思科 Firepower 4100/9300 FXOS 发行说明，2.6(1)

首次发布日期: 2019 年 3 月 13 日

上次修改日期: 2019 年 6 月 27 日

思科 Firepower 4100/9300 FXOS 发行说明，2.6(1)

本文档包含思科 Firepower 可扩展操作系统 (FXOS) 2.6(1) 的版本信息。

此版本说明可作为文档规划图中所列出的其他文档的补充内容：

- http://www.cisco.com/go/firepower9300-docs
- http://www.cisco.com/go/firepower4100-docs

注释 用户文档的在线版本在初始发布后有时会有更新。因此，如果 Cisco.com 上的文档中包含的信息与产品上下文相关帮助中包含的任何信息不一致，应以前者为准。

简介

思科 Firepower 安全设备是网络和内容安全解决方案的下一代平台。Firepower 安全设备是思科以应用为中心的基础设施 (ACI) 安全解决方案的一部分，并且提供为实现可扩展性、一致控制和简化管理而构建的灵活、开放、安全的平台。

Firepower 安全设备提供以下功能：

- 基于机箱的模块化安全系统 - 提供高性能、灵活的输入/输出配置和可扩展性。
- Firepower 机箱管理器 - 图形用户界面可简单、直观地显示当前机箱状态并支持简化的机箱功能配置。
- FXOS CLI - 提供基于命令的接口，用于配置功能，监控机箱状态和访问高级故障排除功能。
- FXOS REST API - 允许用户以编程方式配置和管理其机箱。

新增内容

FXOS 2.6.1.157 的新增功能

思科 FXOS 2.6.1.157 推出了以下新功能：

- 支持 Firepower 威胁防御 6.4.0。
- 支持 56 物理核心安全模块 SM-56。
- 您现在可以在同一个 Firepower 9300 上同时部署 ASA 和 FTD 逻辑设备。

  注释 要求使用 ASA 9.12(1) 和 Firepower 6.4.0。

- 您现在可以启用用于模块/安全引擎上的一个容器实例的 TLS/SSL 硬件加速。TLS/SSL 硬件加速对其他容器实例禁用，但对本地实例启用。有关详细信息，请参阅《Firepower 管理中心配置指南》。
- 新增/修改的命令：**config hwCrypto enable, show hwCrypto**
- 各种问题的修复补丁（请参阅 FXOS 2.6.1.157 中已解决的漏洞，第 7 页）。

FXOS 2.6.1.131 的新增功能

思科 FXOS 2.6.1.131 推出了以下新功能：

- 支持 ASA 9.12(1)。
- 支持 Radware DefensePro 8.13.01.09-3。
- 支持 Firepower 4115、4125 和 4145 安全设备。
- 支持 40 和 48 物理核心安全模块 SM-40 和 SM-48。
- 现在，您可以在同一 Firepower 9300 上混装不同类型的安全模块。支持此功能需要 ASA 9.12(1) 或更高版本。

  注释 要对 Firepower 9300 使用群集，安装在机箱上的所有安全模块必须为同一类型。

- 对于 FTD 引导程序配置，您现在可以在 Firepower 机箱管理器中设置 FMC 的 NAT ID。以前，您只能在 FXOS CLI 或 FTD CLI 内设置 NAT ID。通常，无论是出于路由目的还是为了进行身份验证，都需要两个 IP 地址（连同一个注册密钥）- FMC 指定设备 IP 地址，设备指定 FMC IP 地址。但是，如果您只知道其中一个 IP 地址（这是实现路由目的的最低要求），您还必须在连接的两端指定唯一的 NAT ID，以建立对初始通信的信任，并查找正确的注册密钥。FMC 和设备使用注册密钥和 NAT ID（而不是 IP 地址）对初始注册进行身份验证和授权。

