决了在某些情况下，无法编辑访问控制策略，并且系统生成`未知错误 (9999)：无法锁定 /var/tmp/.ac_lock (Unknown Error (9999): Couldn't get a lock on /var/tmp/.ac_lock)` 错误消息的问题。(CSCur55338)
- 解决了当创建预设任务以便在已运行新版本漏洞数据库 (VDB) 的 Firepower 管理中心上安装同一版本的 VDB 时，系统在每次预设任务时都重新安装 VDB，并从主用模式切换到备用模式的问题。(CSCur59252)
- 解决了当发生入侵事件或连接事件，并且发生条件与入口安全区、出口安全区、入口接口或出口接口的条件匹配时，虽然您创建了要触发的关联规则，但系统不识别此规则，并且无法针对与此规则匹配的流量生成事件的问题。(CSCur59840)
- 解决了在 Firepower 7000 系列和 8000 系列受管设备上，在设备重新启动的过程中，系统在启用旁路的内联设置上断开内联连接长达 25 秒的问题。(CSCur64678)
- 现在您可以禁用会话终止日志记录功能，以降低磁盘空间要求。(CSCur73008)
- 解决了当您从 Network Map 的“漏洞”(Vulnerabilities) 选项卡扩展基于客户端应用的漏洞时，系统不显示关联的主机的问题。(CSCur86191)
- 解决了当您将集群 Firepower 7000 系列或 8000 系列受管设备上的路由接口配置为私用 IP 地址和 Cisco 冗余协议 (SFRP) IP 地址时，系统无法识别哪一个 IP 地址是主要地址，且无法创建开放最短路径优先 (OSPF) 连接的问题。(CSCur86355)
- 解决了当您在“用户首选项”(User Preferences) 页面上的“时区首选项”(Time Zone Preference) 选项卡中更改选定的时区时，系统不包括夏时制的问题。(CSCur92028)
- 解决了系统在包含大型数据库的情况下无法生成完整的故障排除文件的问题。(CSCur97450)
- 解决了在某些情况下，当您的其中一个访问控制规则操作设置为**阻止 (Block)** 或**交互式阻止 (Interactive Block)** 时，主机无法始终显示阻止页面的问题。(CSCus06868)
- 解决了系统无法正确复制“入侵策略”(Intrusion Policy) 页面上的已注册目标数量的问题。(CSCus08840)
- 解决了系统在 Snort 重启期间有时会出现延迟的问题。(CSCus11068)
- 解决了在仅监控模式下配置的 ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X 或 ASA 5555-X 设备在处理大量流量时出现故障切换的问题。(CSCus15229)
- 解决了在使用 Windows 文件共享 (SMB) 时，因报告名称中包含不受支持的字符，致使系统不支持生成多个报告类型的问题。(CSCus21871)
- 解决了在配置的域名中不包含 DNS 条目时，Web 界面页面无法加载的问题。（CSCus28155 和 CSCut89714）
- 解决了在编辑入侵策略时导入入侵规则失败的问题。(CSCus29526)
- 解决了您在默认操作设为**不解密 (Do Not Decrypt)** 的情况下创建 SSL 策略，并且试图建立会话时，系统在未阻止会话的情况下错误地报告会话被阻止的问题。(CSCus41127)
- 解决了当您将 Cisco IOS 补救措施添加到 Cisco IOS 空路由实例，并输入密码登录路由器时，设备不接受密码且补救失败的问题。(CSCus45769)
- 进一步优化了某些事件的工作流程。(CSCus52203)

