



思科 FXOS 2.1(1) 版本说明

首次发布日期：2017 年 1 月 23 日

最新修订日期：2017 年 4 月 24 日

本文档包含思科 Firepower 可扩展操作系统 2.1(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：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 2.1.1.77 的新增功能（第 2 页）
 - FXOS 2.1.1.73 的新增功能（第 2 页）
 - FXOS 2.1.1.64 的新增功能（第 2 页）
- 软件下载（第 3 页）
- 重要说明（第 4 页）
- 系统要求（第 4 页）
- 升级说明（第 4 页）
 - 安装说明（第 5 页）
 - 升级运行独立 ASA 逻辑设备或 ASA 机箱内集群的 Firepower 安全设备（第 5 页）
 - 使用增强的零停机流程升级 ASA 故障切换对（第 6 页）
 - 升级 ASA 故障切换对（第 8 页）
 - 使用增强的零停机流程升级 ASA 机箱内集群（第 12 页）
 - 升级 ASA 机箱内集群（第 14 页）
- 尚未解决和已解决的缺陷（第 18 页）
 - 遗留漏洞（第 18 页）
 - FXOS 2.1.1.77 中已解决的漏洞（第 19 页）
 - FXOS 2.1.1.73 中已解决的漏洞（第 20 页）
 - FXOS 2.1.1.64 中已解决的漏洞（第 21 页）
- 相关文档（第 21 页）
- 获取文档和提交服务请求（第 21 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 2.1.1.77 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2.1.1.77 还推出了以下新功能：

- 各种问题的修复补丁（请参阅 [FXOS 2.1.1.77 中已解决的漏洞（第 19 页）](#)）。

FXOS 2.1.1.73 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2.1.1.73 还推出了以下新功能：

- 所有 Firepower 4100 和 9300 设备均支持配备了 Firepower 威胁防御的 Radware DefensePro (vDP) 服务链。
注意：FXOS 2.1.1.64 及更高版本支持配备了 Firepower 威胁防御的 Radware DefensePro (vDP)，但需要使用与 FXOS 2.1.1.73 同时发布的 Radware vDP 版本 8.10.01.17-2。有关版本兼容性的更多信息，请参阅 [思科 FXOS 兼容性 \(http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html\)](http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html)。
- 各种问题的修复补丁（请参阅 [FXOS 2.1.1.73 中已解决的漏洞（第 20 页）](#)）。

FXOS 2.1.1.64 的新增功能

思科 Firepower 可扩展操作系统2.1.1.64 推出了以下新功能：

- 用于通过 Firepower 机箱管理器或 FXOS CLI 删除 Call Home URL 的新选项。
- 现在，可以使用 Firepower 机箱管理器配置控制台身份验证。
- 现在，可以使用 Firepower 机箱管理器查看和配置 AAA 身份验证回退方法。
- 现在，FXOS 将验证系统上安装的 CSP 文件的完整性。
- 支持 Firepower 威胁防御 6.2。
- 支持 ASA 9.7(1)。
- 所有 Firepower 4100 和 9300 设备均支持配备了 Firepower 威胁防御的 Radware DefensePro (vDP) 服务链。
- Firepower 4100 系列安全设备支持 1GB FTW 网络模块。
- Firepower 9300 安全设备支持高压直流 (HVDC) 电源模块。
- 支持使用 Firepower 威胁防御 6.2 及更高版本进行机箱内集群。
- 改进了站点间的集群。

- 现在，可以使用 FXOS 机箱管理器启用 FIPS/通用标准模式，以为符合 FIPS（联邦信息处理标准）140-2 及通用标准安全认证提供支持。
- FXOS 2.1(1) 包含多项新功能以及大量增强功能，以为符合 UC-APL（统一功能获准产品清单）安全认证提供支持：
 - 通过 Firepower 机箱管理器启用/禁用 FIPS/CC 模式
 - 通过 Firepower 机箱管理器配置管理 ACL（ip 块）
 - 通过 Firepower 机箱管理器配置 SSH 服务器 - MAC 身份验证
 - 通过 Firepower 机箱管理器配置 SSH 服务器 - 加密算法
 - 登录通知
 - CRL 列表定期更新
 - 客户端证书身份验证
- 现在可以启用 NTP 服务器身份验证。
- FXOS 现在设有一个绝对超时值，达到该值即会关闭 Firepower 机箱管理器会话，而不管会话使用状况如何。该绝对超时值默认为 60 分钟，可使用 FXOS CLI 进行更改。要了解更多信息，请参阅《FXOS CLI 配置指南》。
- 现在，数据端口通道内联对的相关信息可从 Firepower 威胁防御传播到 FXOS。
- 现在，可以使用 Firepower 机箱管理器删除不属于逻辑设备的应用实例。
- 数据包捕获功能的增强：
 - 根据 IPv6 地址进行过滤。
 - 指定会话的快照长度。
 - 支持 1 MB 至 2 GB 的会话大小。以前的版本中，支持的大小为 256 MB 至 2 GB。
 - 用于删除所有数据包捕获会话的命令。
- QoS 增强功能：
 - 通过 LACP 控制 FXOS 中配置的端口通道的流量优先排序。
 - 通过修改 MIO CPU 端口队列设置，来优化内部控制平面流量的优先排序。
- ASA 故障切换对的许可发生变化。只有活动设备请求许可证授权。过去，两种设备都请求许可证授权。
- 各种问题的修复补丁（请参阅 [FXOS 2.1.1.64 中已解决的漏洞（第 21 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 FXOS 特定版本支持的应用的信息，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