新增/修改的屏幕：

逻辑设备 > 添加设备 > 设置 > Firepower 管理中心 NAT ID 字段

- 现在，您可以在配置导出期间配置用于加密敏感数据的密钥。必须先设置加密密钥，才可导出配置。导入该配置时，请确保在系统上设置相同的加密密钥。
- 现在，您可以从 Firepower 机箱管理器生成和下载技术支持日志文件。
- 现在，您可以选择是启用还是禁用 LLDP。
- 现在，您可以使用新的低接触调配方法在管理端口上首次进行设置。
- 各种问题的修复补丁（请参阅 FXOS 2.6.1.131 中已解决的漏洞，第 7 页）。

软件下载

可从以下某个 URL 下载 FXOS 的软件映像及受支持的应用：

- Firepower 9300 - https://software.cisco.com/download/type.html?mdfid=286287252
- Firepower 4100 - https://software.cisco.com/download/navigator.html?mdfid=286305164

有关特定版本 FXOS 支持的应用的信息，请参阅以下 URL 中的思科 *FXOS* 兼容性指南：

http://www.cisco.com/c/en/us/td/docs/security/Firepower/fxos/compatibility/fxos-compatibility.html

重要说明

- 在 Firepower 4110 或 4120 设备上当前运行的 Firepower 威胁防护应用程序的服务链中配置 Radware DefensePro (vDP) 时，安装将会失败并显示故障警报。解决办法是在安装 Radware DefensePro 应用程序之前停止 Firepower 威胁防护应用程序实例。请注意，此问题和解决方法适用于 Firepower 4110 和 4120 设备上使用 Firepower 威胁防御链接的所有受支持版本的 Radware DefensePro 服务。
- 固件升级 - 建议使用最新固件升级 Firepower 4100/9300 安全设备。有关如何安装固件更新和每个更新中包含的修补程序的信息，请参阅 https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/firmware-upgrade/fxos-firmware-upgrade.html。
- 升级网络或安全模块时，系统会生成某些故障，然后自动清除。其中包括“不支持　热插拔”或者“在联机状态时删除模块”错误。如果按照《思科 *Firepower 9300* 硬件安装指南》(http://www.cisco.com/go/firepower9300-install) 或《思科 *Firepower 4100* 系列硬件安装指南》(http://www.cisco.com/go/firepower4100-install) 中所述的相应程序操作，这些故障将自动清除，无需执行其他操作。

适配器引导加载程序升级

FXOS 2.6(1) 包含额外的测试，用于验证安全设备上的安全模块适配器。安装 FXOS 2.4.1.101 或更高版本后，您可能会收到一则类似以下内容的严重故障，指示您应更新安全模块适配器的固件：

严重故障 *F1715 2017-05-11T11:43:33.121 339561* 安全模块 *1* 上的适配器 *1* 需要进行重要的固件升级。请参阅随本版本发布的 *FXOS* 发行说明中的适配器引导程序升级说明。

如果收到上述消息，请按以下程序为适配器更新启动映像：

1. 连接到 Firepower 安全设备上的 FXOS CLI。有关说明，请参阅《思科 Firepower 4100/9300 FXOS CLI 配置指南 [2.6(1)]》或《思科 Firepower 4100/9300 FXOS Firepower 机箱管理器配置指南 [2.6(1)]》中的“访问 FXOS CLI”主题。
2. 输入您要更新其启动镜像的适配器的适配器模式：

   fxos-chassis# **scope adapter 1**/*security_module_number*/*adapter_number*
3. 输入 **show image** 以查看可用的适配器映像，并验证是否可以安装 fxos-m83-8p40-cruzboot.4.0.1.62.bin：

```
fxos-chassis /chassis/server/adapter # show image
Name Type Version

------------------------------------------- ------------------- -------

fxos-m83-8p40-cruzboot.4.0.1.62.bin Adapter Boot 4.0(1.62)

fxos-m83-8p40-vic.4.0.1.51.gbin Adapter 4.0(1.51)
```

