



思科 FXOS 1.1(4) 版本说明

首次发布日期：2016 年 3 月 20 日

最新修订日期：2016 年 11 月 18 日

本文档包含思科 Firepower 可扩展操作系统 1.1(4) 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：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。

本文档包含以下部分：

- 简介（第 2 页）
- 新功能（第 2 页）
 - FXOS 1.1.4.140 的新增功能（第 2 页）
 - FXOS 1.1.4.117 的新增功能（第 2 页）
 - FXOS 1.1.4.95 的新增功能（第 2 页）
- 映像详细信息（第 3 页）
- 重要说明（第 3 页）
- 系统要求（第 4 页）
- 升级说明（第 4 页）
 - Firepower 9300 上的 FXOS/ASA 的升级路径（第 4 页）
 - 安装说明（第 5 页）
 - 升级独立的 Firepower 安全设备（第 5 页）
 - 升级 ASA 故障切换对（第 5 页）
 - 升级机箱间集群（第 8 页）
- 尚未解决和已解决的缺陷（第 10 页）
 - 遗留漏洞（第 10 页）
 - FXOS 1.1.4.140 中已解决的漏洞（第 11 页）
 - FXOS 1.1.4.117 中已解决的漏洞（第 12 页）
 - FXOS 1.1.4.95 中已解决的漏洞（第 12 页）
- 相关文档（第 13 页）
- 获取文档和提交服务请求（第 13 页）

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。

新功能

FXOS 1.1.4.140 的新增功能

除了早期版本中的功能以外，思科 Firepower 可扩展操作系统 1.1.4.140 还推出了以下新功能：

- 在 Firepower 4100 系列安全设备上支持直流电源模块。
- 将可能的最大 MTU 值增加到 9216，从而可以在逻辑设备上支持巨型帧。
- 各种问题的修复补丁（请参阅FXOS 1.1.4.140 中已解决的漏洞（第 11 页））。

FXOS 1.1.4.117 的新增功能

除了早期版本中的功能以外，思科 Firepower 可扩展操作系统 1.1.4.117 还推出了以下新功能：

- 各种问题的修复补丁（请参阅FXOS 1.1.4.117 中已解决的漏洞（第 12 页））。

FXOS 1.1.4.95 的新增功能

思科 Firepower 可扩展操作系统 1.1.4.95 推出了以下新功能：

- 各种问题的修复补丁（请参阅FXOS 1.1.4.95 中已解决的漏洞（第 12 页））。
- 支持 ASA 9.6(1)。
- 支持 Firepower 威胁防御 6.0.1。
- 服务链 - Firepower 9300 可支持在单个安全模块上将两项服务链接在一起。在当前支持的服务链配置中，Radware DefensePro (vDP) 第三方应用在 ASA 防火墙前面运行，可防止客户和其他应用受到 DDoS 攻击。Radware DefensePro 应用不支持在 Firepower 4100 系列安全设备上使用，也不支持与 Firepower 威胁防御配合使用。
- 您现在可以使用 CLI 来更新 Firepower 安全设备上的固件。
- 您现在可以在 Firepower 机箱管理器中存储配置导入/导出设置，以便在今后执行导入或导出操作时可以使用这些设置。
- 在 Firepower 9300 安全设备上支持 Firepower 双端口 100G 双位宽网络模块 (FPR-DNM-2X100G)。有关详细信息，请参阅《*思科 Firepower 9300 硬件安装指南*》，网址是：
http://www.cisco.com/c/en/us/td/docs/security/firepower/9300/hw/guide/b_install_guide_9300.html。

注：Firepower 9300 安全设备必须安装有固件包 1.0.10 或更高版本，才能使用 Firepower 100G 网络模块。有关如何验证固件包版本以及在需要时更新固件的说明，请参阅《*思科 FXOS CLI 配置指南, 1.1(4)*》或《*思科 FXOS Firepower 机箱管理器配置指南, 1.1(4)*》中的“固件升级”主题，网址是：
<http://www.cisco.com/go/firepower9300-config>。