- 自 ASA 9.7 开始，故障切换对的智能许可配置行为发生了变化。若要将 ASA 故障切换对从 9.6 及更早版本升级到 9.7 及更高版本，必须执行以下步骤来升级设备上的授权（活动设备为设备 A，备用设备为设备 B）：
 - a. 如果当前的备用设备（设备 B）上已配置任何授权，请在备用设备中删除该配置，改为在活动设备（设备 A）上配置相同的授权。对于上下文计数，请合并活动设备和备用设备中的值，并在活动设备上请求总数。
 - b. 升级备用设备（设备 B），然后将其重新加入故障切换对作为备用设备。此时，设备 B 上没有智能许可证配置。有关详细信息，请参阅[升级 ASA 故障切换对（第 8 页）](#)。
 - c. 升级活动设备（设备 A）。在升级期间，设备 A 将脱离故障切换对，而设备 B 将变成活动状态。当设备 A 升级时，需要在设备 B 上配置在设备 A 中配置的所有授权。
 - d. 设备 A 在完成升级后会作为备用设备重新加入故障切换对。由于设备 A 现在是备用状态，所以会释放所有授权并删除智能许可证配置。

在从设备 B（活动）向设备 A（备用）同步配置期间，设备 A 会从设备 B 接收和缓存智能许可证配置，以便在其成为活动设备后知道需要请求哪些授权。

- 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如何在需要时升级固件的说明，请参阅《[思科 FXOS CLI 配置指南，2.1\(1\)](#)》或《[思科 FXOS Firepower 机箱管理器配置指南，2.1\(1\)](#)》(<http://www.cisco.com/go/firepower9300-config>) 中的“固件升级”主题。
- 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。

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

使用 Mozilla Firefox 版本 42、Google Chrome 版本 47 和 Internet Explorer 版本 11 在 FXOS 2.1(1) 上执行测试。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 或 Firepower 4100 系列安全设备当前运行的是任何 FXOS 2.1(1) 内部版本，可以将其升级到 FXOS 2.1(1.77)。

如果您运行的是 FXOS 的早期版本，请参阅 [Firepower 9300 上的 FXOS 的升级路径](#)，了解有关如何将系统升级到 FXOS 2.1(1.77) 的信息。

Firepower 9300 上的 FXOS 的升级路径

通过下表可了解从较早版本升级到此版本所需的升级路径。有关升级到特定版本的说明，请参阅该版本的版本说明文档：

<http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html>

升级时，可能还需要升级已安装的所有逻辑设备的应用版本。请密切关注每个 FXOS 版本所支持的应用版本。有关受支持版本的详细信息，请参阅 *思科 FXOS 兼容性指南*，网址为：

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

注意：如果您当前运行的是 FXOS 1.1(4) 之前的 FXOS 版本，请参阅 *思科 FXOS 版本说明, 1.1(4)* 了解如何将系统升级至 FXOS 1.1(4)。

当前版本	升级路径			
FXOS 2.1(1.73)	→	FXOS 2.1(1.77)		
FXOS 2.1(1.64)	→	FXOS 2.1(1.77)		
FXOS 2.0(1.x)	→	FXOS 2.1(1.64)	→	FXOS 2.1(1.77)
FXOS 1.1(4.x)	→	FXOS 2.0(1.37)	→	FXOS 2.1(1.64) → FXOS 2.1(1.77)

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。

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 Firepower 安全设备（如果正在使用 Firepower 威胁防御）的说明，请参阅您希望升级到的版本的 Firepower 系统版本说明 (<http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html>)。
- 有关如何升级运行独立 ASA 逻辑设备或 ASA 机箱内集群的 Firepower 安全设备的说明，请参阅 [升级运行独立 ASA 逻辑设备或 ASA 机箱内集群的 Firepower 安全设备（第 5 页）](#)。
- 要升级配置为 ASA 故障切换对的两个 Firepower 安全设备，请执行适合您当前版本和目标版本的相应程序：
 - 有关如何从 FXOS 2.0(1.129) 或更高版本升级至 FXOS 2.1(1.64) 或从 FXOS 2.1(1.64) 或更高版本升级至 FXOS 2.1(1.77) 的说明，请参阅 [使用增强的零停机流程升级 ASA 故障切换对（第 6 页）](#)。
 - 有关如何从 FXOS 2.0(1.37)-2.0(1.86) 升级至 FXOS 2.1(1.64) 的说明，请参阅 [升级 ASA 故障切换对（第 8 页）](#)。
- 要升级配置为机箱内集群的 Firepower 安全设备，请执行适合您当前版本和目标版本的相应程序：
 - 有关如何从 FXOS 2.0(1.129) 或更高版本升级至 FXOS 2.1(1.64) 或从 FXOS 2.1(1.64) 或更高版本升级至 FXOS 2.1(1.77) 的说明，请参阅 [使用增强的零停机流程升级 ASA 机箱内集群（第 12 页）](#)。
 - 有关如何从 FXOS 2.0(1.37)-2.0(1.86) 升级至 FXOS 2.0(1.64) 的说明，请参阅 [升级 ASA 机箱内集群（第 14 页）](#)。

