升级到版本 6.4.0

本章提供版本 6.4.0的关键和版本特定信息。

您还应该参阅特性和功能，了解有关任何新特性和功能、弃用的功能和平台、菜单和术语更改、列入黑名单的 FlexConfig 命令等的信息。

指引和警告： 版本 6.4.0

此核对表中包含为版本 6.4.0新增的重要升级指引和警告。您还应查看以前发布的指引和警告， 第 3 页和一般指引和警告， 第 11 页。

表 *1:* 版本 *6.4.0* 新指引

	指南	平台	升级自	直接至
	Firepower 1010 设备上的 Etherchannel 可以将出口流量引入黑洞， 第 2 页	Firepower 1010	6.4.0	6.4.0.3 至 6.4.0.5
	升级失败：容器实例上的磁盘空间不足， 第 2 页	Firepower 4100/9300	6.3.0 至 6.4.0.x	6.3.0.1 至6.5。0
	升级失败：版本 6.2.3.12 之前的 NGIPS 设备， 第 2 页	Firepower 7000/8000 系列 ASA FirePOWER NGIPSv	6.2.3 至 6.3.0.x	仅 6.4.0

	指南	平台	升级自	直接至
	TLS 加密加速已启用/不能禁用，第 3 页	Firepower 2100 系列 Firepower 4100/9300	6.1.0 至 6.3.0.x	6.4.0+
	Firepower 4100/9300 需要版本 6.2.0 以进行升级，第 3 页	Firepower 4100/9300	6.1.0.x	仅 6.4.0

Firepower 1010 设备上的 Etherchannel 可以将出口流量引入黑洞

部署：使用 FTD 的 Firepower 1010

受影响的版本：版本 6.4.0 至 6.4.0.5

相关漏洞： CSCvq81354

我们强烈建议您不要在运行 FTD version 6.4.0 to version 6.4.0.5 的 Firepower 1010 设备上配置 etherchannel。（请注意，此型号不支持版本 6.4.0.1 和 6.4.0.2。）

由于内部流量散列问题，Firepower 1010 设备上的某些 Etherchannel 可能会将某些出口流量引入黑洞。散列计算基于源/目标 IP 地址，因此对于给定的源/目标 IP 而言，行为将一致。也就是说，某些流量会正常工作，有些流量会一直失败。

我们将在即将推出的 6.4.0.x 补丁中修复此问题。它也已在版本 6.5.0 中修复。

升级失败：容器实例上的磁盘空间不足

部署：使用 FTD 的 Firepower 4100/9300

升级自：版本 6.3.0 至 6.4.0.x

直接到：版本 6.3.0.1 到版本 6.5.0

最常见的情况是在主要升级期间，但在修补过程中，配置了容器实例的 FTD 设备可能会在预检查阶段失败，并出现错误磁盘空间不足的警告。

如果发生这种情况，您可以尝试释放更多的磁盘空间。如果不起作用，请联系思科 TAC。

升级失败：版本 6.2.3.12 之前的 NGIPS 设备

部署：7000/8000 系列、ASA FirePOWER 和 NGIPSv

相关漏洞：CSCvp42398

升级自：版本 6.2.3 至 6.3.0.x

直接至：仅版本 6.4.0

以下情况不能将 NGIPS 设备升级到版本 6.4.0：

- 设备之前运行版本 6.2.3.12，然后
- 您卸载了版本 6.2.3.12 的修补程序，或者已升级到版本 6.3.0.x。

  这也包括您卸载版本 6.2.3.12 的修补程序并升级到版本 6.3.0.x 的情况。

如果这是您目前的情况，请联系思科 TAC。

TLS 加密加速已启用/不能禁用

部署：Firepower 2100 系列、Firepower 4100/9300 机箱

升级自：版本 6.1.0 至 6.3.x

直接至：版本 6.4.0+

SSL 硬件加速已重命名为 *TLS* 加密加速。

根据设备的不同，TLS 加密加速可以在软件或硬件中执行。升级会自动在所有符合条件的设备上启用加速，即使先前已手动禁用该功能也不例外。在大多数情况下，您无法配置此功能；它会自动启用，您无法禁用它。

升级到版本 *6.4.0*： 如果您使用的是 Firepower 4100/9300 机箱的多实例功能，则可以使用 FXOS CLI 为每个模块/安全引擎的一个容器实例启用 TLS 加密加速。加速对其他容器实例禁用，但对本地实例启用。

升级到版本 *6.5.0*+： 如果您使用的是 Firepower 4100/9300 机箱的多实例功能，可以使用 FXOS CLI 为 Firepower 4100/9300 机箱上的多个容器实例（最多16个）启用 TLS 加密加速。新实例默认启用此功能。但是，升级不会在现有实例上启用加速。相反，使用 **config hwCrypto enable** CLI 命令。

Firepower 4100/9300 需要版本 6.2.0 以进行升级

部署：使用 FTD 的 Firepower 4100/9300

升级自：版本 6.1.x

直接至：仅版本 6.4.0

与其他 FMC 管理的设备不同，您无法在 Firepower 4100/9300 系列设备上直接将 Firepower 威胁防御软件从版本 6.1 升级到 6.4。这是因为 FXOS 2.6.1 与 FTD 版本 6.1 不兼容，但对版本 6.4 而言必要。

我们建议将 FXOS 2.3.1 上的版本 6.2.3 作为中间版本，并记住先升级 FXOS。不要将版本 6.3 用作中间版本；请参阅 Firepower 发行说明（版本 6.3.0）中的指导原则和警告。