映像详细信息

FXOS 1.1.4.140 包括/支持以下组件：

组件	内部版本号	映像位置
FXOS 1.1(4) 平台捆绑包	fxos-k9.1.1.4.140.SPA	FXOS 1.1(4) 软件下载
Firepower 威胁防御 6.1.0	cisco-ftd.6.1.0.330.SPA.csp	FTD 6.1.0 软件下载
ASA 9.6(2)	cisco-asa.9.6.2.SPA.csp	ASA 9.6(2) 软件下载
Radware vDP	radware-vdp.1.1.2.32-3.SPA.csp	Radware vDP 软件下载

FXOS 1.1.4.117 包括/支持以下组件：

组件	内部版本号	映像位置
FXOS 1.1(4) 平台捆绑包	fxos-k9.1.1.4.117.SPA	FXOS 1.1(4) 软件下载
Firepower 威胁防御 6.0.1	cisco-ftd.6.0.1.1213.SPA.csp	FTD 6.0.1 软件下载
ASA 9.6(1)	cisco-asa.9.6.1.5.SPA.csp	ASA 9.6(1) 软件下载
Radware vDP	radware-vdp.1.1.2.32-3.SPA.csp	Radware vDP 软件下载

FXOS 1.1.4.95 包括/支持以下组件：

组件	内部版本号	映像位置
FXOS 1.1(4) 平台捆绑包	fxos-k9.1.1.4.95.SPA	FXOS 1.1(4) 软件下载
Firepower 威胁防御 6.0.1	cisco-ftd.6.0.1.1213.SPA.csp	FTD 6.0.1 软件下载
ASA 9.6(1)	cisco-asa.9.6.1.SPA.csp	ASA 9.6(1) 软件下载
Radware vDP	radware-vdp.1.1.2.32-3.SPA.csp	Radware vDP 软件下载

有关 FXOS 特定版本支持的应用的信息，请参阅《*思科 FXOS 兼容性指南*》，网址是：
<http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html>

重要说明

- Firepower 9300 安全设备必须安装有固件包 1.0.10 或更高版本，才能结合使用 Firepower 100G 网络模块。有关如何验证固件包版本以及在需要时更新固件的说明，请参阅《*思科 FXOS CLI 配置指南, 1.1(4)*》或《*思科 FXOS Firepower 机箱管理器配置指南, 1.1(4)*》中的“固件升级”主题，网址是：
<http://www.cisco.com/go/firepower9300-config>。
- 如果您运行的是 FXOS 2.0(1)，并且具有运行 9.6(2) 的 ASA 逻辑设备，则在将 FXOS 降级到 1.1(4) 时，逻辑设备将离线。要继续使用您的逻辑设备，您必须将 ASA 降级到 9.6(1)，这样可使逻辑设备恢复在线状态。之后，您可以将 ASA 升级回 9.6(2)。
- 在将 FXOS 逻辑设备升级到 ASA 9.6(1) 时，不支持零停机时间升级。

- 从 FXOS 1.1(3) 开始，端口通道的行为已更改。在 FXOS 1.1(3) 和更高版本中，默认情况下，当创建端口通道时，端口通道随即会被配置为 lACP 集群分离，即使已建立物理链路，其状态也显示为断开。在下列情况下，端口通道将退出集群分离模式。
 - 端口通道的端口类型将设置为集群或管理
 - 将端口通道添加为集群中的逻辑设备的数据端口，而且至少有一个安全模块已加入该集群
 如果从逻辑设备删除端口通道或删除逻辑设备，端口通道将恢复为集群分离模式。
- 要使用 ASDM 和其他强加密功能（如 VPN），在部署 ASA 集群后，必须使用 ASA CLI 在主设备上启用强加密 (3DES) 许可证。