升级运行独立 ASA 逻辑设备或 ASA 机箱内集群的 Firepower 安全设备

执行以下步骤将系统更新到 2.1(1)：

1. 将 FXOS 2.1(1) 映像下载到本地计算机（请参阅 [软件下载](#)）。
2. 将 FXOS 2.1(1) 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 21 页）](#)）。
3. 使用 FXOS 2.1(1) 平台捆绑包映像升级 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. 将 ASA 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* 中的“将映像上传至 Firepower 设备”主题。
5. 使用 ASA CSP 映像升级所有 ASA 逻辑设备（独立设备或机箱内集群）。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。

使用增强的零停机流程升级 ASA 故障切换对

注意：只有从 FXOS 2.0(1.129) 或更高版本升级至 FXOS 2.1(1.64) 或从 FXOS 2.1(1.64) 或更高版本升级至 FXOS 2.1(1.77) 时，才支持此流程。若要从 FXOS 2.0(1.37)-2.0(1.86) 升级至 FXOS 2.1(1.64)，请参阅 [升级 ASA 故障切换对（第 8 页）](#)。

1. 将 FXOS 2.1(1) 映像下载到本地计算机（请参阅 [软件下载](#)）。
2. 升级包含 **备用** 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 2.1(1) 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 21 页）](#)）。
 - b. 使用 FXOS 2.1(1) 平台捆绑包映像升级 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。
3. 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 slot** 命令来验证插槽是否已恢复“在线”状态。
 - c. 使用 **scope ssa** 下的 **show app-instance** 命令来验证应用是否已恢复“在线”状态。
4. 升级 ASA 和 vDP 逻辑设备映像：
 - a. 将 ASA CSP 映像上传至 Firepower 安全设备。如果 Radware DefensePro (vDP) 被配置为此 ASA 应用的修饰器，并且存在可用更新，请同时上传 vDP CSP 映像。

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 21 页）](#)）。

- b. 使用 ASA CSP 映像升级逻辑设备映像：

```
top (将范围设置为模式层次结构的最顶层)
scope ssa
scope slot x (其中 x 为配置 ASA 逻辑设备所依据的插槽 ID)
scope app-instance asa
set startup-version <版本>
exit
```

- c. 如果 Radware DefensePro 被配置为此 ASA 应用的修饰器，请升级 vDP 映像：

```
scope app-instance vdp
set startup-version <版本>
exit
```

- d. 确认配置：

```
commit-buffer
```

- e. 如果 Firepower 安全设备上配置了多个故障切换对（无论是否配备 Radware DefensePro 修饰器），请使用步骤 **b-d** 升级它们。

5. 升级过程完成后，验证应用是否处于在线状态：

```
scope ssa
show app-instance
```

6. 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 **备用** ASA 逻辑设备的 Firepower 安全设备上的 ASA 控制台。

- b. 将此设备设为活动状态：

```
failover active
```

- c. 保存配置：

```
write memory
```

- d. 验证设备是否处于活动状态：

```
show failover
```

7. 升级包含 **新备用** 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 2.1(1) 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 21 页）](#)）。

- b. 使用 FXOS 2.1(1) 平台捆绑包映像升级 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。

8. 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 slot** 命令来验证插槽是否已恢复“在线”状态。

- c. 使用 **scope ssa** 下的 **show app-instance** 命令来验证应用是否已恢复“在线”状态。

9. 升级 ASA 和 vDP 逻辑设备映像：

- a. 将 ASA CSP 映像上传至 Firepower 安全设备。如果 Radware DefensePro (vDP) 被配置为此 ASA 应用的修饰器，并且存在可用更新，请同时上传 vDP CSP 映像。

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 21 页）](#)）。

- b. 使用 ASA CSP 映像升级逻辑设备映像：

```
top (将范围设置为模式层次结构的最顶层)
scope ssa
scope slot x (其中 x 为配置 ASA 逻辑设备所依据的插槽 ID)
scope app-instance asa
set startup-version <版本>
exit
```

- c. 如果 Radware DefensePro 被配置为此 ASA 应用的修饰器，请升级 vDP 映像：

```
scope app-instance vdp
set startup-version <版本>
exit
```

- d. 确认配置：
commit-buffer
 - e. 如果 Firepower 安全设备上配置了多个故障切换对（无论是否配备 Radware DefensePro 修饰器），请使用步骤 **b-d** 升级它们。
10. 升级过程完成后，验证应用是否处于在线状态：
- ```
scope ssa
show app-instance
```
11. 将刚才升级的设备设为 *活动* 设备，同升级前一样：
- a. 连接到包含 *新备用* ASA 逻辑设备的 Firepower 安全设备的 ASA 控制台。
  - b. 将此设备设为活动状态：  
**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 ASA 故障切换对

**注意：**只有从 FXOS 2.0(1.37)-2.0(1.86) 升级至 FXOS 2.1(1.64) 时，才支持此流程。若要从 FXOS 2.0(1.129) 或更高版本升级至 FXOS 2.1(1.64) 或从 FXOS 2.1(1.64) 或更高版本升级至 FXOS 2.1(1.77)，请参阅[使用增强的零停机流程升级 ASA 故障切换对（第 6 页）](#)。