- 解决了在入侵策略的配置十分复杂的情况下，系统截断配置以及入侵策略部署失败的问题。(CSCus53911)
- 提高了内存利用率。（CSCus59008、CSCuu38535 和 CSCuu81679）
- 解决了当您创建的访问控制规则使用包含 Web 应用条件的访问控制规则后面的**阻止恶意软件 (Block Malware)** 规则引用文件策略时，系统无法识别恶意软件文件的问题。（CSCus64393 和 CSCus6452）
- 解决了在已注册的 ASA FirePOWER 模块的密码包含不受支持的字符的情况下，系统生成内部服务器错误消息的问题。(CSCus68604)
- 解决了当您同时配置恶意软件阻止和 SSL 解密时，即使文件不包含恶意软件，也仍然无法通过 HTTPS 下载文件的问题。(CSCus72505)
- 改进了 Firepower 管理中心和受管设备之间的通信。(CSCus79643)
- 您现在可以借助已注册的 Firepower 7030 设备在 Firepower 管理中心中部署同时包含 SSL 策略和 URL 类别条件的访问控制策略。(CSCut02823)
- 解决了当您删除网络映射中的主机时系统出现延迟的问题。(CSCut02913)
- 改进了关联事件表的修剪。(CSCut02984)
- 解决了当您在启用 Spero 分析和文件捕获的条件下创建文件策略时，系统无法捕获传入流量中检测到的文件的问题。(CSCut06837)
- 解决了在您恢复 Windows 网络文件服务器 (NFS) 上的备份存档时，备份恢复失败的问题。(CSCut08317)
- 解决了在您向启用**检查本地路由器流量 (Inspect Local Router Traffic)** 的受管设备部署引用 SSL 策略的访问控制策略时，系统生成错误和出现问题的问题。(CSCut12631)
- 解决了在向一组设备部署（在版本 6.0 中，称为高可用性）时，导致系统发生不应发生的故障切换的问题。(CSCut12919)
- 解决了当将您创建的访问控制规则配置为向外部系统日志服务器发送连接事件，并且此规则匹配了大量的流量时，受管设备停止向外部系统日志服务器发送事件的问题。(CSCut14629)
- 解决了在您的入侵策略层共用完全相同的名称，并且您执行了系统更新时，系统出现问题的问题。(CSCut16772)
- 改进了处理交易历史邮件和 eStreamer 事件时的网络映射生成。(CSCut23688)
- 解决了在您编辑具有多个 URL 类别条件的访问控制规则，并且尝试删除其中一个条件时，系统仅删除列出的第一个类别条件的问题。(CSCut25082)
- 解决了在某些情况下，Firepower 管理中心出现系统问题，并且无法加载访问控制规则的问题。(CSCut30047)
- 解决了当您在 Firepower 8000 系列设备上创建被动区域并执行 `show fastpath-rules` CLI 命令时，系统将入侵规则报告为非活动状态的问题。(CSCut32479)
- 改进了备份和恢复的可靠性。(CSCut34456)
- 如果您在未启用**在应用策略的过程中检查流量 (Inpsect traffic during policy apply)** 的情况下进行部署，系统会生成禁用在应用策略的过程中检查流量可能会导致网络中断，而且部署完成之前会一直处于中断状态 (Having Inspect traffic during policy apply disabled may cause network disruptions until deployment completes) 这一警告。(CSCut36078)
- 解决了当您创建的文件策略配置为**检查存档 (Inspect Archives)** 时，系统出现问题并停止处理流量的问题。（CSCut39253 和 CSCuu14892）
- 解决了当您在入侵事件表视图中选择“原始客户端 IP”(Original Client IP) 列中的一个或多个单元格时，系统生成错误，并且无法显示您所选的行的问题。(CSCut41458)
- 解决了当您创建访问控制规则，用以定位包含大量访问控制用户的 LDAP 组中的用户时，系统出现延迟并且无法匹配流量的问题。(CSCut56233)
- 解决了在您针对生成的事件创建和编辑某项搜索，然后在搜索开始之前取消此搜索时，即使搜索名称不正确，系统仍然将您重定向到与搜索相关的事件页面的问题。(CSCut63265)