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

我们使用 Mozilla Firefox 版本 42 和 Google Chrome 版本 47 在 FXOS 1.1(4) 上执行了测试。我们希望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 安全设备当前运行的是 FXOS 1.1(4.117)，可以将其升级到 FXOS 1.1(4.140)。如果您运行的是 FXOS 的早期版本，请参阅 Firepower 9300 上的 FXOS/ASA 的升级路径（第 4 页），了解有关如何将系统升级到 FXOS 1.1(4.140) 的信息。

Firepower 9300 上的 FXOS/ASA 的升级路径

当前版本	升级路径							
FXOS 1.1(4.117) 和 ASA 9.6.1/9.6.2	→	FXOS 1.1(4.140) 和 ASA 9.6.1/9.6.2						
FXOS 1.1(4.95) 和 ASA 9.6.1/9.6.2	→	FXOS 1.1(4.117) 和 ASA 9.6.1/9.6.2	→	FXOS 1.1(4.140) 和 ASA 9.6.1/9.6.2				
FXOS 1.1(3.x) 和 ASA 9.5.2.x	→	FXOS 1.1(4.95) 和 ASA 9.6.1	→	FXOS 1.1(4.117) 和 ASA 9.6.1/9.6.2	→	FXOS 1.1(4.140) 和 ASA 9.6.1/9.6.2		
FXOS 1.1(2.x) 和 ASA 9.4.x.x	→	FXOS 1.1(3.86) 和 ASA 9.5.2.2	→	FXOS 1.1(4.95) 和 ASA 9.6.1	→	FXOS 1.1(4.117) 和 ASA 9.6.1/9.6.2	→	FXOS 1.1(4.140) 和 ASA 9.6.1/9.6.2
FXOS 1.1(1.x) 和 ASA 9.4.1.152	→	FXOS 1.1(2.178) 和 ASA 9.4.2.146	→	FXOS 1.1(3.86) 和 ASA 9.5.2.2	→	FXOS 1.1(4.95) 和 ASA 9.6.1	→	FXOS 1.1(4.117) 和 ASA 9.6.1/9.6.2
	→	FXOS 1.1(4.140) 和 ASA 9.6.1/9.6.2						

安装说明

- 同时升级 FXOS 平台捆绑包软件和应用 CSP 映像时，在升级 FXOS 平台捆绑包软件之前，请不要将应用 CSP 映像上传到您的安全设备。
- 在将 FXOS 逻辑设备升级到 ASA 9.6(1) 时，不支持零停机时间升级。

升级说明

请参阅适用于您的设备配置的升级说明：

- 有关如何升级独立的 Firepower 安全设备的说明，请参阅[升级独立的 Firepower 安全设备（第 5 页）](#)。
- 有关如何升级配置为 ASA 故障切换对的两个 Firepower 安全设备的说明，请参阅[升级 ASA 故障切换对（第 5 页）](#)。
- 有关如何升级配置为机箱间集群的 Firepower 安全设备的说明，请参阅[升级机箱间集群（第 8 页）](#)。

升级独立的 Firepower 安全设备

执行以下步骤将系统更新到 1.1(4)：

1. 将所需的 FXOS 1.1(4) 映像下载到本地计算机（请参阅映像详细信息）。
2. 将 FXOS 1.1(4) 平台捆绑包映像上传至 Firepower 安全设备。有关说明，请参阅《[思科 Firepower 机箱管理器配置指南 1.1\(4\)](#)》中的“将映像上传至 Firepower 设备”主题（请参阅[相关文档（第 13 页）](#)）。
注： 此时请不要上传应用 CSP 映像。只有当您已经使用平台捆绑包映像成功升级机箱之后，才能上传应用 CSP 映像。
3. 使用 FXOS 1.1(4) 平台捆绑包映像升级您的 Firepower 安全设备。有关说明，请参阅《[思科 Firepower 机箱管理器配置指南，1.1\(4\)](#)》中的“升级 Firepower 可扩展操作系统平台捆绑包”主题（请参阅[相关文档（第 13 页）](#)）。
4. 将应用 CSP 映像上传至 Firepower 安全设备。有关说明，请参阅《[思科 Firepower 机箱管理器配置指南，1.1\(4\) 试用版](#)》中的“将映像上传至 Firepower 设备”主题（请参阅[相关文档（第 13 页）](#)）。