4. 输入 **update boot-loader** 将适配器启动映像更新到版本 4.0.1.62：

```
fxos-chassis /chassis/server/adapter # update boot-loader 4.0(1.62)
Warning: Please DO NOT reboot blade or chassis during upgrade, otherwise, it may cause
adapter to become UNUSABLE!
After upgrade has completed, blade will be power cycled automatically
fxos-chassis /chassis/server/adapter* # commit-buffer
```

5. 输入 **show boot-update status** 以监控更新状态：

```
fxos-chassis /chassis/server/adapter # show boot-update status
State: Updating
fxos-chassis /chassis/server/adapter # show boot-update status
State: Ready
```

6. 输入 **show version detail** 以验证更新是否成功：

注释 您的 **show version detail** 输出可能不同于以下示例。不过，请验证并确保 Bootloader-Update-Status 为“就绪”且 Bootloader-Vers 为 4.0(1.62)。

```
fxos-chassis /chassis/server/adapter # show version detail
Adapter 1:
Running-Vers: 5.2(1.2)
Package-Vers: 2.2(2.17)
Update-Status: Ready
Activate-Status: Ready
Bootloader-Update-Status: Ready
Startup-Vers: 5.2(1.2)
Backup-Vers: 5.0(1.2)
Bootloader-Vers: 4.0(1.62)
```

系统要求

您可以使用以下浏览器访问 Firepower 机箱管理器：

- Mozilla Firefox - 版本 42 及更高版本
- Google Chrome - 版本 47 及更高版本
- Microsoft Internet Explorer - 版本 11 及更高版本

我们使用 Mozilla Firefox 版本 42、Google Chrome 版本 47 和 Internet Explorer 版本 11 对 FXOS 2.3(1) 对 FXOS 2.3(1) 进行了测试。我们预计这些浏览器的未来版本也能正常运行。但是，如果您遇到任何浏览器相关问题，我们建议您恢复到其中一个经过测试的版本。

升级说明

如果您的 Firepower 9300 或 Firepower 4100 系列安全设备当前运行的是 FXOS 2.0(1) 或更高的内部版本，可以将其升级到 FXOS 2.6(1.157)。

有关升级说明，请参阅《思科 Firepower 4100/9300 升级指南》。

安装说明

- 升级到 FXOS 2.6(1) 可能需要长达 45 分钟。请相应规划您的升级活动。
- 如果要升级运行独立逻辑设备的 Firepower 9300 或 Firepower 4100 系列安全设备，或者要升级运行机箱内群集的 Firepower 9300 安全设备，则升级期间流量不会通过该设备。
- 如果要升级属于某机箱间群集的 Firepower 9300 或 Firepower 4100 系列安全设备，则升级期间流量不会通过正在升级的设备。但是，该群集中的其他设备仍然会通过流量。

尚未解决和已解决的漏洞

可通过思科缺陷搜索工具查看这一版本中尚未解决和已解决的缺陷。通过这一基于 Web 的工具，您可以访问思科缺陷追踪系统，其中记录了关于此本产品和其他思科硬件及软件产品的缺陷和漏洞信息。