以前发布的指引和警告

如果升级路径跳过主版本，请查看此核对表。您可以从多个之前的主版本升级到版本 6.4.0；请参阅要升级的最低版本，第 13 页。

表 *2:* 版本 *6.4.0* 以前发布的指引

	指南	平台	升级自	直接至
	URL 过滤缓存的超时可能会更改，第 5 页	任意	6.2.3.x	6.3.0+
	对 FMC、7000/8000 系列、NGIPSv 的准备情况检查可能失败，第 5 页	FMC Firepower 7000/8000 系列 NGIPSv	6.1.0 至 6.1.0.6 6.2.0 至 6.2.0.6 6.2.1 6.2.2 至 6.2.2.4 6.2.3 至 6.2.3.4	6.3.0+
	RA VPN 默认设置更改可以封锁 VPN 流量，第 6 页	使用 FMC 的 FTD	6.2.0 至 6.2.3.x	6.3.0+
	FMC 1000/2500/4500 可能需要预升级修复程序，第 6 页	MC1000、2500 和 4500	6.2.0 至 6.2.3.7	6.3.0+
	更新了设备访问的安全性，第 7 页	任意	6.1.0 至 6.2.3.x	6.3.0+
	安全情报启用应用程序识别，第 7 页	FMC 部署	6.1.0 至 6.2.3.x	6.3.0+
	升级后更新 VDB 以启用 CIP 检测，第 8 页	任意	6.1.0 至 6.2.3.x	6.3.0+
	无效的入侵变量集可能导致部署失败，第 8 页	任意	6.1.0 至 6.2.3.x	6.3.0+
	连接和入侵事件的系统日志行为更改，第 8 页	FMC	6.1.0 至 6.2.3.x	6.3.0+
	升级可以从 CSSM 取消 FTD/FDM 的注册，第 9 页	使用 FDM 的 FTD	6.2.0 至 6.2.2.x	6.2.3 至 6.4.0
	报告中对结果限制的更改，第 9 页	FMC	6.1.0 至 6.2.2.x	6.2.3 至 6.4.0
	升级前从版本 6.1.x FTD群集删除站点 ID，第 10 页	FTD 群集	6.1.0.x	6.2.3 至 6.4.0
	升级失败：6.2.0 版本 ASA 5500-X 系列上的 FDM，第 10 页	使用 FDM 的 FTD	仅 6.2.0	6.2.2 至 6.4.0
	访问控制可以从 SRU 获取基于延迟的性能设置，第 10 页	FMC	6.1.0.x	6.2.0 至 6.4.0

	指南	平台	升级自	直接至
	FTD 上“Snort 故障时自动打开”取代了“故障保护” ，第 11 页	使用 FMC 的 FTD	6.1.0.x	6.2.0 至 6.4.0

URL 过滤缓存的超时可能会更改

部署：任意

升级自：版本 6.2.3.x

直接至：版本 6.3.0+

版本 6.3.0 新功能 - 您可以通过 GUI 为 URL 过滤缓存配置超时值。要尽量减少与过时数据匹配的 URL 实例，可以将缓存中的 URL 设置为过期。如果您与思科 TAC 合作为 URL 过滤缓存指定超时值，则升级可能会更改该值。

升级完成后：

- FMC：选择 **System** > **Integration**，单击 Cisco CSI 选项卡，评估 **Cached URLs Expire** 设置。
- FDM：选择 **System Settings** > **Traffic Settings** > **URL Filtering Preferences**，评估 **URL Time to Live** 设置。

对 FMC、7000/8000 系列、NGIPSv 的准备情况检查可能失败

部署：FMC、7000/8000 系列设备、NGIPSv

升级自：版本 6.1.0 至 6.1.0.6、版本 6.2.0 至 6.2.0.6、版本 6.2.1、版本 6.2.2 至 6.2.2.4，以及版本 6.2.3 至 6.2.3.4

直接至：版本 6.3.0+

如果是从上方列出的任一Firepower版本升级，无法对列出的型号运行准备情况检查。发生这种情况的原因是，准备情况检查过程与较新的升级包不兼容。

表 *3:* 适用于版本 *6.3.0+* 的含准备情况检查的修补程序

不支持准备情况检查	含补丁的第一个修补程序
6.1.0 至 6.1.0.6	6.1.0.7
6.2.0 至 6.2.0.6	6.2.0.7
6.2.1	无。升级至版本 6.2.3.5+。
6.2.2 至 6.2.2.4	6.2.2.5
6.2.3 至 6.2.3.4	6.2.3.5

RA VPN 默认设置更改可以封锁 VPN 流量

部署： Firepower 威胁防御为远程访问 VPN 配置

升级自：版本 6.2.x

直接至：版本 6.3+

版本 6.3 更改了隐藏选项的默认设置，**sysopt connection permit-vpn**。升级可能导致远程访问 VPN 停止传送流量。如果发生这种情况，请采用以下任一方法：

- 创建配置 **sysopt connection permit-vpn** 命令的 FlexConfig 对象。此命令的新默认值是 **no sysopt connection permit-vpn**。

  外部用户无法在远程接入 VPN 地址池中伪造 IP 地址，因此这种允许 VPN 流量的方法较为安全。但它的缺点是，VPN 流量得不到检测，也就是说不会对流量应用入侵和文件保护、URL 过滤或其他高级功能。

- 创建访问控制规则以允许来自远程接入 VPN 地址池的连接。

  此方法可确保对 VPN 流量进行检测，并将高级服务应用于连接。但它的缺点是，有可能造成外部用户伪造 IP 地址，进而获得访问内部网络的权限。

FMC 1000/2500/4500 可能需要预升级修复程序

部署： Firepower 管理中心型号 FMC 1000、2500 和 4500

升级自：版本 6.2.0 至 6.2.3.7

直接至：版本 6.3.0+

在将 FMC1000、MC2500 或 MC4500 从版本 6.2.0 到 6.2.3.7 升级到版本 6.3.0+ 之前，必须应用预安装修复程序。或者，您也可以升级到版本 6.2.3.8+。请勿将此修复程序应用于其他 FMC 型号或版本。

此修复程序（或补丁）将 RAID 控制器的固件更新为 24.12.1-0411 版本。如果没有更新固件，则运行版本 6.3.0+ 的受影响的升级版 FMC 可能会遇到性能问题。

注释 在某些情况下，即使您运行的是受影响的版本，您的固件也可能已是最新的。在这种情况下，修复程序失败，显示错误：映像文件的版本比控制器上的版本低。控制器未刷新。如果您看到此消息，则无需此修复程序即可安全地进行升级。

要在应用修复程序之前仔细检查固件版本，请访问 FMC 上的 Linux shell（也称为专家模式）并运行以下命令：**`sudo storcli/c0 show | Grep "FW version"`**。