您的系统已成功更新。

您现在可以使用 ASA 映像更新现有的 ASA 逻辑设备，也可以在创建新逻辑设备时使用 ASA 映像。

您可以使用 Firepower 威胁防御映像来配置 Firepower 威胁防御逻辑设备。有关说明，请参阅《[适用于 Firepower 4100 的思科 Firepower 威胁防御快速入门指南](#)》或《[适用于 Firepower 9300 的思科 Firepower 威胁防御快速入门指南](#)》中的“部署 Firepower 威胁防御”一节（请参阅[相关文档（第 13 页）](#)）。

注： 如果您要在当前安装有 ASA 的安全模块上安装 Firepower 威胁防御，则必须先删除现有的 ASA 逻辑设备。有关说明，请参阅《[适用于 Firepower 4100 的思科 Firepower 威胁防御快速入门指南](#)》或《[适用于 Firepower 9300 的思科 Firepower 威胁防御快速入门指南](#)》中的“删除现有逻辑设备和应用配置”主题（请参阅[相关文档（第 13 页）](#)）。

升级 ASA 故障切换对

1. 下载 FXOS 1.1(4) 映像（请参阅[映像详细信息（第 3 页）](#)）。
2. 禁用故障切换：
 - a. 连接到包含 **主** ASA 逻辑设备的 Firepower 安全设备上的 ASA 控制台。有关说明，请参阅《[思科 Firepower 机箱管理器配置指南](#)》中的“连接到应用或修饰器的控制台”（请参阅[相关文档（第 13 页）](#)）。
 - b. 禁用故障切换：
no failover

- c. 在包含 **主** ASA 逻辑设备的 Firepower 安全设备和包含 **辅助** ASA 逻辑设备的 Firepower 安全设备上保存配置：
write memory
3. 升级包含 **辅助** ASA 逻辑设备的 Firepower 安全设备上的 Firepower 可扩展操作系统捆绑包：
 - a. 将 FXOS 1.1(4) 平台捆绑包映像上传至 Firepower 安全设备。有关说明，请参阅《*思科 Firepower 机箱管理器配置指南*》中的“将映像上传至 Firepower 设备”主题（请参阅[相关文档（第 13 页）](#)）。

注：此时请不要上传 ASA 映像。只有当您已经使用 FXOS 1.1(4) 平台捆绑包映像成功升级机箱之后，才能上传 ASA 映像。

 - b. 使用 FXOS 1.1(4) 平台捆绑包映像升级您的 Firepower 安全设备。有关说明，请参阅《*思科 Firepower 机箱管理器配置指南*》中的“升级 Firepower 可扩展操作系统平台捆绑包”主题。
4. 等待机箱重新启动并成功升级：
 - a. 使用 **scope system** 下的 **show firmware monitor** 命令来监控升级过程。
 - b. 升级过程完成后，使用 **scope ssa** 下的 **show app-instance** 命令来验证 ASA 应用已恢复“在线”状态。
5. 升级 **辅助** ASA 逻辑设备上的 ASA 软件：
 - a. 将 ASA 映像上传至 Firepower 安全设备。有关说明，请参阅《*思科 Firepower 机箱管理器配置指南*》中的“将映像上传至 Firepower 设备”主题（请参阅[相关文档（第 13 页）](#)）。
 - b. 使用 ASA 映像升级 **辅助** ASA 逻辑设备。有关说明，请参阅《*思科 Firepower 机箱管理器配置指南*》中的“更新逻辑设备的映像版本”主题（请参阅[相关文档（第 13 页）](#)）。
 - c. 等待直至升级过程完成。使用 **scope ssa** 下的 **show app-instance** 命令来验证 ASA 应用已恢复“在线”状态。
6. 重新启用故障切换：
 - a. 连接到包含 **主** ASA 逻辑设备的 Firepower 安全设备上的 ASA 控制台。
 - b. 启用故障切换：
failover
 - c. 保存配置：
write memory
 - d. 验证设备是否处于活动状态：
show failover
7. 将刚才升级的设备设为 **活动**设备，以使流量流向已升级的设备：
 - a. 连接到包含 **辅助** ASA 逻辑设备的 Firepower 安全设备上的 ASA 控制台。
 - b. 启用故障切换并激活：
failover
failover active
 - c. 保存配置：
write memory
 - d. 验证设备是否处于 **活动**状态：
show failover