- 改进了磁盘管理器的功能。(CSCut65740)
- 解决了当映射列表中的最后一个条目为复制条目时，系统出现问题的问题。(CSCut65738)
- 解决了导入入侵规则更新时系统出现问题的问题。(CSCut65772)
- 解决了在某些情况下，系统终止数据库通信并且遇到错误的问题。(CSCut71816)
- 解决了在某些情况下，使用已注册的 Firepower 7000 系列和 8000 系列这对高可用性设备在 Firepower 管理中心上进行部署时，导致出现故障切换的问题。(CSCut72278)
- 改进了云查找故障的运行状况警报通知。(CSCut77594)
- 解决了在系统遇到两次连续故障后，即使未启用旁路模式，系统也会转入此模式的问题。(CSCut80892)
- 解决了可追溯性恶意软件事件表视图中的“消息”列不包含可追溯性恶意软件事件的旧处理值或新处理值的问题。(CSCut83512)
- 解决了在您重启配置有大量子接口的 ASA 5585-X 设备，而未重启 SFR5585-X 服务卡时，SFR5585-X 服务卡发生故障的问题。(CSCut89619)
- 解决了当在已经注册到配置了多个接口的系统中的设备上使用 `show managers` CLI 命令时，导致系统显示错误 IP 地址的问题。(CSCut95947)
- 解决了在某些情况下，不能及时获悉更新失败的问题。(CSCuu01055)
- 解决了在遇到系统问题时，云不断检查是否有新更新的问题。(CSCuu04844)
- 解决了当您创建包含 URL 类别条件的访问控制策略，并且网络映射未能加载完整的数据库时，系统遇到问题的问题。(CSCuu06714)
- 解决了漏洞数据库 (VDB) 安装意外花费很长时间的问题。(CSCuu06786)
- 解决了在某些情况下，Firepower 管理中心停止从已注册设备接收运行状况事件的问题。(CSCuu18450)
- 解决了当您在连接到 Cisco Nexus 7000 交换机的 Firepower 7000 系列或 8000 系列设备上创建链路聚合组 (LAG) 时，系统出现延迟的问题。(CSCuu31626)
- 解决了在您将系统时区更改为东时区，并且将至少具有一个不活动时段的关联规则添加到关联策略时，激活关联规则失败的问题。(CSCuu37600)
- 解决了您在集群 Firepower 7000 系列或 8000 系列设备（在版本 6.0 中，称为高可用性）上创建路由接口时遇到连接问题的问题。(CSCuu37668)
- 解决了 Cisco 冗余协议 (SFRP) 路由器广告值在您添加或编辑路由 IP 地址时显示为可配置，而原本不应这样显示的问题。(CSCuu37687)
- 解决了在您启用两个或多个管理接口，并且 Web 客户端断开到其中一个接口的连接时，系统默认使用不正确的网关 IP 地址，您无法访问接口的问题。(CSCuu44020)
- 解决了当您创建包含地理位置条件的访问控制策略时，应与此条件匹配的流量并未匹配的问题。(CSCuu48800)
- 改进了网络映射生成。（CSCuu53215、CSCuu94784、CSCuv72386 和 CSCuw06359）
- 缩短了包含访问控制策略中引用的手动 URL 条件的访问控制规则的加载时间。(CSCuu55853)
- 解决了运行最低 ASA 版本 9.3.2.2 或更高版本的 ASA Firepower 模块（ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X 和 ASA 5516-X）无法执行 mpf-policy-map-class 模式的问题。(CSCuu68273)
- 解决了在使用否定子网 IP 地址为采用原始客户端 IP 的入侵事件创建搜索时，导致系统错误排除未采用原始客户端 IP 的入侵事件的问题。(CSCuu68438)
- 解决了在极少数情况下，系统显得不稳定，并且无法通过重启恢复的问题。(CSCuu93154)
- 解决了某些 DC4000 设备上的驱动器故障导致 RAID 控制器发生故障和数据丢失的问题。(CSCuu93159)
- 改进了 eStreamer 的性能。(CSCuu94902)