此修复程序可从思科支持和下载站点获取，与您主要版本的升级和安装包在同一位置。通过常规升级页面 (**System** > **Updates**) 应用热补丁。

表 *4:* 预安装热补丁包

当前版本	修复程序	数据包
6.3.0+	—	如果您在没有安装修复程序或补丁的情况下升级到 6.3.0+，请联系思科 TAC。
6.2.3.8 或更高版本补丁	—	正常升级。无需任何修复程序。
6.2.3 至 6.2.3.7	热补丁 AJ	Sourcefire_3D_Defense_Center_S3_Hotfix_AJ-6.2.3.999-5.sh.REL.tar
6.2.2.x	热补丁 BY	Sourcefire_3D_Defense_Center_S3_Hotfix_BY-6.2.2.999-1.sh.REL.tar
6.2.1	-	升级到版本 6.2.3 并对 6.2.3.8+ 应用修复程序 AJ 或补丁。
6.2.0.x	—	升级到版本 6.2.3 并对 6.2.3.8+ 应用修复程序 AJ 或补丁。

更新了设备访问的安全性

部署：任意

升级自：版本 6.1 至 6.2.3.x

直接至：版本 6.3+

为提高安全性，在版本 6.3 中，我们更新了支持的密码和加密算法列表，以实现安全的 SSH 访问。如果由于密码错误导致 SSH 客户端无法与 Firepower 设备连接，请将客户端更新到最新版本。

安全情报启用应用程序识别

部署：Firepower 管理中心

升级自：版本 6.1 至 6.2.3.x

直接至：版本 6.3+

在版本 6.3 中，安全情报配置支持应用程序检测和识别。如果在当前部署中禁用了发现，升级进程可能会再次启用它。在不需要的情况下禁用发现（例如，在仅限 IPS 的部署中）可以提高性能。

要禁用发现，您必须：

- 从网络发现策略中删除所有规则。
- 仅使用简单的、基于网络的条件执行访问控制：区域、IP 地址、VLAN 标记和端口。不要执行任何类型的应用程序、用户、URL 或地理位置控制。
- （**全新**）通过从访问控制策略的安全情报配置中删除所有白名单和黑名单（包括默认全局名单）来禁用基于网络和 URL 的安全情报。
- （**全新**）通过删除或禁用关联的 DNS 策略中的所有规则（包括 DNS 的默认全局白名单和 DNS 规则的全局黑名单）来禁用基于 DNS 的安全情报。

升级后更新 VDB 以启用 CIP 检测

部署：任意

升级自：版本 6.1.0 至 6.2.3.x，使用 VDB 299+

直接至：版本 6.3.0+

如果在使用漏洞数据库 (VDB) 299 或更高版本时升级，则升级过程会出现问题，使得您在升级后无法使用 CIP 检测。这包括从 2018 年 6 月到现在发布的每个 VDB，甚至是最新的 VDB。

尽管我们一直建议您在升级后将漏洞数据库 (VDB) 更新到最新版本，但这一做法在这种情况下尤为重要。

要检查您是否受到此问题的影响，请尝试使用基于 CIP 的应用程序条件配置访问控制规则。如果在规则编辑器中找不到任何 CIP 应用程序，请手动更新 VDB。

无效的入侵变量集可能导致部署失败

部署：任意

升级自：版本 6.1 至 6.2.3.x

直接至：版本 6.3.0+

对于入侵变量集中的网络变量，排除的任何 IP 地址必须为包含的 IP 地址的子集。此表显示了有效和无效配置的示例。

生效	无效
包含：10.0.0.0/8 排除：10.1.0.0/16	包含：10.1.0.0/16 排除：172.16.0.0/12 排除：10.0.0.0/8

在版本 6.3.0 之前，您可以使用此类无效配置成功保存网络变量。现在，这些配置会阻止部署并显示错误：变量集有无效的排除值。

如果发生这种情况，识别并编辑错误配置的变量集，然后重新部署。请注意，您可能必须编辑变量集引用的网络对象和组。

连接和入侵事件的系统日志行为更改

部署：Firepower 管理中心

升级自：版本 6.1.0 至 6.2.3.x

直接至：版本 6.3.0+

版本 6.3.0 更改并集中了系统通过系统日志记录连接和入侵事件的方式。您可以在访问控制策略中的新 Logging 选项卡上访问这些设置。

升级不会更改连接事件日志记录的现有设置。但是，您可能会突然开始通过系统日志收到预期外的入侵事件。这是因为在升级到版本 6.3.0+ 之后，入侵策略会将系统日志事件发送到新 Logging 选项卡上的目标。（在版本 6.3.0 之前，您可以在入侵策略中配置系统日志警报，以将事件发送到受管设备本身 [而非外部主机] 的系统日志。）

此外，NGIPS 设备（7000/8000 系列、ASA FirePOWER、NGIPSv）发送的消息现在使用 RFC 5425 中指定的 ISO 8601 时间戳格式。

升级可以从 CSSM 取消 FTD/FDM 的注册

部署：使用 FDM 的 FTD

升级自：版本 6.2 至 6.2.2.x

直接至：版本 6.2.3 至 6.4.0

升级 Firepower 设备管理器管理的 Firepower 威胁防御设备可能会从思科智能软件管理器取消设备的注册。升级完成后，请检查您的许可证状态。

步骤 1 单击 **设备**，然后单击 Smart License 摘要中的 **View Configuration**。

步骤 2 如果设备没有注册，单击 **Register Device**。

报告中对结果限制的更改

部署： Firepower 管理中心

升级自：版本 6.1.0 至 6.2.2.x

直接至：版本 6.2.3 至 6.4.0

版本 6.2.3 限制您可以在报告部分中使用或包括的结果数，如下所示。对于表格和详细信息视图，您可以在 PDF 报告中包括比 HTML/CSV 报告少的记录。

表 *5:* 报告中对结果的新限制

报告部分类型	最大记录数：**HTML/CSV** 报告部分	最大记录数：**PDF** 报告部分
条形图 饼图	100（顶部或底部）	100（顶部或底部）
表格视图	400,000	100,000
详细信息视图	1,000	500