注释 您必须拥有 Cisco.com 帐户才能登录并访问思科缺陷搜索工具。如果您还没有此帐户，请注册一个帐户。

有关思科漏洞搜索工具的详细信息，请参阅漏洞搜索工具帮助及常见问题。

遗留漏洞

下表列出了在发布此发行说明时尚未解决的漏洞。

表 *1:* 影响 ***FXOS 2.6(1)*** 的遗留漏洞

标识符	描述
CSCus73654	对于 LD 分配的管理接口，ASA 未标记为仅管理
CSCuu33739	端口通道中的物理接口速度有误
CSCuw31077	应验证应用于接口的过滤器
CSCux37821	平台设置身份验证顺序字段显示仅最低可用
CSCux63101	内存阵列下的所有内存在“可操作”列中显示为“未知”
CSCux77947	当以高速率发送数据时，Pcap 文件大小未正确更新
CSCux98517	应允许从机箱管理器取消修饰 VDP 的数据端口
CSCuz93180	如果验证失败，AAA LDAP 配置不会保留信息
CSCva86452	关闭电源期间，连接到 10G 和 40G SR FTW 卡的交换机中出现链路振荡
CSCvc03494	无法将 Radware vDP 添加到 APSolute Vision 中。解决方法是，必须手动下载设备驱动程序并将其安装到 Vision 中。
CSCvc44522	警告：管理控制器服务器 1/1 中的日志容量处于非常低的警告状态
CSCvd90177	通过 FXOS 2.2.1.57 在 4150 上重新加载管理引擎后，安全模块进入故障状态
CSCvf16473	MIO 上未捕获到 LLDP 数据包
CSCvf94658	擦除配置后，设备无法访问 SSH
CSCvg68299	故障转移后，FXOS 机箱管理器接口与 FTD 的关联被取消
CSCvi71367	重新启动后管理引擎崩溃 - 无法处理内核 NULL 指针取消引用
CSCvj93832	在 sspos 中使用 "init 6" 的 x86 电源循环后，M5 Blades x86 cpu 无法启动
CSCvk26697	使用 92.4.1.2889 映像检测到 bcm_usd_log 核心文件
CSCvk72915	重新启动后，安全模块卡在 Rommon 中不一致
CSCvm66013	重新启动期间管理引擎没有反应。发现内核死机问题。
CSCvm84592	当为捕获会话完成“编辑会话”时，过滤器配置丢失
CSCvm86523	第六个节点不会 ssp3ru 群集 6.3.0-1592
CSCvn42252	低接触调配调试命令模式提示无法正常工作
CSCvn57429	Ftd 应用程序实例卡在安装失败状态，同时显示 INSTALL_ERROR。应用程序内部脚本错误。
CSCvo03589	在 MI 情境下，应用程序代理心跳可能丢失
CSCvo30356	升级后端口通道处于挂起状态
CSCvo40078	显示正常运行时间错误

标识符	描述
CSCvo55237	即使一个安全模块正在运行，全局升级按钮仍会灰显
CSCvo55510	FXOS 低接触调配屏幕不允许前缀
CSCvo55809	ASA 应用在 2.6.1.112 + ASA 上卡在安装状态 9.12.0.125
CSCvo58998	FXOS Cruz 适配器未验证逻辑设备发送的数据，导致卸载的数据包丢失
CSCvo60117	尽管在机箱管理器中显示为已分配，但接口未关联到 MI 实例
CSCvo74625	6.4.0 - 当管理网关配置为数据接口时，IPv6 路由不适用于 WM 和 KP
CSCvo83802	重新启动后，群集节点管理连接丢失
CSCvp10674	在安装 vDP 并将 FXOS 升级到版本 2.4.1 后，FTD 无法联机
CSCvp44939	在 2.6.1.157 + 9.12.1.111 上，ASA 应用程序卡在“正在安装”状态，并显示错误 'SMA_blade_reboot_inprogress'

FXOS 2.6.1.157 中已解决的漏洞

下表列出了以前版本中注明的由客户发现的漏洞，这些漏洞在 FXOS 2.6.1.157 中已得到解决：

表 *2: FXOS 2.6.1.157* 中已解决的漏洞

标识符	描述
CSCvm72541	如果端口通道的状态为“关闭”，则 interfaceMapping 消息中的速度为 0
CSCvo10291	预共享密钥包含数据库字符时，使用 RADIUS 的 FTD 外部验证失败
CSCvo29067	FXOS 升级挂起并已开始生成 DME 核心文件
CSCvo44171	由于许可证管理器每 30 秒进行一次不正常的身份验证更新，Firepower 版本 2.2.2.86 重新加载
CSCvo64091	SSP：群集从属 FTD 调配失败，因为“必要的外部端口不可用”
CSCvo65464	FPR2100：EIGRP 路由（通过端口通道学习的接口）变为无限 FD
CSCvo75349	由于内存损坏，FXOS Blade CRUZ FW 核心转储
CSCvo87116	MTS 消息卡在 AppAG recv_q 中
CSCvp09791	FXOS/FTD 多实例部署多播流量中断