8. 再次禁用故障切换:
 - a. 连接到包含 **辅助** ASA 逻辑设备（当前是 **活动** 设备）的 Firepower 安全设备上的 ASA 控制台。
 - b. 禁用故障切换:
no failover
 - c. 在包含 **主** ASA 逻辑设备的 Firepower 安全设备和包含 **辅助** ASA 逻辑设备的 Firepower 安全设备上保存配置:
write memory
9. 升级包含 **主** ASA 逻辑设备的 Firepower 安全设备上的 Firepower 可扩展操作系统捆绑包:
 - a. 将 FXOS 1.1(4) 平台捆绑包映像上传至 Firepower 安全设备。有关说明，请参阅《*思科 Firepower 机箱管理器配置指南*》中的“将映像上传至 Firepower 设备”主题（请参阅[相关文档（第 13 页）](#)）。

注：此时请不要上传 ASA 映像。只有当您已经使用 FXOS 1.1(4) 平台捆绑包映像成功升级机箱之后，才能上传 ASA 映像。

 - b. 使用 FXOS 1.1(4) 平台捆绑包映像升级您的 Firepower 安全设备。有关说明，请参阅《*思科 Firepower 机箱管理器配置指南*》中的“升级 Firepower 可扩展操作系统平台捆绑包”主题（请参阅[相关文档（第 13 页）](#)）。
10. 等待机箱重新启动并成功升级:
 - a. 使用 **scope system** 下的 **show firmware monitor** 命令来监控升级过程。
 - b. 升级过程完成后，使用 **scope ssa** 下的 **show app-instance** 命令来验证 ASA 应用已恢复“在线”状态。
11. 升级 **主** ASA 逻辑设备上的 ASA 软件:
 - a. 将 ASA 映像上传至 Firepower 安全设备。有关说明，请参阅《*思科 Firepower 机箱管理器配置指南*》中的“将映像上传至 Firepower 设备”主题（请参阅[相关文档（第 13 页）](#)）。
 - b. 使用 ASA 映像升级 **主** ASA 逻辑设备。有关说明，请参阅《*思科 Firepower 机箱管理器配置指南*》中的“更新逻辑设备的映像版本”主题（请参阅[相关文档（第 13 页）](#)）。
 - c. 等待直至升级过程完成。使用 **scope ssa** 下的 **show app-instance** 命令来验证 ASA 应用已恢复“在线”状态。
12. 重新启用故障切换:
 - a. 连接到包含 **辅助** ASA 逻辑设备的 Firepower 安全设备上的 ASA 控制台。
 - b. 启用故障切换:
failover
 - c. 保存配置:
write memory
 - d. 验证设备是否处于活动状态:
show failover
13. 将 **主** 设备设为 **活动** 设备:
 - a. 连接到包含 **主** ASA 逻辑设备的 Firepower 安全设备上的 ASA 控制台。
 - b. 启用故障切换并激活:
failover
failover active