如果在升级 Firepower 管理中心之前，报告模板中的某个部分指定的结果数大于 HTML/CSV 最大值，则升级进程会将该设置降至新的最大值。

对于生成PDF报告的报告模板，如果在任何模板部分中超过PDF限制，升级过程会将输出格式更改为HTML。要继续生成PDF，请将结果限制降低到PDF最大值。如果您在升级后执行此操作，则将输出格式设置回PDF。

升级前从版本 6.1.x FTD群集删除站点 ID

部署： Firepower 威胁防御群集

升级自：版本 6.1.x

直接至：版本 6.2.3 至 6.4.0

Firepower 威胁防御版本 6.1.x 群集不支持站点间群集（您可以从版本 6.2.0 开始使用 FlexConfig 配置站点间功能）。

如果在 FXOS 2.1.1 中部署或重新部署了版本 6.1.x 群集，并且输入了（不受支持的）站点 ID 值，请在升级之前删除 FXOS 中每个设备上的站点 ID（设置为 **0**）。否则，升级后设备将无法重新加入群集。

如果已经升级，请从每个设备中删除站点 ID，然后重新建立群集。要查看或更改站点 ID，请参阅《思科 FXOS CLI 配置指南》。

升级失败：6.2.0 版本 ASA 5500-X 系列上的 FDM

部署：使用 FDM 的 FTD，在内存较小的 ASA 5500-X 系列设备上运行

升级自：版本 6.2.0

直接至：版本 6.2.2 至 6.4.0

如果从版本6.2.0升级，升级可能会失败并显示一则错误消息：`Uploaded file is not a valid system upgrade file`。即使您使用的是正确的文件，也可能出现这种情况。

如果发生这种情况，您可以尝试以下解决办法：

- 请重试。
- 使用 CLI 进行升级。
- 先升级至 6.2.0.1。

访问控制可以从 SRU 获取基于延迟的性能设置

部署：FMC

升级自：6.1.x

直接至： 6.2.0+

版本 6.2.0+ 中的新访问控制策略默认从最新的入侵规则更新 (SRU) 获取其基于延迟的性能设置。此行为受 **Apply Settings From** 选项控制。要配置此选项，请编辑或创建访问控制策略，单击 **Advanced**，然后编辑基于延迟的性能设置。

升级到版本 6.2.0+ 后，系统将根据当前（版本 6.1.x）配置设置新选项。如果您的当前设置是：

- 默认：新选项设置为 **Installed Rule Update**。在升级后部署时，系统将使用最新 SRU 中基于延迟的性能设置。流量处理可能会发生变化，具体取决于最新 SRU 指定的内容。
- 自定义：新选项设置为 **Custom**。系统保留其当前的性能设置。由于此选项，行为应该不会有任何更改。

我们建议您在升级之前查看配置。在版本 6.1.x FMC Web 界面中，如前所述查看策略的基于延迟的性能设置，并查看 **Revert to Defaults** 按钮是否变暗。如果按钮变暗，表示您使用的是默认设置。如果其处于活动状态，则表示您已配置自定义设置。

FTD 上“Snort 故障时自动打开”取代了“故障保护”

部署：使用 FMC 的 FTD

升级自：版本 6.1.x

直接至：版本 6.2+

在 6.2 版本中，Snort 故障时自动打开的配置将取代 FMC 管理的 Firepower 威胁防御设备上的故障保护选项。虽然故障保护允许您在 Snort 忙碌时丢弃流量，但当 Snort 关闭时，流量会自动通过而不会接受检查。借助 Snort 故障时自动打开功能，您可以丢弃此流量。

升级 FTD 设备时，其新的 Snort 故障时自动打开设置取决于旧的故障保护设置，如下所示。虽然新配置不应更改流量处理，我们仍建议您在升级之前考虑是启用还是禁用故障保护。

表 *6:* 将故障保护迁移至 *Snort* 故障时自动打开

版本 6.1 故障保护	版本 6.2 Snort 故障时自动打开	行为
已禁用（默认行为）	**忙碌**：禁用 **关闭**：启用	新的和现有的连接在 Snort 进程繁忙时丢弃，在 Snort 进程关闭时不检查直接通过。
已启用	**忙碌**：启用 **关闭**：启用	新的和现有的连接在 Snort 进程繁忙或关闭时不检查直接通过。

请注意，Snort 故障时自动打开需要在设备上安装版本 6.2。如果您管理的是版本 6.1.x 的设备，FMC Web 界面会显示故障保护选项。

一般指引和警告

这些重要的指引和警告适用于所有升级。但这份清单并不全面。如需与升级过程相关的其他重要信息的链接，包括规划升级路径、操作系统升级、准备情况检查、备份、维护窗口等，请参阅升级说明，第 24 页。

备份事件和配置数据

我们强烈建议备份到外部位置并验证传输是否成功。在升级设备时，它会清除本地存储的备份。在 FMC 部署中，我们还建议您在升级部署后备份 FMC。这是因为您有一个新的 FMC 备份文件，它 "知道" 其设备已升级。

作为任何备份的第一步，请注意补丁级别和VDB版本。这一点很重要，因为如果您需要将备份恢复到新的或重新映像设备，则必须首先将该新设备更新为与这些版本完全相同的设备完全相同的设备。您只能从相同型号和 Firepower 版本、具有相同 VDB 的设备还原备份。

设备访问

Firepower 设备可以在升级期间或在升级失败时停止传输流量（具体取决于接口配置）。在升级 Firepower设备之前，请确保来自您所在位置的流量不必遍历设备本身即可访问设备的管理界面。在 Firepower 管理中心部署中，您还必须能够访问 FMC 管理界面而不遍历设备。

签名的升级软件包

因此，Firepower可以证实您使用的是正确的文件，来自版本 6.2.1+ 的升级包（以及到版本 6.2.1+ 的热补丁）是签名的 tar 档案 (.tar)。早期版本的升级继续使用未签名的包。

当您手动从思科支持和下载站点下载升级包时 - 例如用于重要升级或物理隔离部署 - 确保下载正确的包。 不要解压签名的 (.tar) 包。

注释 上传签名的升级包后，GUI 可能需要几分钟才能加载，因为系统需要对包进行验证。要加快显示速度，可删除不再需要的签名的包。

在 ASA FirePOWER 设备上禁用 ASA REST API

在升级 ASA FirePOWER 模块之前，确保禁用 ASA REST API。否则，升级可能会失败。从 ASA CLI：`no rest api agent`。可以在卸载后重新启用：`rest-api agent`。