- 解决了当您在 Web 浏览器上查看视频流等占用内存较大的媒体时，系统未能在“摘要控制面板”(Summary Dashboard) 上的“上线的顶级 Web 应用”(Top Web Applications Seen) 和“上线的顶级客户端应用”(Top Client Applications Seen) 构件中显示正确的字节数量的问题。(CSCuu97036)
- 解决了当您在受管设备上部署设置为**解密 - 放弃 (Decrypt-Resign)** 的 SSL 策略，从一个接口中出来的解密流量被设置为已交换或已路由，以使流量进入同一台受管设备上的另一个接口中时，系统出现 SSL 流量中断的问题。(CSCuu97712)
- 解决了当您生成报告、离开“报告模板”(Report Templates) 选项卡，然后再生成其他报告时，“报告”(Reporting) 页面中“报告模板”(Report Templates) 选项卡上的**发送邮件 (Send email)** 复选框未保持选中状态，并且您停止通过邮件接收报告的问题。（CSCuu97750、CSCuu41580 和 CSCuv43116）
- 解决了点击交互式阻止网页上的**继续 (Continue)** 按钮后，无法总是将您重定向至已阻止的网页的问题。（CSCuu97934 和 CSCuu97946）
- 解决了在某些情况下，更新失败的问题。(CSCuu99337)
- 解决了系统无法确认用户是其主要 LDAP 组的成员的问题。(CSCuv03821)
- 解决了当您生成连接事件报告并修改**最大结果 (Maximum Results)** 值后，系统未保存新值，并且生成具有默认值的报告的问题。(CSCuv06557)
- 解决了当您将系统配置为使用远程 NTP 服务器将时间与具有运行版本低于 5.4 的受管设备的系统保持同步时，您经历闰秒，系统使用大量 CPU 的问题。(CSCuv11738)
- 解决了当您创建配置有交互式阻止操作的访问控制规则并在 Chrome Web 浏览器中查看已阻止的网页时，用于绕开阻止页面的**继续 (Continue)** 按钮无法正常工作的问题。(CSCuv21748)
- 解决了已生成的内部 CA 证书的有效期只有 30 天而不是 10 年的问题。(CSCuv29004)
- 解决了当主机生成危害表现 (IoC)，而您在“主机配置文件”(Host Profile) 页面上禁用该主机的 IoC 时，“主机控制面板”(Host dashboard) 构件的危害表现未正确显示本应正确显示的 IoC 的问题。(CSCuv41376)
- 解决了当您在 7000 系列或 8000 系列设备上创建默认操作设置为**解密 - 已知密钥 (Decrypt - Known Key)** 或**解密 - 放弃 (Decrypt - Resign)** 的 SSL 策略，并选择使用其他源 IP 地址重新开始 SSL 会话时，SSL 检查失败，并且连接日志显示的 SSL 策略默认操作不正确的问题。(CSCuv48689)
- 改进了文件检测和阻止。(CSCuv59181)
- 改进了访问控制规则中端口范围的内存利用率。(CSCuv64114)
- 解决了当您注册了许多台设备或在一台受管设备上配置了许多个接口或创建了许多 VPN 部署时，系统未在其各自的页面上为所有设备或接口或 VPN 部署生成信息的问题。(CSCuv76287)
- 改进了运行状况监视器警报。(CSCuv96121)
- 解决了合并入侵策略层时产生错误的问题。(CSCuw34380)
- 改进了邮件通知的可靠性。(CSCuw36354)
- 解决了在某些情况下，系统遇到由无效的用户名值引起的错误的问题。(CSCuw39725)
- 解决了当从 LAN 上串行 (SOL) 切换到 MC4000 上的远端控制管理 (LOM)（或对调切换方向）时，系统的控制台端口无法使用的问题。(CSCuw67319)
- 解决了当您通过 `system support ssl-debug` 或 `system support debug-DAQ-NSE` CLI 命令启用 SSL 调试日志记录，并且系统长时间遇到大量流量时，系统遇到磁盘空间问题的问题。(CSCuw68004)
- 解决了当您部署默认操作设置为**恶意软件阻止 (Malware Block)** 的文件策略，并且系统检测到 SMB 流量时，系统遇到问题的问题。(CSCux49653)