- c. 保存配置：
write memory
- d. 验证设备是否处于 *活动* 状态：
show failover

升级机箱间集群

升级前检查表

1. 连接到机箱 2（应该是没有主设备的机箱）上的 FXOS CLI。有关说明，请参阅《*思科 FXOS CLI 配置指南*》或《*思科 FXOS Firepower 机箱管理器配置指南*》中的“访问 FXOS CLI”主题（请参阅[相关文档（第 13 页）](#)）。
2. 验证已安装的所有安全模块是否均处于在线状态：
scope ssa
show slot
3. 验证已安装的所有安全模块是否安装有正确的 FXOS 版本和 ASA 版本：
scope server 1/x
show version
scope ssa
show logical-device
4. 对于安装在机箱中的所有安全模块，验证集群运行状态为“集群内”：
scope ssa
show app-instance
5. 验证安装的所有安全模块显示为集群的一部分：
connect module x console
show cluster info
6. 验证主设备不在该机箱中。

程序

1. 将 FXOS 1.1(4) 映像下载到本地计算机（请参阅映像详细信息）。
2. 连接到机箱 2（应该是没有主设备的机箱）上的 FXOS CLI。有关说明，请参阅《*思科 FXOS CLI 配置指南*》或《*思科 FXOS Firepower 机箱管理器配置指南*》中的“访问 FXOS CLI”主题（请参阅[相关文档（第 13 页）](#)）。
3. 对于安装在机箱 2 中的所有安全模块，请连接到每个模块上的 ASA 控制台并禁用集群：
connect module x console
configure terminal
cluster group name
no enable
4. 升级机箱 2 中的 Firepower 可扩展操作系统捆绑包：
 - a. 将 FXOS 1.1(4) 平台捆绑包映像上传至 Firepower 安全设备。有关说明，请参阅《*思科 Firepower 机箱管理器配置指南*》中的“将映像上传至 Firepower 设备”主题（请参阅[相关文档（第 13 页）](#)）。

13. 等待机箱重新启动并成功升级（大约需要 15-20 分钟）。

使用 **scope system** 下的 **show firmware monitor** 命令来监控升级过程。每个组件应显示“升级状态：就绪” (Upgrade-Status: Ready)。

成功升级后，ASA 节点将自动重新加入现有集群。

14. 升级过程完成后：

a. 使用 **scope ssa** 下的 **show slot** 命令来确认每个插槽均处于“在线”状态。

b. 使用 **scope ssa** 下的 **show app-instance** 命令来验证 ASA 应用已恢复“在线”状态。

c. 对于安装在机箱中的所有安全模块，使用 **scope ssa** 下的 **show app-instance** 命令来验证集群运行状态为“集群内”。

15. 将 ASA 映像上传到机箱 1。有关说明，请参阅《思科 Firepower 机箱管理器配置指南》中的“将映像上传至 Firepower 设备”主题（请参阅[相关文档（第 13 页）](#)）。**16.** 对于机箱 1 中的每个安全模块：

a. 使用 ASA 映像升级 ASA 逻辑设备。有关说明，请参阅《思科 Firepower 机箱管理器配置指南》中的“更新逻辑设备的映像版本”主题（请参阅[相关文档（第 13 页）](#)）。

b. 等待直至升级过程完成。

c. 使用 **scope ssa** 下的 **show app-instance** 命令来验证 ASA 应用已恢复“在线”状态。

d. 验证每个安全模块的集群运行状态为“集群内”：

```
connect module x console
```

```
show cluster info
```

17. 如果集群中包含任何额外的机箱，请针对这些机箱重复执行步骤 10. 至 16.。

尚未解决和已解决的缺陷

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。您可通过该基于 Web 的工具访问思科漏洞跟踪系统，在上面查看此产品和其他思科硬件和软件产品存在的缺陷和漏洞。