与思科共享数据

一些功能包括与思科共享数据。

在 6.2.3+ 中，思科成功网络会将使用情况信息和统计信息发送到思科，这些信息对于为您提供技术支持至关重要。升级期间，系统可能会要求您接受或拒绝参与。您还可以随时选择加入或退出。

在 6.2.3+ 中，*Web* 分析跟踪会将非个人可识别使用情况数据发送到思科，包括但不限于页面交互情况、浏览器版本、产品版本、用户位置以及您的 FMC 的管理 IP 地址或主机名。如果要从版本 6.1 升级到 6.2.2.x，升级将启用 Web 分析跟踪。如果您不希望思科收集这些数据，可以在升级后选择退出。（如果是从版本 6.2.3.x或版本 6.3.0.x 升级，升级过程会考虑您当前的设置。）

在 6.5.0+ 中，思科支持诊断 （有时称为思科主动支持）将配置和运行状况数据发送到思科，并通过我们的自动化问题检测系统处理该数据，使我们能够主动通知您的问题。在TAC情况下，此功能还允许思科TAC从您的设备收集基本信息。升级期间，系统可能会要求您接受或拒绝参与。您还可以随时选择加入或退出。

升级可以导入和自动启用入侵规则

如果新的入侵规则使用您的不受当前 Firepower 版本支持的关键字，则在更新入侵规则数据库 (SRU) 时不会导入该规则。

升级 Firepower 软件并支持这些关键字后，系统将导入新的入侵规则，并且根据 IPS 配置，可以自动启用，从而开始生成事件并影响流量。

受支持的关键字取决于 Firepower 软件随附的 Snort 版本：

- FMC：依次选择**帮助 > 关于**。
- 使用 FDM 的 FTD：使用**show summary** CLI 命令。
- 使用 ASDM 的 ASA FirePOWER：选择 **ASA FirePOWER 配置 > 系统信息**。

您还可以在《Cisco Firepower 兼容性指南》的捆绑组件部分找到您的 Snort 版本。

Snort 版本说明包含有关新关键字的详细信息。您可以阅读 Snort 下载页面上的版本说明：https://www.snort.org/downloads。

无响应的升级

请勿将更改部署到正在升级的设备或从其部署更改，手动重启正在升级的设备，或者关闭正在升级的设备。请勿重启正在进行的升级。升级过程在预检查期间可能会显示为非活动；这是预期行为。如果您遇到升级问题，包括升级失败或设备无响应，请联系思科 TAC。

要升级的最低版本

您可以从多个之前的主版本序列直接升级到版本 6.4.0。不需要运行任何先前版本的最新修补程序即可升级。

表 *7:* 将 *Firepower* 软件升级到 *6.4.0* 的最低版本

平台	最低版本
Firepower 管理中心 FMC 部署中的所有受管设备（Firepower 4100/9300 系列除外）。	6.1.0

平台	最低版本
使用 FMC 的 Firepower 4100/9300 上的 Firepower 威胁防御	使用 FXOS 2.6.1.157+ 的 6.2.0（先升级 FXOS） 在 FMC 管理的 Firepower 4100/9300 系列设备上，无法将 FTD 直接从版本 6.1 升级到 6.4。我们建议将 FXOS 2.3.1 上的版本 6.2.3 作为中间版本。请参阅 Firepower 4100/9300 需要版本 6.2.0 以进行升级，第 3 页。 如果要从版本 6.2.0.x、6.2.2.0 或 6.2.2.1 升级高可用性或集群部署，并且需要无故障升级，请参阅 FTD 升级行为：Firepower 4100/9300 机箱，第 16 页。
使用 FDM 的 Firepower 威胁防御（所有平台）	6.2.0
使用 ASDM 的 ASA FirePOWER	6.2.0

时间测试和磁盘空间要求

要升级 Firepower 设备，必须具有足够的可用磁盘空间，否则升级会失败。使用 Firepower 管理中心升级受管设备时，FMC 的 /Volume 分区必须具备额外的磁盘空间来存放设备升级包。此外，您还必须具有足够的时间来执行升级。

我们提供内部时间和磁盘空间测试报告以供参考。

关于时间测试

此处给出的时间值基于内部测试。虽然我们报告的是针对特定平台/系列测试的所有升级的最慢时间，但由于多种原因（见下文），您的升级所需的时间可能比提供的时间长。

基本测试条件

- 部署：值来自于 Firepower 管理中心部署中的测试。这是因为在类似条件下，远程和本地管理设备的原始升级时间相似。
- 版本：对于主版本升级，我们测试所有先前符合条件的主版本的升级。对于修补程序，我们测试基础版本和前一个修补程序的升级。
- 型号：大多数情况下，我们测试每个系列中的最低端型号，有时会对系列中的多个型号进行测试。
- 虚拟设置：我们使用内存和资源的默认设置进行测试。

不包括推送和重新启动

值仅表示 Firepower 升级脚本本身以运行所花费的时间。值不包括将升级包上传到本地受管设备或 FMC 所需的时间，也不包括将升级包从 FMC 复制（推送）到受管设备所需的时间。

在 FMC部署中，如果 FMC与受管设备之间的带宽不足，可能会延长升级时间甚至导致升级超时。请确保您的带宽足以将大量数据从 FMC传输到其设备。有关详细信息，请参阅将数据从 Firepower 管理中心下载到受管设备的准则（故障排除技术说明）。

值也不包括重新启动、准备情况检查、操作系统升级或配置部署。

时间适用于单个设备

值是按设备提供的。在高可用性或群集配置中，设备一次升级一个可保持操作的连续性，每个设备在升级时以维护模式运行。因此，升级一对设备或整个群集所需的时间比升级独立设备所需的时间长。

请注意，堆叠的8000系列设备会同时升级，堆栈在有限的混合版本状态下运行，直到所有设备完成升级。这样做所需的时间应该不会比升级独立设备花费的时间长。

受影响的配置和数据

我们对具有最小配置和流量负载的设备进行了测试。升级时间会随着配置的复杂性、事件数据库的大小以及这些事物是否/如何受到升级的影响而增加。例如，如果您使用大量访问控制规则并且升级需要对这些规则的存储方式进行后端更改，则升级可能需要更长时间。