已知问题

您可以使用思科漏洞搜索工具 (https://tools.cisco.com/bugsearch/) 查看该版本说明中报告的已知问题。需要登录思科帐户。

版本 6.0 中报告了以下已知问题：

- 在更新至版本 6.0 之前，您必须先安装 FireSIGHT 系统 6.0.0 版预安装软件包。有关详细信息，请参阅 *"FireSIGHT System Release Notes Version 6.0.0 Pre-Installation Package"*（FireSIGHT 系统 6.0.0 版预安装软件包的版本说明）。
- 如果您使用 Firefox 38.0.1 版本查看 Firepower 管理中心的界面，可能会出现延迟。解决方法：使用 Firefox 41 或更高版本，或者使用其他 Web 浏览器。(CSCuv11830)
- 在某些情况下，如果您在子域中注册设备时创建访问控制策略，则系统会在全局域（而不是原本计划的子域）中创建访问控制策略。(CSCut56951)
- 在某些情况下，如果您在"访问控制"(Access Control) 页面（**策略 [Policies] > 访问控制 [Access Control]**）的"高级"(Advanced) 选项卡中编辑默认网络访问策略，则系统会在部署对话窗口中误将默认的网络访问策略显示为入侵策略。(CSCuv48221)
- 点击通过 ASDM 托管的 ASA FirePOWER 模块的"选择比较"页面（**ASA FirePOWER 配置 [ASA FirePOWER Configuration] > 策略 [Policies] > 文件 [Files] > 比较策略 [Compare Policies]**）上的帮助图标时，无法打开在线帮助。(CSCuw21863)
- 在某些情况下，如果您查看 Firepower 7000 系列或 8000 系列设备的入侵事件表视图页面中的**所有事件（未删除）(All Events [Not Dropped])**，并且按最多六个字段（包括**审核依据 (Review By)** 和**计数 (Count)** 对此表进行排序，然后生成报告，则会导致报告生成失败。解决方法：排除**审核依据 (Review By)** 和**计数 (Count)** 字段值，或者如果您同时添加了**审核依据 (Review By)** 和**计数 (Count)** 字段，那么通过"入侵事件"(Intrusion Events) 页面生成报告时最多也只能包括三个其他字段值。(CSCuw29993)
- 您无法使用包含加号 (+) 字符的名称为设备组命名，尽管系统会生成该字段包含无效字符，只允许使用字母数字、连字符 (-)、下划线 (_)、句号 (.) 和加号 (+) (This field contains invalid characters. Only alphanumerics, hyphen (-), underscore (_), period (.), and plus (+) are allowed) 这一消息。(CSCuw44373)
- 在某些情况下，如果您在"Shell 超时"(Shell Timeout) 页面（**系统 [System] > 配置 [Configuration] > Shell 超时 [Shell Timeout]**）上编辑浏览器和 Shell 超时阈值，然后重新部署，则系统会在超出已配置的阈值后一分钟内注销不活动的 Firepower 管理中心。(CSCuw48568)
- 在某些情况下，编辑域中的文件列表会导致该域中的任意文件策略被标记为过时。(CSCuw52764)
- "设备管理"(Device Management) 页面（**设备 [Devices] > 设备管理 [Device Management]**）里的设备对象的工具提示中不显示设备替代值。(CSCuw53371)
- 版本 5.4.x 中的外部证书在版本 6.0 中不受支持：版本 6.0 中仅支持 `prime192v1`、`prime256v1`、`secp384r1` 和 `secp521r1` 曲线。您必须将系统更新至版本 6.0 才能获得受支持的外部证书。(CSCuw54749)
- 在某些情况下，如果您在使用 Outlook 2013 发送和接收邮件的系统上创建的访问控制策略同时引用了文件策略（包含配置为**检测文件 [Detect Files]** 的文件规则）和 SSL 策略（配置为**解密 - 放弃 [Decrypt--Resign]** 或**解密 - 已知密钥 [Decrypt--known key]**），则"连接事件"(Connection Events) 页面（**分析 [Analysis] > 连接 [Connections] > 事件 [Events]**）在生成的事件中不包含邮件文件附件。(CSCuw65152)
- 在某些情况下，当您刷新"设备管理"(Device Management) 页面（**设备 [Devices] > 设备管理 [Device Management]**）、NAT 页面（**设备 [Devices] > NAT**）或 VPN 页面（**设备 [Devices] > VPN**）中的选项卡时，系统不会清除正在刷新的页面上的缓存，而且**保存 (Save)** 按钮无法使用。解决方法：取消对页面或选项卡所做的任何编辑，然后重新选择您要编辑的设备。(CSCuw75367)
- 在某些情况下，如果您创建的 SSL 策略所包含的证书具有多个状态（例如已过期或已撤销），则"连接事件"(Connection Events) 页面（**分析 [Analysis] > 连接 [Connections] > 事件 [Events]**）上的"证书状态"(Certificate Status) 列不显示状态。(CSCuw76040)