说明：您必须使用 Cisco.com 帐户才能登录并访问思科缺陷搜索工具。如果没有，您可以[注册一个帐户](#)。

有关思科缺陷搜索工具的详细信息，请参阅[缺陷搜索工具帮助及常见问题](#)。

遗留漏洞

下表列出了有关 Firepower 可扩展操作系统 1.1(4) 的严重性为 3 及更高的遗留漏洞：

表 1 影响 FXOS 1.1(4) 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
CSCuu50615	内置机箱管理器：在内置机箱管理器上列出了不受支持的时区
CSCuv76823	EPM 上的 1G 铜缆和光纤指示灯闪烁。应保持绿色常亮
CSCuv99740	当会话内存使用量已满时，未显示错误消息
CSCuw03704	FXOS 软件显示错误的管理引擎 VID
CSCuw31077	应验证应用于接口的过滤器

表 1 影响 FXOS 1.1(4) 的遗留漏洞 (续)

标识符	描述
CSCUw37616	在附加模式下删除和添加接口时删除了接口文件
CSCUw65954	vDP: 在更改管理引导程序后, vDP 中的管理 IP 未更新
CSCUw81066	当启用超出磁盘空间的会话时, 应发出错误消息
CSCUw89854	创建超过 5 GB 或 5 GB 左右的会话时, 显示错误消息
CSCUx18974	SNMP 值被截断并且需要更新版权
CSCUx19618	SSP: “show mem” 导致在 CPU 高负载的情况下丢弃 TCP
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存在“可操作”列中显示为“未知”
CSCUx65728	从 vDP 和 APsolute Vision 中删除默认用户名/密码
CSCUx76704	在逻辑设备保存复选框下意外显示“>>”框, 并且无下拉信息
CSCUx77947	当以高速率发送数据时, Pcap 文件大小未正确更新
CSCUx85255	如果会话名称具有“port”, Pkt 捕获会话创建失败
CSCUx85969	QP: 如果 PSU 不存在, 则显示为空
CSCUx94525	在固件升级期间, 允许 FXOS 升级。
CSCUx98517	应允许从机箱管理器取消修饰 VDP 的数据端口
CSCUy00041	登录后, 无法点击 CM 中的任何选项卡
CSCUy05758	SSH: 如果外部身份验证已启用, 通过身份验证域进行本地身份验证将失败
CSCUy21573	机箱管理器: 在更新页面中的排序中断
CSCUy31784	当使用过滤器时, 映像在删除后未列出
CSCUy38586	将 40G EPM 换为 10G EPM 后, 未删除分流端口
CSCUy42650	即使未登录, 系统也会显示机箱管理器屏幕
CSCUy58732	在采用流量分流的 ASA + VDP 集群中, 数据流量延迟增加
CSCva42606	出现统计数据客户端故障

FXOS 1.1.4.140 中已解决的漏洞

下表列出了在 Firepower 可扩展操作系统 1.1.4.140 中已解决的问题:

表 2 FXOS 1.1.4.140 中已解决的漏洞

标识符	描述
CSCUy79646	SSP: UCSM 不应将具有可更正错误的刀片标记为降级
CSCva32531	增加 vNIC MTU
CSCva47313	在 FXOS 1.1.4.120 的 show l2-table 中缺少 MAC 地址
CSCva48653	FP9300 机箱重新加载, 显示原因为“内核错误”
CSCva60362	将端口 CiscoSSL 6.0 恢复到 1.1.4 版
CSCvb29020	FP9300 上的系统日志消息 %KERN-3-SYSTEM_MSG
CSCvb59511	由于服务“lldp”hap 故障, FP9300 发生意外重新加载