关于磁盘空间要求

空间估计值在为所有升级报告的值中最大，为：

- 没有四舍五入（小于 1 MB）。
- 四舍五入到下一个 1 MB (1 MB - 100 MB)。
- 四舍五入到下一个 10 MB (100 MB - 1GB)。
- 四舍五入到下一个 100 MB（大于 1 GB）。

版本 6.4.0 的时间和磁盘空间

表 *8:* 版本 *6.4.0* 的时间和磁盘空间

平台	/Volume 上的空间	/ 上的空间	FMC 上的空间	时间
FMC	13.3 GB	26 MB	-	41 分钟
FMCv：VMware 6.0	13.6 GB	29 MB	-	30 分钟
Firepower 2100 系列	12 MB	8.9 GB	950 MB	20 分钟

平台	/Volume 上的空间	/ 上的空间	FMC 上的空间	时间
Firepower 4100 系列	10 MB	7.5 GB	920 MB	6 分钟
Firepower 9300	10 MB	7.7 GB	920 MB	7 分钟
具有 ASA 5500-X 系列的 FTD	9 GB	110 KB	1.1 GB	24 分钟
FTDv：VMware 6.0	7.5 GB	100 KB	1.1 GB	12 分钟
Firepower 7000/8000 系列	7.7 GB	19 MB	980 MB	34 分钟
ASA FirePOWER	11.5 GB	22 MB	1.3 GB	66 分钟
NGIPSv：VMware 6.0	6.5 GB	19 MB	840 MB	16 分钟

流量、检查和设备行为

升级期间必须确定流量和检测中的潜在中断。以下情况下可能出现这种问题：

- 设备重新启动时。
- 在设备上升级操作系统或虚拟主机环境时。
- 在设备上升级 Firepower 软件或卸载修补程序时。
- 在升级或卸载过程中部署配置更改时（Snort 进程重新启动）。

设备类型、部署类型（独立、高可用性、群集）和接口配置（被动、IPS、防火墙等）决定了中断的性质。我们强烈建议在维护窗口或者中断对部署的影响最小时执行升级或卸载。

FTD 升级行为：Firepower 4100/9300 机箱

本部分介绍在升级含 FTD的 Firepower 4100/9300 机箱时的设备和流量行为。

Firepower 4100/9300 机箱：FXOS 升级

在每个机箱上独立升级 FXOS，即使配置了机箱间群集或高可用性对也是如此。您执行升级的方式会确定设备在 FXOS 升级期间处理流量的方式。

表 *9: FXOS* 升级期间的流量行为

部署	方法	流量行为
独立式	-	被丢弃

部署	方法	流量行为
高可用性	**最佳实践**：在备用设备上更新FXOS，切换主用对等设备，升级新的备用设备。	不受影响
	在备用设备完成升级之前，在主用对等设备上升级 FXOS。	被丢弃，直到一个对等设备处于在线状态
机箱间群集（6.2及更高版本）	**最佳实践**：一次升级一个机箱，以便至少有一个模块始终处于在线状态。	不受影响
	同时升级机箱，因此在某个时间所有模块都处于关闭状态。	被丢弃，直到至少一个模块处于在线状态
机箱内群集（仅限Firepower 9300）	已启用故障时自动绕过：**Bypass: Standby** 或 **Bypass-Force**。（6.1 及更高版本）	不检查直接通过
	已禁用故障时自动绕过：**Bypass: Disabled**。（6.1 及更高版本）	被丢弃，直到至少一个模块处于在线状态
	没有故障时自动旁路模块。	被丢弃，直到至少一个模块处于在线状态

独立式 FTD 设备：Firepower 软件升级

接口配置会确定在升级期间独立设备如何处理流量。

表 *10: Firepower* 软件升级期间的流量行为：独立式 *FTD* 设备

接口配置		流量行为
防火墙接口	路由或交换，包括 EtherChannel、冗余、子接口 切换接口也称为桥接组或透明接口。	被丢弃

接口配置		流量行为
仅限 IPS 接口	内联集，故障时自动旁路启用：**Bypass: Standby** 或 **Bypass-Force** (6.1+)	可以为以下任意一项： • 被丢弃（6.1 至 6.2.2.x） • 不检查直接通过（6.2.3 及更高版本）
	内联集，已禁用故障时自动旁路：**Bypass: Disabled** (6.1+)	被丢弃
	内联集，没有故障时自动旁路模块	被丢弃
	内联集，分流模式	立即传出数据包，不检查副本
	被动，ERSPAN 被动	不中断，不检查

高可用性对：Firepower 软件升级

在高可用性对中的设备上升级 Firepower 软件时，流量或检查中不应出现中断。为确保操作的连续性，它们一次升级一个。升级时，设备会在维护模式下运行。

首先升级备用设备。设备会交换角色，然后新的备用设备进行升级。升级完成后，设备的角色保持交换后的状态。如果您想要保留主用/备用角色，请先手动交换角色，然后再进行升级。这样，升级流程会将它们交换回来。

群集：Firepower 软件升级

在 Firepower 威胁防御群集中的设备上升级 Firepower 软件时，流量或检查中不应出现中断。为确保操作的连续性，它们一次升级一个。升级时，设备会在维护模式下运行。

首先升级一个或多个从属安全模块，然后升级主模块。升级时，安全模块在维护模式下运行。

在主安全模块升级期间，尽管流量检查和处理通常会继续，但系统会停止记录事件。升级完成后，在日志记录关闭期间处理的流量事件显示有不同步的时间戳。但是，如果日志记录关闭较长时间，则系统可能会删除最早事件，然后再记录事件。

注释 从版本 6.2.0、6.2.0.1 或 6.2.0.2 升级机箱间群集会导致从群集中删除每个模块时，流量检查中出现 2-3 秒的流量中断。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于设备处理流量的方式。

高可用性和集群无中断升级要求

执行无中断升级具有以下额外要求。

流负载分流：由于在流负载分流功能中修复了漏洞，因此 FXOS 和 FTD 的一些组合不支持流负载分流；请参阅思科 Firepower 兼容性指南。要在高可用性或集群部署中执行无中断升级，必须确保始终运行兼容的组合。