1. 将 FXOS 2.1(1) 映像下载到本地计算机（请参阅[软件下载](#)）。
2. 禁用 *备用* ASA 逻辑设备上的应用：
  - a. 连接到包含 *备用* ASA 逻辑设备的 Firepower 安全设备上的 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 21 页）](#)）。
  - b. 关闭 ASA 应用：

```
scope ssa
scope slot x（其中 x 为配置 ASA 逻辑设备所依据的插槽 ID）
scope app-instance asa
disable
exit
```
  - c. 如果 Radware DefensePro 被配置为此 ASA 应用的修饰器，则将其禁用。否则，请继续执行步骤 **d**。

```
scope app-instance vdp
disable
exit
```
  - d. 确认配置：  
**commit-buffer**



- e. 验证应用是否处于离线状态 :  
**show app-instance**
- 注意：**可能需要 2-5 分钟，所有应用才会变为“离线”状态，因为 vDP 在 ASA 停止且安全模块重启后才会开始停止。如果任何停止作业失败，请重复**步骤 b-d**。
- f. 如果 Firepower 安全设备上配置了多个故障切换对（无论是否配备 Radware DefensePro 修饰器），请执行**步骤 b-e** 禁用它们并进行验证。
3. 升级包含**备用**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 2.1(1) 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 21 页）](#)）。
    - b. 使用 FXOS 2.1(1) 平台捆绑包映像升级 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 slot** 命令来验证插槽是否已恢复“在线”状态。
  5. 升级 ASA 和 vDP 逻辑设备映像：
    - a. 将 ASA CSP 映像上传至 Firepower 安全设备。如果 Radware DefensePro (vDP) 被配置为此 ASA 应用的修饰器，并且存在可用更新，请同时上传 vDP CSP 映像。  
  
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 21 页）](#)）。
    - b. 使用 ASA CSP 映像升级逻辑设备映像：  
**top**（将范围设置为模式层次结构的最顶层）  
**scope ssa**  
**scope slot x**（其中 x 为配置 ASA 逻辑设备所依据的插槽 ID）  
**scope app-instance asa**  
**set startup-version <版本>**  
**exit**
    - c. 如果 Radware DefensePro 被配置为此 ASA 应用的修饰器，请升级 vDP 映像：  
**scope app-instance vdp**  
**set startup-version <版本>**  
**exit**
    - d. 确认配置：  
**commit-buffer**
    - e. 如果 Firepower 安全设备上配置了多个故障切换对（无论是否配备 Radware DefensePro 修饰器），请使用**步骤 b-d** 升级它们。
  6. 升级过程完成后，重新启用**备用**ASA 逻辑设备上的应用：
    - 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** 命令验证应用是否已成功完成升级，且目前处于“离线”状态。

- c. 打开 ASA 应用：  

```
scope ssa
scope slot x (其中 x 为配置 ASA 逻辑设备所依据的插槽 ID)
scope app-instance asa
enable
exit
```
  - d. 如果 Radware DefensePro 被配置为此 ASA 应用的修饰器，请将其启用。否则，请继续执行步骤 e。  

```
scope app-instance vdp
enable
exit
```
  - e. 确认配置：  

```
commit-buffer
```
  - f. 验证应用是否处于在线状态：  

```
show app-instance
```
  - g. 如果 Firepower 安全设备上配置了多个故障切换对（无论是否配备 Radware DefensePro 修饰器），请执行步骤 a-f 启用它们并进行验证。
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. 连接到包含备用 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：  

```
故障切换
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. 禁用新备用 ASA 逻辑设备上的应用：
    - a. 连接到包含新备用 ASA 逻辑设备的 Firepower 安全设备上的 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 21 页））。
    - b. 关闭 ASA 应用：  

```
scope ssa
scope slot x (其中 x 为配置 ASA 逻辑设备所依据的插槽 ID)
scope app-instance asa
disable
exit
```
    - c. 如果 Radware DefensePro 被配置为此 ASA 应用的修饰器，则将其禁用。否则，请继续执行步骤 d。  

```
scope app-instance vdp
disable
exit
```

## d. 确认配置：

```
commit-buffer
```

## e. 验证应用是否处于离线状态：

```
show app-instance
```

**注意：**可能需要 2-5 分钟，所有应用才会变为“离线”状态，因为 vDP 在 ASA 停止且安全模块重启后才会开始停止。如果任何停止作业失败，请重复步骤 b-d。

## f. 如果 Firepower 安全设备上配置了多个故障切换对（无论是否配备 Radware DefensePro 修饰器），请执行步骤 b-e 禁用它们并进行验证。

9. 升级包含 **新备用** 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 2.1(1) 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 21 页）](#)）。

## b. 使用 FXOS 2.1(1) 平台捆绑包映像升级 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。

## 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 slot** 命令来验证插槽是否已恢复“在线”状态。

## 11. 升级 ASA 和 vDP 逻辑设备映像：

## a. 将 ASA CSP 映像上传至 Firepower 安全设备。如果 Radware DefensePro (vDP) 被配置为此 ASA 应用的修饰器，并且存在可用更新，请同时上传 vDP CSP 映像。

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 21 页）](#)）。

## b. 使用 ASA CSP 映像升级逻辑设备映像：

```
top（将范围设置为模式层次结构的最顶层）
scope ssa
scope slot x（其中 x 为配置 ASA 逻辑设备所依据的插槽 ID）
scope app-instance asa
set startup-version <版本>
exit
```

## c. 如果 Radware DefensePro 被配置为此 ASA 应用的修饰器，请升级 vDP 映像：