- 在极少数情况下，当您在“设备管理”(Device Management) 页面（**设备 [Devices] > 设备管理 [Devices Management]**）上创建或编辑设备接口时，系统会生成没有要舍弃和恢复的缓存 (No cache exists to discard and resume) 错误，并且您无法进行部署。解决方法：刷新“设备管理”(Device Management page) 页面，然后重新部署。(CSCuw77505)
- 在某些情况下，如果您未在设备的“虚拟路由器”(Virtual Router) 页面（**设备 [Devices] > 设备管理 [Devices Management] > 虚拟路由器 [Virtual Router]**）上正确配置 OSPFv3、RIP 或边界网关协议，并且在未保存配置更改的情况下就离开页面，则系统会生成**恢复配置 (To revert back the configuration)** 弹出窗口；点击**是 (Yes)** 可清除虚拟路由器配置页面上的任何编辑，点击**否 (No)** 会让系统在不进行任何编辑的情况下保存虚拟路由器配置页面之前多次生成**恢复配置 (To revert back the configuration)** 弹出窗口。(CSCuw78916)
- 如果将网络发现策略部署到 集群或堆叠 Firepower 7000 系列/8000 系列设备（在版本 6.0 中称为高可用性对），系统会错误地计算集群或堆栈中的所有设备的数量，而不是为集群或堆栈指示一台设备。（CSCuw79241 和 CSCuw79243）
- 在 Firepower 管理中心、Firepower 7000 系列或 8000 系列设备上进行初始化设置后，如果您从网络地址转换器 (NAT) 设备后面连接设备，系统会提供一个重定向 URL，此 URL 包含的 IP 地址是您为设备配置的 IP 地址，而非您要连接到的 NAT IP，并且会话会超时。解决方法：更正 URL，以便使用用于通过 Web 进行连接的 NAT IP。(CSCuw79967)
- 如果您卸载版本 5.4.1.3 或更高版本，然后安装更低的 5.4.x 版本，再将系统更新到版本 6.0，则更新到版本 6.0 失败。请先将系统更新到最新版本，然后再将系统更新到版本 6.0。(CSCuw81780)
- 在某些情况下，如果您未在注册设备之前为设备选择所需的许可证，系统会生成由于验证错误，初始策略部署未开始。要了解详细信息，请重新进行手动部署 (Initial policy deployment not started due to validation errors. For details, redeploy manually) 这一消息。有关为设备选择正确的许可证的详细信息，请参阅 *《Firepower 管理中心配置指南》* 中的“Licensing the FireSIGHT System”（许可 FireSIGHT 系统）一章。(CSCuw85743)
- 在某些情况下，如果您部署的 NAT 策略中包含的规则定位到 Firepower 7000 系列或 8000 系列受管设备的路由接口，然后集群化处理受管设备（在版本 6.0 中，称为高可用性对），则某些 NAT 规则会继续定位受管设备的路由接口，而非改为定位本应定位的高可用性接口。解决方法：编辑包含个别接口的规则，手动创建高可用性接口，然后重新部署。(CSCuw89223)
- “HTTP 列表”(HTTP Listing) 页面（**设备 [Device] > 平台设置 [Platform Settings] > Firepower 威胁防御平台设置 [Firepower Threat Defense Platform Settings] > HTTP**）将**身份验证证书 (Authentication Certificate)** 列为可配置字段，而实际上该字段并不是可配置字段。(CSCuw89605)
- 在某些情况下，系统会针对由 HTTP 预处理器规则中未指定的端口处理的大量 HTTP 流量生成事件。解决方法：使用 GID 119 和 SID 15 将端口添加到 HTTP 预处理器规则中。(CSCuw90033)
- 如果您在备份 Firepower 管理中心时开始部署，系统不会提示您通信渠道受阻且策略无法部署。请等到备份过程处理完毕，然后再开始部署。(CSCuw90629)
- 在某些情况下，如果您创建将入侵策略作为默认操作的访问控制策略，则默认操作旁边的变量设置图标将无法正确显示。解决方法：更改默认操作以使用其他入侵策略（这样会使图标显示出来），然后再重新将默认操作改回之前的入侵策略。(CSCuw94067)
- 在某些情况下，Firepower 管理中心的部署窗口会在您将 Firepower 管理中心更新为版本 6.0 并部署配置更改后显示不正确的时间戳。(CSCuw94083)
- 在某些情况下，如果您创建了 OSPFv3 路由器，但未在路由器页面（**设备 [Devices] > 设备管理 [Device Management] > 路由器 [Router]**）的“高级设置”(Advanced Settings) 选项卡中配置手动路由器 ID，则系统不会使用未命名的 IPv4 IP 地址，并且会生成OPSFv3 路由器进程未启动，因为尚未配置路由器 ID。OSPFv3 中未配置路由器 ID，并且接口中未配置 Ipv4 地址 (OPSFv3 router process will not start as no router ID has been configured. Neither router ID in OSPFv3 nor IPv4 address configured in Interfaces) 错误消息。(CSCuw95485)
- 如果您创建的关联规则配置为与 **MAC 供应商是 (MAC Vendor is)** 条件匹配，则系统会生成警告：没有任何供应商与此字符串匹配 (Warning: no vendors match this string) 的警告，并且不会执行关联规则。解决方法：更新漏洞数据库 (VDB)。如果 VDB 更新不能解决此问题，请使用 **MAC 供应商包含 (MAC Vendor contains)** 条件，而非 **MAC 供应商是 (MAC Vendor is)** 条件。(CSCuw96022)