如果您的升级路径包括将 FXOS 升级到 2.2.2.91、2.3.1.130 或更高版本（包括 FXOS 2.4.1. x、2.6.1. x 等），请使用此路径：

1. 将 FTD 升级到 6.2.2.2 或更高版本。

2. 将 FXOS 升级到 2.2.2.91、2.3.1.130 或更高版本。

3. 将 FTD 升级到您的最终版本。

例如，如果您运行的是 FXOS 2.2.2.17/FTD 6.2.2.0，并且要升级到 FXOS 2.6.1/FTD 6.4.0，则可以执行以下操作：

1. 将 FTD 升级到 6.2.2.5。

2. 将 FXOS 升级到 2.6.1。

3. 将 FTD 升级到 6.4.0。

版本 6.1.0 升级：对 FTD 高可用性对执行到版本 6.1.0 升级的无中断升级需要预安装软件包。有关详细信息，请参阅Firepower 系统发行说明 6.1.0 版预安装包。

部署过程中的流量行为

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅Firepower 管理中心配置指南中的在部署或激活时重启 *Snort* 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，重启 Snort 进程会中断所有 Firepower 设备上的流量检查，包括为 HA/可伸缩性配置的检查。在中断期间，接口配置会确定是丢弃流量还是在不检查的情况下允许流量通过。

表 *11: FTD* 部署过程中的流量行为

接口配置		流量行为
防火墙接口	路由或交换，包括 EtherChannel、冗余、子接口 切换接口也称为桥接组或透明接口。	被丢弃

接口配置		流量行为
仅限 IPS 接口	内联集，已启用或禁用 **Failsafe** (6.0.1-6.1.0.x)	不检查直接通过 如果已禁用 **Failsafe**，并且 Snort 处于繁忙而非关闭状态，则系统可能会丢弃一些数据包。
	内联集，**Snort Fail Open: Down**：已禁用（6.2 及更高版本）	被丢弃
	内联集，**Snort Fail Open: Down**：启用 (6.2+)	不检查直接通过
	内联集，分流模式	立即传出数据包，不检查副本
	被动，ERSPAN 被动	不中断，不检查

FTD 升级行为：其他设备

本部分介绍在 Firepower 1000/2100 系列、ASA 5500-X 系列、 ISA 3000、和 FTDv上升级 Firepower 威胁防御时的设备和流量行为。

独立式 FTD 设备：Firepower 软件升级

接口配置会确定在升级期间独立设备如何处理流量。

表 *12: Firepower* 软件升级期间的流量行为：独立式 *FTD* 设备

接口配置		流量行为
防火墙接口	路由或交换，包括 EtherChannel、冗余、子接口 切换接口也称为桥接组或透明接口。	被丢弃
仅限 IPS 接口	内联集，故障时自动旁路启用：**Bypass: Standby** 或 **Bypass-Force** (6.1+)	可以为以下任意一项： • 被丢弃（6.1 至 6.2.2.x） • 不检查直接通过（6.2.3 及更高版本）
	内联集，已禁用故障时自动旁路：**Bypass: Disabled** (6.1+)	被丢弃
	内联集，没有故障时自动旁路模块	被丢弃
	内联集，分流模式	立即传出数据包，不检查副本
	被动，ERSPAN 被动	不中断，不检查

高可用性对：Firepower 软件升级

在高可用性对中的设备上升级 Firepower 软件时，流量或检查中不应出现中断。为确保操作的连续性，它们一次升级一个。升级时，设备会在维护模式下运行。

首先升级备用设备。设备会交换角色，然后新的备用设备进行升级。升级完成后，设备的角色保持交换后的状态。如果您想要保留主用/备用角色，请先手动交换角色，然后再进行升级。这样，升级流程会将它们交换回来。

部署过程中的流量行为

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅Firepower管理中心配置指南中的在部署或激活时重启 *Snort* 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，重启 Snort 进程会中断所有 Firepower 设备上的流量检查，包括为 HA/可伸缩性配置的检查。在中断期间，接口配置会确定是丢弃流量还是在不检查的情况下允许流量通过。

表 *13: FTD* 部署过程中的流量行为

接口配置		流量行为
防火墙接口	路由或交换，包括 EtherChannel、冗余、子接口 切换接口也称为桥接组或透明接口。	被丢弃
仅限 IPS 接口	内联集，已启用或禁用 **Failsafe** (6.0.1-6.1.0.x)	不检查直接通过 如果已禁用 **Failsafe**，并且 Snort 处于繁忙而非关闭状态，则系统可能会丢弃一些数据包。
	内联集，**Snort Fail Open: Down**：已禁用（6.2 及更高版本）	被丢弃
	内联集，**Snort Fail Open: Down**：启用 (6.2+)	不检查直接通过
	内联集，分流模式	立即传出数据包，不检查副本
	被动，ERSPAN 被动	不中断，不检查

Firepower 7000/8000 系列升级行为

以下部分介绍升级 Firepower 7000/8000 系列设备时的设备和流量行为。

独立式 7000/8000 系列：Firepower 软件升级

接口配置会确定在升级期间独立设备如何处理流量。

表 *14:* 升级时的流量行为：独立式 *7000/8000* 系列

接口配置	流量行为
内联，已启用硬件绕过 (**Bypass Mode: Bypass**)	不检查直接通过，但是流量会在以下两个时间点短暂中断： • 升级过程开始时，链路关闭并重新开启（振荡），网卡切换到硬件绕过模式。 • 升级完成后，链路再次出现振荡，网卡退出硬件绕过模式。终端重新连接并与设备接口重新建立链路后，检查会恢复。
内联，没有硬件绕过模块，或已禁用硬件绕过模式 (**Bypass Mode: Non-Bypass**)	被丢弃
内联，分流模式	立即传出数据包，不检查副本
被动	不中断，不检查
路由式、交换式	被丢弃