```
scope app-instance vdp
set startup-version <版本>
exit
```

## d. 确认配置：

```
commit-buffer
```

## e. 如果 Firepower 安全设备上配置了多个故障切换对（无论是否配备 Radware DefensePro 修饰器），请使用步骤 b-d 升级它们。

12. 升级过程完成后，重新启用 **新备用** ASA 逻辑设备上的应用：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** 命令验证应用是否已成功完成升级，且目前处于“离线”状态。

- c. 打开 ASA 应用 :
    - scope ssa**
    - scope slot x** (其中 x 为配置 ASA 逻辑设备所依据的插槽 ID)
    - scope app-instance asa**
    - enable**
    - exit**
  - d. 如果 Radware DefensePro 被配置为此 ASA 应用的修饰器, 请将其启用。否则, 请继续执行步骤 e。
    - scope app-instance vdp**
    - enable**
    - exit**
  - e. 确认配置 :
    - commit-buffer**
  - f. 验证应用是否处于在线状态 :
    - show app-instance**
  - g. 如果 Firepower 安全设备上配置了多个故障切换对 ( 无论是否配备 Radware DefensePro 修饰器 ), 请执行步骤 a-f 启用它们并进行验证。
13. 将刚才升级的设备设为 *活动* 设备, 同升级前一样 :
- a. 连接到包含 *新备用* ASA 逻辑设备的 Firepower 安全设备的 ASA 控制台。
  - b. 启用故障切换并激活 :
    - 故障切换**
    - failover active**
  - c. 保存配置 :
    - write memory**
  - d. 验证设备是否处于 *活动* 状态 :
    - show failover**

## 使用增强的零停机流程升级 ASA 机箱内集群

**注意：**只有从 FXOS 2.0(1.129) 或更高版本升级至 FXOS 2.1(1.64) 或从 FXOS 2.1(1.64) 或更高版本升级至 FXOS 2.1(1.77) 时, 才支持此流程。若要从 FXOS 2.0(1.37)-2.0(1.86) 升级至 FXOS 2.1(1.64), 请参阅[升级 ASA 机箱内集群 \(第 14 页\)](#)。

### 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 \(第 21 页\)](#) )。
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**

- 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
```

- 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
```

- 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
```

- 验证去设备不在该机箱中：

```
scope ssa
show app-instance
```

不应存在“集群角色”(Cluster Role) 设置为“主”的任何 ASA 实例。

## 程序

- 将 FXOS 2.1(1) 映像下载到本地计算机（请参阅[软件下载](#)）。
- 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 21 页）](#)）。
- 升级机箱 2 中的 Firepower 可扩展操作系统捆绑包：
  - 将 FXOS 2.1(1) 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 21 页）](#)）。
  - 使用 FXOS 2.1(1) 平台捆绑包映像升级 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 21 页）](#)）。
- 等待机箱重新引导并成功升级（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)。
  - 升级过程完成后，验证安装的所有安全模块是否处于在线状态：
 

```
scope ssa
show slot
```
  - 验证所有 ASA 应用当前是否处于在线状态：
 

```
scope ssa
show app-instance
```
- 升级 ASA 和 vDP 逻辑设备映像：
  - 将 ASA CSP 映像上传至 Firepower 安全设备。如果 Radware DefensePro (vDP) 被配置为此 ASA 应用的修饰器，并且存在可用更新，请同时上传 vDP CSP 映像。

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 21 页）](#)）。

- b. 使用 ASA CSP 映像升级逻辑设备映像：
 

```

top (将范围设置为模式层次结构的最顶层)
scope ssa
scope slot x (其中 x 为配置 ASA 逻辑设备所依据的插槽 ID)
scope app-instance asa
set startup-version <版本>
exit

```
- c. 如果 Radware DefensePro 被配置为此 ASA 应用的修饰器，请升级 vDP 映像：
 

```

scope app-instance vdp
set startup-version <版本>
exit

```
- d. 对于此安全设备上安装的逻辑设备的所有插槽，重复步骤 b-c。
- e. 确认配置：
 

```

commit-buffer

```
6. 升级过程完成后，验证应用是否处于在线状态：
 

```

scope ssa
show app-instance

```

验证机箱中所有 ASA 和 vDP 应用的运行状态是否为“在线”。

验证机箱中所有 ASA 和 vDP 应用的集群运行状态是否为“集群内”。

验证机箱中所有 ASA 应用的集群角色是否为“从”。
7. 将机箱 2 中的其中一个安全模块设为主：
 

```

connect module x console
configure terminal
cluster master

```

将机箱 2 上的某个安全模块设置为“主”后，机箱 1 不再包含主设备，现在即可对其进行升级。
8. 针对机箱 1 重复“升级前检查表”和步骤 1-6。
9. 如果集群中包含任何其他机箱，请针对这些机箱重复“升级前检查表”和步骤 1-6。
10. 要将“主”角色返还机箱 1，请将机箱 1 上的某个安全模块设置为“主”：
 

```

connect module x console
configure terminal
cluster master