FXOS 1.1.4.117 中已解决的漏洞

下表列出了在 Firepower 可扩展操作系统 1.1.4.117 中已解决的问题：

表 3 FXOS 1.1.4.117 中已解决的漏洞

标识符	描述
CSCuu70441	机箱管理器应支持集群无中断升级
CSCux32873	SSP: CCL 端口通道 LACP 挂起
CSCux83883	9.6.1/QP - 在 appagent_async_client_send_thread 中回溯
CSCuy05579	在 MIO 升级/重新启动期间, 需要隐藏错误消息
CSCuy40667	QP: 机箱管理器提供未知的存储控制器可操作性
CSCuy45358	QP: 未显示安全服务器磁盘 PID/VID
CSCuy66912	Ping 不传递到外部 network.FXOS-1.1(4.85) + ASA-9.6.0.124
CSCuy70690	为 feature/snm 添加 app_id support
CSCuy79839	处理 portAG 中的 MTS_OPC_SNM_NOTIF_MSG 消息
CSCuy85449	R114: show fan-module 显示处于无法正常工作状态的风扇
CSCuy96662	QP-D: 本地磁盘驱动器状态、电源状态和链路状态未知
CSCuz01181	EC: 在 MIO 重新启动后, QP FTD 重新启动若干次
CSCuz08655	FPR 机箱管理器 “无法获取接口列表”
CSCuz28099	在机箱 2 上启动升级之后, 机箱间主设备放弃角色
CSCuz64859	电源切换和关闭实施调用 FPGA power cycle 命令
CSCuz67201	SSP: LLDP HAP 重置
CSCuz67424	机箱间: 数据端口绑定意外需要很长时间
CSCuz87408	在安全模块上对硬件和服务状态消失信息进行排序

FXOS 1.1.4.95 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缺陷, 这些缺陷在 Firepower 可扩展操作系统 1.1.4.95 中已得到解决:

表 4 FXOS 1.1.4.95 中已解决的漏洞

标识符	描述
CSCut76730	数据流分流: 在新的 CSP 安装上, 未启用分流引擎
CSCuu17780	即使用户设置为 “sha”, CLI 也允许将陷阱配置为 “priv”
CSCuu18497	即使已配置 NTP 单选按钮, 也处于未选中状态
CSCuv18505	使用 CM 创建端口通道 (分流端口成员) 时, 出现 UI 问题
CSCuv97491	消息 enic_get_flowtable_ctrl(): error enic_get_ft_ctrl failed!!
CSCuw61160	编辑集群之后, 显示 3 次警告消息
CSCuw68106	导入所有配置后, 旧用户密码可能不起作用
CSCuw82080	机箱管理器: 必须显示 “端口通道可操作” 状态
CSCuw86671	导出/导入中应包括智能许可证信息
CSCuw95062	从机箱管理器中将 ASA 降级时显示的错误消息有误
CSCux03547	SNMP MIB 对象输出已更改。
CSCux05403	9.5.2/主: 通过 SSP 进行 VPN 负载均衡会将设备显示为 SpykerD

表 4 FXOS 1.1.4.95 中已解决的漏洞（续）

标识符	描述
CSCux05661	机箱管理器：确认安全模块是指“刀片服务器”
CSCux17304	刀片“不响应”，但似乎处于运行状态
CSCux21401	禁用集群成员可能导致添加附加许可证，而不使用标准许可证
CSCux26822	如果具有授权的从属设备成为主设备，未同步其他从属设备
CSCux36990	机箱管理器间歇性地将网络模块显示为“空”
CSCux37611	在 TFTP 导出失败后，导出配置仍保持启用状态
CSCux37677	ASA 控制台响应速度缓慢
CSCux37994	在 SSP 上的“show interface”输出中未显示 VLAN 信息
CSCux44527	不应允许用户取消正在进行的导入配置
CSCux45823	对于“show fan-module detail”，PID 值在输出中显示为空
CSCux46537	导入配置在阶段 4 importWaitForSwitch 失败

相关文档

有关 Firepower 9300 安全设备和 Firepower 可扩展操作系统的更多信息，请参阅[思科 Firepower 9300 文档导航](#)。

获取文档和提交服务请求

有关获取文档、使用思科漏洞搜索工具 (BST)、提交服务请求和收集其他信息的信息，请参阅[思科产品文档更新](#)。

要将新的和经过修订的思科技术文档直接接收到桌面，可订阅[思科产品文档更新 RSS 源](#)。RSS 源是一种免费服务。

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关系。(1110R)

© 2016 年 思科系统公司。版权所有。