7000/8000 系列高可用性对：Firepower 软件升级

在高可用性对中升级设备（或设备堆叠）时，流量流或检查不应出现中断。为确保操作的连续性，它们一次升级一个。升级时，设备会在维护模式下运行。

首先升级哪一个对等设备取决于您的部署：

- 路由式或交换式：优先升级备用设备。设备会交换角色，然后新的备用设备进行升级。升级完成后，设备的角色保持交换后的状态。如果您想要保留主用/备用角色，请先手动交换角色，然后再进行升级。这样，升级流程会将它们交换回来。
- 纯访问控制：优先升级主用设备。升级完成后，主用设备和备用设备保持其原有角色。

8000 系列堆栈：Firepower 软件升级

在8000系列堆栈中，设备同时进行升级。在主设备完成其升级并且堆栈恢复操作之前，流量都会受到影响，就像堆栈是一个独立设备一样。在所有设备完成升级之前，堆栈会在一个受限的混合版本状态下运行。

部署过程中的流量行为

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅Firepower管理中心配置指南中的在部署或激活时重启 *Snort* 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，重启 Snort 进程会中断所有 Firepower 设备上的流量检查，包括为 HA/可伸缩性配置的检查。在中断期间，接口配置会确定是丢弃流量还是在不检查的情况下允许流量通过。

表 *15:* 部署期间的流量行为： *7000/8000* 系列

接口配置	流量行为
内联，**Failsafe** 已启用或已禁用	不检查直接通过 如果已禁用 **Failsafe**，并且 Snort 处于繁忙而非关闭状态，则系统可能会丢弃一些数据包。
内联，分流模式	立即传出数据包，副本绕过 Snort
被动	不中断，不检查
路由式、交换式	被丢弃

ASA FirePOWER升级行为

在 Firepower 软件升级期间（包括在您部署会导致 Snort 进程重启的某些配置时），模块处理流量的方式由用于将流量重定向到 ASA FirePOWER 模块的 ASA 服务策略决定。

表 *16: ASA FirePOWER* 升级期间的流量行为

流量重定向策略	流量行为
故障时打开 (**sfr fail-open**)	不检查直接通过
故障时关闭 (**sfr fail-close**)	被丢弃
仅监控 (**sfr {fail-close}|{fail-open} monitor-only**)	立即传出数据包，不检查副本

ASA FirePOWER部署过程中的流量行为

Snort 进程重启时的流量行为与升级 ASA FirePOWER 模块时相同。

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅Firepower管理中心配置指南中的在部署或激活时重启 *Snort* 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，重启 Snort 进程会中断流量检查。在中断期间，您的服务策略会确定是丢弃流量还是在不检查的情况下允许流量通过。

NGIPSv 升级行为

本部分介绍在升级 NGIPSv时的设备和流量行为。

Firepower 软件升级

接口配置决定了NGIPSv在升级期间如何处理流量。

表 *17: NGIPSv*升级期间的流量行为

接口配置	流量行为
内联	被丢弃
内联，分流模式	立即传出数据包，不检查副本
被动	不中断，不检查

部署过程中的流量行为

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort 通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅 Firepower 管理中心配置指南中的在部署或激活时重启 *Snort* 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，重启 Snort 进程会中断流量检查。在中断期间，接口配置会确定是丢弃流量还是在不检查的情况下允许流量通过。

表 *18: NGIPSv*部署过程中的流量行为

接口配置	流量行为
内联，**Failsafe** 已启用或已禁用	不检查直接通过 如果已禁用 **Failsafe**，并且 Snort 处于繁忙而非关闭状态，则系统可能会丢弃一些数据包。
内联，分流模式	立即传出数据包，副本绕过 Snort
被动	不中断，不检查

升级说明

发行说明中不含升级说明。读完这些发行说明中的指引和警告后，参阅以下任一资料：

- 《思科 Firepower 管理中心升级指南》：升级 FMC 部署，包括受管设备和配套的操作系统。
- 思科 ASA 升级指南：使用 ASDM 升级 ASA FirePOWER 模块
- 适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南：使用 FDM 升级 FTD。

升级程序包

思科支持和下载站点上提供了升级包。

- Firepower 管理中心，包括FMCv：https://www.cisco.com/go/firepower-software
- Firepower 威胁防御 (ISA 3000)： https://www.cisco.com/go/isa3000-software

- Firepower 威胁防御（所有其他型号，包括 FTDv）：https://www.cisco.com/go/ftd-software
- Firepower 7000 系列： https://www.cisco.com/go/7000series-software
- Firepower 8000 系列： https://www.cisco.com/go/8000series-software
- 具备 FirePOWER 服务的 ASA（ASA 5500-X 系列）： https://www.cisco.com/go/asa-firepower-sw
- 具备 FirePOWER 服务的 ASA (ISA 3000)： https://www.cisco.com/go/isa3000-software
- NGIPSv： https://www.cisco.com/go/ngipsv-software

版本 6.2.1+ 中的升级包是签名的 tar 存档 (.tar)。不要解压。

表 *19:* 从版本 *6.2.1+* 升级的升级包

平台	数据包
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Upgrade-版本-内部版本.sh.REL.tar
Firepower 2100 系列	Cisco_FTD_SSP_FP2K_Upgrade-版本-内部版本.sh.REL.tar
Firepower 4100/9300 机箱	Cisco_FTD_SSP_Upgrade-版本-内部版本.sh.REL.tar
ASA 5500-X 系列，含 FTD ISA 3000，含 FTD Firepower 威胁防御虚拟	Cisco_FTD_Upgrade-版本-内部版本.sh.REL.tar
Firepower 7000/8000 系列	Cisco_Firepower_NGIPS_Appliance_Upgrade-版本-内部版本.sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Upgrade-版本-内部版本.sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Upgrade-版本-内部版本.sh.REL.tar

表 *20:* 从版本 *6.1.x* 或 *6.2.0.x* 升级的升级包

平台	数据包
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Upgrade-版本-内部版本.sh
Firepower 4100/9300 机箱	Cisco_FTD_SSP_Upgrade-版本-内部版本.sh
ASA 5500-X 系列，含 FTD Firepower 威胁防御虚拟	Cisco_FTD_Upgrade-版本-内部版本.sh
Firepower 7000/8000 系列	Cisco_Firepower_NGIPS_Appliance_Upgrade-版本-内部版本.sh
ASA FirePOWER	Cisco_Network_Sensor_Upgrade-版本-内部版本.sh
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Upgrade-版本-内部版本.sh