```

## 升级 ASA 机箱内集群

**注意：**只有从 FXOS 2.0(1.37)-FXOS 2.0(1.86) 升级至 FXOS 2.1(1.64) 时，才支持此流程。若要从 FXOS 2.0(1.129) 或更高版本升级至 FXOS 2.1(1.64) 或从 FXOS 2.1(1.64) 或更高版本升级至 FXOS 2.1(1.77)，请参阅[使用增强的零停机流程升级 ASA 机箱内集群](#)（第 12 页）。

## 升级前检查表

1. 连接到机箱 2（应该没有主设备的机箱）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 21 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. 验证去设备不在该机箱中：

```
scope ssa
show app-instance
```

不应存在“集群角色”(Cluster Role) 设置为“主”的任何 ASA 实例。

## 程序

1. 将 FXOS 2.1(1) 映像下载到本地计算机（请参阅[软件下载](#)）。
2. 连接到机箱 2（应该没有主设备的机箱）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 21 页）](#)）。
3. 关闭机箱 2 上的所有应用：

- a. 关闭 ASA 应用：

```
scope ssa
scope slot x（其中 x 为配置 ASA 逻辑设备所依据的插槽 ID）
scope app-instance asa
disable
exit
```

- b. 如果 Radware DefensePro 被配置为此 ASA 应用的修饰器，则将其禁用。否则，请继续执行[步骤 c](#)。

```
scope app-instance vdp
disable
exit
```

- c. 对于此安全设备上安装的逻辑设备的所有插槽，重复[步骤 a-b](#)。

- d. 确认配置：

```
commit-buffer
```

- e. 验证应用是否处于离线状态：

```
top (将范围设置为模式层次结构的最顶层)
scope ssa
show app-instance
```

**注意：**可能需要 2-5 分钟，所有应用才会变为“离线”状态。如果任何停止作业失败，请重复步骤 a-d。

- 4. 升级机箱 2 中的 Firepower 可扩展操作系统捆绑包：

- a. 将 FXOS 2.1(1) 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 21 页）](#)）。
- b. 使用 FXOS 2.1(1) 平台捆绑包映像升级 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 21 页）](#)）。

- 5. 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)。

- 6. 升级 ASA 和 vDP 逻辑设备映像：

- a. 将 ASA CSP 映像上传至 Firepower 安全设备。如果 Radware DefensePro (vDP) 被配置为此 ASA 应用的修饰器，并且存在可用更新，请同时上传 vDP CSP 映像。

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 21 页）](#)）。

- b. 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
```

- c. 验证所有 ASA 应用当前是否处于离线状态：

```
scope ssa
show app-instance
```

- d. 使用 ASA CSP 映像升级逻辑设备映像：

```
top (将范围设置为模式层次结构的最顶层)
scope ssa
scope slot x (其中 x 为配置 ASA 逻辑设备所依据的插槽 ID)
scope app-instance asa
set startup-version <版本>
exit
```

- e. 如果 Radware DefensePro 被配置为此 ASA 应用的修饰器，请升级 vDP 映像：

```
scope app-instance vdp
set startup-version <版本>
exit
```

- f. 对于此安全设备上安装的逻辑设备的所有插槽，重复步骤 d-e。

- g. 确认配置：

```
commit-buffer
```



7. 升级过程完成后，重新启用机箱 2 上的应用：

- 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** 命令验证所有应用是否已成功完成升级，且目前处于“离线”状态。

c. 打开 ASA 应用：

```
scope ssa
scope slot x (其中 x 为配置 ASA 逻辑设备所依据的插槽 ID)
scope app-instance asa
enable
exit
```

- d. 如果 Radware DefensePro 被配置为此 ASA 应用的修饰器，请将其启用。否则，请继续执行步骤 e。

```
scope app-instance vdp
enable
exit
```

- e. 对于此安全设备上安装的逻辑设备的所有插槽，重复步骤 c-d。

f. 确认配置：

```
commit-buffer
```

成功升级并重新启用后，ASA 节点将自动重新加入现有集群。

- g. 验证应用是否处于在线状态：

```
show app-instance
```

验证机箱中所有 ASA 和 vDP 应用的运行状态是否为“在线”。

验证机箱中所有 ASA 和 vDP 应用的集群运行状态是否为“集群内”。

验证机箱中所有 ASA 应用的集群角色是否为“从”。

8. 将机箱 2 中的其中一个安全模块设为主：

```
connect module x console
configure terminal
cluster master
```

将机箱 2 上的某个安全模块设置为“主”后，机箱 1 不再包含主设备，现在即可对其进行升级。

9. 针对机箱 1 重复“升级前检查表”和步骤 1-7。

10. 如果集群中包含任何其他机箱，请针对这些机箱重复“升级前检查表”和步骤 1-7。

11. 要将“主”角色返还机箱 1，请将机箱 1 上的某个安全模块设置为“主”：