- 从 Firepower 管理中心“智能许可用户界面”(Smart Licensing user interface) 页面（**系统 [System] > 本地 [Local] > 系统策略 [System Policy]**）到 Cisco Smart Software Manager 的链接指向已更新的链接，而且这个更新后的链接还会重定向。解决方法：如果重定向出现的速度不太快，请连接到 https://software.cisco.com/#module/SmartLicensing。(CSCuw96552)
- 在某些情况下，如果您部署的访问控制策略引用了出于恶意软件防护目的配置的文件策略，则在已注册到运行版本 6.0 的 Firepower 管理中心且运行版本 5.4.0 的设备上进行部署会失败。(CSCuw97809)
- 在某些情况下，如果您在“入侵策略”页面（**策略 [Policies] > 入侵 [Intrusion] > 入侵策略 [Intrusion Policy]**）上的“高级设置”(Advanced Settings) 中启用敏感数据检测，则系统不会在目标域中重新加载“入侵策略”(Intrusion Policy) 页面，但它原本应该这么做。解决方法：保存或手动重新加载“入侵策略”(Intrusion Policy) 页面。(CSCuw97864)
- 在某些情况下，如果将在运行版本 6.0 的设备上配置的时间设置为比 Firepower 管理中心中配置的时间早，那么向 Firepower 管理中心注册受管设备会导致恢复连接时出现问题。解决方法：执行 `/etc/rc.d/init.d/pm restart` CLI 命令。如果连接问题依然存在，请与支持部门联系。(CSCuw97948)
- 在某些情况下，如果将在运行版本 6.0 的设备上配置的时间设置为比 Firepower 管理中心中配置的时间早，那么向 Firepower 管理中心注册受管设备会导致连接问题，并且系统可能无法恢复连接。解决方法：执行 `/etc/rc.d/init.d/pm restart` CLI 命令。如果连接问题依然存在，请与支持部门联系。(CSCuw97948)
- 在某些情况下，如果用户界面启动恢复，会话将会中断，您必须重新登录，才能查看恢复操作的状态。(CSCuw98296)
- 在某些情况下，如果您在运行版本 6.0 的 Firepower 管理中心上创建两个子域，注册 、7000 系列或 8000 系列设备，创建网络对象替代，并部署访问控制策略，然后将一个子域中的设备移到另一个子域中，则系统会删除“对象”(Object) 页面中的替代值。(CSCuw98708)
- 在运行 Mac 操作系统的系统上，版本 6.0 不支持 Safari Web 浏览器。请使用 Firefox、Chrome 或 Internet Explorer。(CSCuw98876)
- 在某些情况下，如果托管虚拟设备的系统使用大量流量，那么向虚拟设备进行部署可能会导致暂时性网络问题。(CSCux00380)
- 在某些情况下，入侵事件不显示正确的源 IP 地址或正确的目标 IP 地址。解决方法：浏览“连接事件”(Connection Events) 页面（**分析 [Analysis] > 连接 [Connections] > 事件 [Events]**），以查看入侵事件的正确的源 IP 地址和目标 IP 地址。(CSCux00385)
- 在某些情况下，系统不会为由使用会话初始协议 (SIP) 的呼叫建立的实时传输协议 (RTP) 连接创建针孔，这样会阻止为 SIP 呼叫创建 VOIP 信道。（CSCux03758 和 CSCux09765）
- 虽然瘦小客户端控制协议 (SCCP) 可以使用应用检测器，但系统不会为 SCCP 数据包建立的 RTP 连接创建针孔。(CSCux05468)
- 在某些情况下，当向大量设备部署策略时，如果 Snort 无法重启，则策略部署会超时和失败。(CSCux07861)
- 如果将子域中的 NAT 策略部署到 Firepower 7000 系列或 8000 系列设备，并将设备移到新域中，则部署失败。解决方法：在新域中创建一个新的 NAT 策略并定位正确的设备，然后重新部署。(CSCux10651)
- 在某些情况下，如果您在已注册的设备上创建 VPN 部署，并将该设备从一个域移到另一个域，然后再部署，则部署会失败，并且系统会生成`预部署全局配置生成。找不到策略信息 (Pre-deploy Global Configuration Generation. Cannot find policy information)` 错误消息。解决方法：先删除 VPN 配置，然后再将设备移到另一个域中。另一种解决方法是，取消注册设备，然后将设备注册到 Firepower 管理中心，而后创建 VPN 部署，再进行部署。(CSCux10820)
- 版本 6.0 不支持在 Firepower 管理中心上使用采用 RSASSA-PSS 签名算法的证书。如果您使用此类证书将 Firepower 管理中心更新到版本 6.0，或者在版本 6.0 中添加此类证书，则系统将不允许您登录管理中心 Web 界面，并且会生成`无法授权访问。如果依然无法访问此设备，请与系统管理员联系 (Unable to authorize access. If you continue to have difficulty accessing this device, please contact the system administrator)` 这一错误。解决方法：在更新之前，使用 `sha1WithRSAEncryption` 或 `sha256WithRSAEncryption` 算法生成并安装 SSL 证书，然后重启 Firepower 管理中心，或者使用默认的 Firepower 管理中心证书，然后重启设备。如果您无法在 Firepower 管理中心上访问用户界面，请与支持部门联系。(CSCux30610)