FXOS 2.6.1.131 中已解决的漏洞

下表列出了以前版本中注明的由客户发现的漏洞，这些漏洞在 FXOS 2.6.1.131 中已得到解决：

表 *3: FXOS 2.6.1.131* 中已解决的漏洞

标识符	描述
CSCvg54742	FTW - 当机箱从 FXOS GUI 正常关闭时，看到流量损失
CSCvj00997	"show open-network-ports" 没有在 FP4100 系列上显示正确的信息
CSCvj47857	因 ethpm hap 重置，MIO 在启动时崩溃
CSCvj96380	如果开关旁路使能失败，SAM 耦合器应强制 FTW 旁路
CSCvk46399	MIO 重新启动后看到 svc_sam_bladeAG_log 核心
CSCvm31905	OpenSSH Bailout 延迟用户枚举漏洞
CSCvm37578	本地用户登录 asaConsoleDbg 权限被拒错误
CSCvm51377	Linux 内核 acpi_ns_evaluate() 函数信息泄漏漏洞
CSCvm97473	Linux 内核驱动程序/tty/n_tty.c 拒绝服务漏洞
CSCvn24594	在启动 NTPD 之前，从管理引擎添加刀片系统时钟的 NTPDATE 更新
CSCvn41072	Linux 内核 vcpu_scan_ioapic 函数问题
CSCvn50990	Wireshark DCOM 解析器拒绝服务漏洞
CSCvn68238	DPDK vhost-user 接口信息泄漏漏洞
CSCvn76908	[ciam] Linux 内核 USB 子系统数据大小检查处理漏洞
CSCvn83018	Firepower 2100：进程 LACP 出现内存泄漏
CSCvo08464	[ciam] Sudo get_process_ttyname 功能设备名称处理安全绕过漏洞
CSCvo31071	当设备重新加入群集时，流量下降。
CSCvo58998	FXOS Cruz 适配器未验证逻辑设备发送的数据，导致卸载的数据包丢失

相关文档

有关 Firepower 9300 或 4100 系列安全设备及 FXOS 的更多信息，请参阅思科 FXOS 导航文档。

网上资源

思科提供在线资源来下载文档/软件/工具、查询错误以及创建服务请求。这些资源可用于安装和配置 Firepower 软件以及解决和消除技术问题。

- 思科技术支持及下载站点：https://www.cisco.com/c/en/us/support/index.html
- 思科漏洞搜索工具：https://tools.cisco.com/bugsearch/
- 思科通知服务：https://www.cisco.com/cisco/support/notifications.html

使用思科技术支持及下载站点上的大多数工具时，需要 Cisco.com 用户 ID 和密码。

联系思科

如果上面列出的联机资源无法解决您的问题，请联系思科 TAC：

- 向思科 TAC 发送电子邮件：tac@cisco.com
- 致电思科 TAC（北美）：1.408.526.7209 或 1.800.553.2447
- 致电思科 TAC（全球）：思科全球支持联系人

通信、服务和其他信息

- 要及时从思科收到相关信息，请注册思科配置文件管理器。
- 要使用重要技术实现您期望实现的业务影响，请访问思科服务。
- 要提交服务请求，请访问思科支持。
- 要了解并浏览安全且经过验证的企业级应用、产品、解决方案和服务，请访问思科 Marketplace。
- 要获取一般网络、培训和认证主题相关的信息，请访问思科出版社。
- 要查找有关特定产品或产品系列的保修信息，请访问思科保修服务查找工具。