```
connect module x console
configure terminal
cluster master
```

## 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 2.1(1) 的严重性为 3 及更高的遗留漏洞：

**表 1** 影响 FXOS 2.1(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                          |
| 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             |
| CSCuw31077 | 应验证应用于接口的过滤器                            |
| 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          |
| CSCuw92801 | 正在等待 Cruz 链路。链路振荡。                      |
| 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”               |
| 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                     |
| CSCux98517 | 应允许从机箱管理器取消修饰 VDP 的数据端口                 |
| CSCuy21573 | 机箱管理器：在更新页面中的排序被打乱                      |
| CSCuy31784 | 当使用过滤器时，映像在删除后未列出                       |
| CSCuy34708 | SSP MIO - MIO 启动期间，MIO 上显示内核自旋锁         |
| CSCuy38842 | 当使用流量分流、ASA 透明 LD、HSRP/VRRP 时，出现 ARP 问题 |
| CSCuy58732 | 在采用流量分流的 ASA + VDP 集群中，数据流量延迟增加         |
| CSCuy73153 | QP 4110：P2D Beta 设备上的固定端口 1-4 不良        |
| CSCuy98317 | 如果 LD 名称包含 -，无法从 LD 软分离接口               |
| CSCuz54858 | FTW 集群：启动 fxos 升级后流量中断                  |
| CSCuz59046 | 在 MIO 重新引导期间，FTW 从旁路切换到备用需要 2-5 秒       |
| CSCuz62795 | POST 证书请求包含无效的错误消息                      |
| CSCuz69280 | MIO 至刀片服务器通信失败。无法发送心跳更新消息。              |
| CSCuz81832 | 在 CM 中执行 FTD 集群内配置期间，接口信息选项卡非常杂乱        |
| CSCuz93180 | 如果验证失败，AAA LDAP 配置不会保留信息                |
| CSCva05729 | 执行 aclmgr 时，MIO 针对 FXOS 2.0.1.24 崩溃     |

表 1 影响 FXOS 2.1(1) 的遗留漏洞

| 标识符        | 描述                                                                       |
|------------|--------------------------------------------------------------------------|
| CSCva11473 | 升级后，插槽偶尔会进入无响应状态                                                         |
| CSCva46249 | 更改引导程序设置后，有 1-2 分钟未对流量旁路。                                                |
| CSCva86402 | 电源打开期间，配备 10G 和 40G SR FTW 模块的链路伙伴中出现链路振荡                                |
| 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                                 |
| CSCvb52076 | 启动期间，配备 Watford 1G 铜缆 FTW 模块的链路伙伴中出现链路振荡                                 |
| CSCvb65011 | EntityPhysical MIB 具有机箱的 Sup 序列号                                         |
| CSCvb87967 | 逻辑设备安装失败，显示错误 SdLduProvisionLDU                                          |
| CSCvc03942 | 机箱管理器未记录不存在的用户登录失败                                                       |
| 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。 |
| CSCvc07229 | 输入的 SSH 主机密钥字符串与 ssh 用户密钥字符串不同                                           |
| CSCvc14775 | 如果从 FXOS 2.0.1.86 + ASA 9.6.2 降级至 FXOX 1.1.4.140，应用实例停滞于无响应状态            |
| CSCvc16980 | 为了确保 CSP 映像完整，FXOS 映像的验证状态最初应显示为“无”                                      |
| CSCvc19428 | FCM：无法针对重大事件创建应用端口                                                       |
| CSCvc22039 | BS/QP：snmpwalk 输出中存在差异                                                   |
| CSCvc37200 | ICC FTD - 由于 EthPM 等待 SNM 消息超时，Po 接口关闭                                   |
| CSCvc38763 | Onbox 管理器：从未在 LD 页面中终止 FCM 中的环路                                          |
| CSCvc41324 | BS：没有针对 ip 块的创建而创建审核日志                                                   |
| CSCvc44522 | 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                                            |
| CSCvc44733 | FPR 链路偶尔与特定链路伙伴发生振荡（因错误而被禁用）。                                            |
| CSCvc52435 | 数据包捕获：IPv6 数据包捕获过滤器问题                                                    |
| CSCvc53082 | 当传递 DNS 和主机名时，FTD 应用代理在 FTD configure manager add 中推送 DONTRESOLVE        |
| CSCvc53247 | 使用“show hardware-bypass-ports”命令时 FTW 状态显示错误                             |
| CSCvd05138 | 与路由模式相比，在透明模式下会更早地检测到攻击流量                                                |
| CSCvd21762 | ASA HA：对于 http CPS 流量而言，辅助备用设备连接计数和 CPU 不断增加                             |

## FXOS 2.1.1.77 中已解决的漏洞

下表列出了在 Firepower 可扩展操作系统 2.1.1.77 中已解决的问题：

表 2 FXOS 2.1.1.77 中已解决的漏洞

| 标识符        | 描述                                             |
|------------|------------------------------------------------|
| CSCuy37194 | SNM 日志文件无法正确显示时间                               |
| CSCvb83067 | 如果只有一项固件变更，FXOS 不执行固件升级                        |
| CSCvb91501 | 在交换 SFP 模块类型时，出现 SFP 校验和错误                     |
| CSCvc33064 | CISCO-FIREPOWER-MIB.MY 不包含陷阱定义                 |
| CSCvc50397 | VDP - START_FAILED、VNIC_Set_Verification_Error |
| CSCvc74558 | 平台需要加强对 cfg xml 进行写入的方式。                       |
| CSCvc74860 | Lina 上显示不同步错误消息后，SSP3RU 集群中断                   |
| CSCvc77412 | 在 FXOS 中发出 show version 时，显示错误                 |

表 2 FXOS 2.1.1.77 中已解决的漏洞

| 标识符        | 描述                                                                      |
|------------|-------------------------------------------------------------------------|