- 在某些情况下，如果您创建的访问控制策略引用的 SSL 策略包含的网络对象在运行版本 5.4 或更高版本的受管 Firepower 设备上有多个条目，并且您将系统更新到版本 6.0，那么在运行版本 6.0 的 Firepower 管理中心上部署策略会失败。解决方法：将系统更新到版本 6.0 后编辑 SSL 策略并删除网络对象，然后添加网络对象，并重新进行部署。(CSCux31618)
- 如果 Firepower 管理中心使用的证书是借助大于 2048 位的公共服务器密钥生成的，则您将无法在更新到版本 6.0 后登录 Firepower 管理中心 Web 界面。解决方法：生成服务器证书请求，然后使用此请求将生成的证书应用到 Firepower 管理中心，从而替代使用较长公共密钥创建的证书。您可以通过 Firepower 管理中心上的本地配置设置执行服务器证书请求和证书上传（**系统 [System] > 本地 [Local] > 配置 [Configuration] > HTTPS 证书 [HTTPS Certificate]**）。如果不使用 Firepower 管理中心中的 CSR 生成证书，请使用大小为 2048 位或更小的公共密钥。如果生成的证书超过 2048 位，并且失去了对管理中心 Web 界面的访问权限，请与支持部门联系。(CSCux35430)
- 在某些情况下，如果您部署的访问控制策略包含自定义 URL，则 CPU 的使用率会比较高，并且系统会出现问题。(CSCux35554)
- 如果运行 Firepower 威胁防御的设备已注册到运行版本 6.0 的 Firepower 管理中心中至少十天，则系统会遇到以下问题：注册新设备时，Firepower 管理中心会生成 `CSM 失败状态：(2) CSM 无法提供设备状态 (2) (CSM failed state: [2] CSM can not provide device state [2])` 错误，并且设备注册失败；将 Firepower 管理中心 从 6.0.0 更新为更新版本时会生成`安装失败。对等机发现不完整。请稍后重试 (Installation failed. Peer discovery incomplete. Please retry after few moments)` 错误，并且更新失败；备份 Firepower 管理中心时，会生成`注册或 CSM 状态阻止备份 (Registration or CSM state are blocking backup)` 错误，并且备份失败；尝试创建、更新或删除 Firepower 管理中心上的域时，会生成`传感器注册流程正在运行。请等待此流程完成。(A sensor registration process is running. Please wait until process completes.)` 错误，并且系统无法成功创建、更新或删除所选的域。解决方法：通过 Firepower 管理中心下载版本 6.0 的安装文件，并以根用户身份执行 `/usr/local/sf/bin/install_update.pl /var/sf/updates/[UPGRADE_PKG_NAME].sh` CLI 命令，将 Firepower 管理中心更新到版本 6.0，而不是通过 Web 界面进行更新。(CSCux89875)

获取帮助

感谢您选用 Firepower 系统。

有关获取文档、使用 Cisco 漏洞搜索工具 (BST)、提交服务请求和收集 Firepower 系统其他相关信息的内容，请参阅 *“What's New in Cisco Product Documentation”*（思科产品新特性文档），网址为：http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html。

请订阅 *“What's New in Cisco Product Documentation”*（思科产品新特性文档），该文档以 RSS 源的形式列出所有新的和经过修订的 Cisco 技术文档，并通过阅读器应用直接将内容提供至您的桌面。RSS 源是一种免费服务。

如果您有任何关于 Firepower 系统的疑问或需要帮助，请通过以下方式与 Cisco 支持部门联系：

- 请访问 Cisco 支持站点，网址为 http://support.cisco.com/。
- 将问题发送至 Cisco 技术支持部门的邮箱：tac@cisco.com。
- 致电 Cisco 支持部门，电话号码为：1.408.526.7209 或 1.800.553.2447。

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。要查看思科商标列表，请转至此 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。(1110R)

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。

© 2016 年思科系统公司。保留所有权利。

本文档使用含 10% 用后废料的再生纸在美国印制出版。