| CSCvc79927 | ROMMON、FPGA 和 EPM FPGA 升级失败                                             |
| CSCvc91000 | 删除刀片服务器的内存、磁盘、CPU 的目录相关性                                                |
| CSCvd00339 | 当使用 sstate 缓存时，ipmitool 可能安装失败                                          |
| CSCvd13036 | FXOS - 无法通过机箱管理器 GUI 注册/注销智能许可                                          |
| CSCvd13121 | SAM 相关技术支持不起作用                                                          |
| CSCvd20784 | 进行客户端证书身份验证时，机箱管理器中显示的用户名不正确                                            |
| CSCvd24987 | SNM 跟踪日志应位于 show tech-support 中                                         |
| CSCvd36898 | FXOS 可能同时向控制和数据平面分配 CPU 核心，这会导致系统不稳定                                    |
| CSCvd43857 | 在 fxos 92.2.1.1953 + ASA 98.1.1.96 下显示 svc_sam_bladeAG_log 核心           |
| CSCvd48060 | FPR 9300 机箱管理器发送消息：警告：检测到可能发生内存泄漏                                       |
| CSCvd51116 | FXOS - 无法从工作空间文件夹中删除已部分生成的文件                                            |
| CSCvd56418 | FP 9300：“显示固件监控器”(show firmware monitor) 下的刀片服务器状态仍显示为“正在升级”(Upgrading) |
| CSCvd63042 | 即使已形成集群，但集群状态和角色仍显示为“不在集群内”(Not in Cluster)                             |
| CSCvd89895 | 链路关闭/启动后，FP4100 FXOS 2.1.1.73 ecmp-groups 会间歇性地变为“del”状态                |
| CSCvd97962 | 清除 samdb 后，不会清除 IP 块                                                    |
| CSCve03445 | 从 2.0.1.144 升级至 2.1.1.76 后，默认 ip 块被删除                                   |

## FXOS 2.1.1.73 中已解决的漏洞

下表列出了在 Firepower 可扩展操作系统 2.1.1.73 中已解决的问题：

表 3 FXOS 2.1.1.73 中已解决的漏洞

| 标识符        | 描述                                                                                                                    |
|------------|-----------------------------------------------------------------------------------------------------------------------|
| CSCvc30488 | SSP MIO CLI 版权信息仍显示 2015                                                                                              |
| CSCvc59936 | 运行数据包捕获并删除 LD 后，MIO appAG 崩溃                                                                                          |
| CSCvc88408 | 无法在 FST 读取 SSD 信息                                                                                                     |
| CSCvc91208 | 删除因 DIMM 不在目录而导致管理器生成的错误                                                                                              |
| CSCvc98489 | 无法使用运行 2.0.1.136 的机箱管理器查找 9.6.1 ASA 应用                                                                                |
| CSCvc98499 | 从 1.1.4.95 升级至 2.0.1.136 后，ASA 应用实例不会恢复在线状态                                                                           |
| CSCvc98978 | BS SSD“可操作性”(Operability) 显示为“不适用”(N/A)，“驱动器状态”(Drive State)、“电源状态”(Power State) 及“链路速度”(Link Speed) 显示为“未知”(Unknown) |

## FXOS 2.1.1.64 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 2.1.1.64 中已得到解决：

**表 4** FXOS 2.1.1.64 中已解决的漏洞

| 标识符        | 描述                                                            |
|------------|---------------------------------------------------------------|
| CSCuw03704 | FXOS 软件显示错误的管理引擎 VID                                          |
| 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                                |
| CSCux18974 | SNMP 值被截断并且需要更新版权                                             |
| CSCux85255 | 如果会话名称具有“port”，Pkt 捕获会话创建失败                                   |
| CSCux94525 | 在固件升级期间，允许 FXOS 升级。                                           |
| CSCuy42650 | 即使未登录，系统也会显示机箱管理器屏幕                                           |
| CSCuz39085 | 无法将 LD 中的管理端口从 Portchannel 改为管理接口 4 FTD                       |
| CSCuz41682 | CM 导出：如果存在计划，无法按需创建所需的消息                                      |
| CSCuz41747 | Onbox 管理器：禁用 scp/ftp/sftp 需要使用添加导出时的密码                        |
| CSCuz60358 | 机箱管理器默认设置拒绝远程用户的访问                                            |
| CSCuz87408 | 在安全模块上对硬件和服务状态消失信息进行排序                                        |
| CSCuz92172 | 当会话内存用完时，显示的错误消息不正确                                           |
| CSCuz99352 | 无法对界面中的任何列排序                                                  |
| CSCva02605 | SSP：交换机 CDP 相邻列表中显示端口通道成员                                     |
| CSCva09907 | 应用启动故障不应停止刀片服务器上的 FXOS 服务                                     |
| CSCva62672 | FxOS：机箱管理器接受使用特殊字符作为注册码                                       |
| CSCva91923 | FTW 端口上的机箱内集群流量中断了 110 秒                                      |
| CSCva98245 | 9300/4100 上的 ASA“show inventory”命令应更加具体                       |
| CSCvb16766 | 使用外部身份验证上传映像时，发生 500 内部服务器错误                                  |
| CSCvb33687 | FxOS：为 FC GUI“安全引擎”(Security Engine) 选项卡中的红色按钮添加工具提示，以指示关闭的对象 |
| CSCvc54102 | 由于节点重新引导后发送邀请的主节点的校验和无效，节点已离开集群                               |

## 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](http://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)

© 2017 年Cisco Systems, Inc. 保留所有权利。