SOURCEFIRE 3D 系统
版本说明

5.3 版

原始发布：2014 年 4 月 21 日
上一次更新日期：2015 年 2 月 17 日

这些版本说明适用于 Sourcefire 3D 系统的 5.3 版。即使您熟悉更新过程，也要确保完全阅读并理解这些版本说明，其中介绍了支持的平台、新增和更改的特性和功能、已知和已解决的问题，以及产品和网络浏览器兼容性。它们还包含有关以下设备的先决条件、警告以及具体安装说明的详细信息：

- 2 系列和 3 系列防御中心 （DC500 修订版 1 和 2、 DC750、 DC1000、 DC1500、 DC3000 以及 DC3500）
- 2 系列和 3 系列受管设备 （3D500、 3D1000、 3D2000、 3D2100、 3D2500、3D3500、3D4500、3D6500、7000 系列、8000 系列、3D9900、AMP7150 和 AMP8150）
- 用于 X 系列的 Sourcefire 软件
- 64 位虚拟防御中心和受管设备

提示！ 有关 Sourcefire 3D 系统的详细信息，请参阅联机帮助或者从支持站点下载《*Sourcefire 3D 系统用户指南*》。

虽然无法直接从 4.10.3.x 版更新到 5.3 版，但可从 4.10.3.x 版 （补丁 4.10.3.5 或更高版本）有限迁移到 5.2.0.x 版，然后将迁移的部署更新到 5.3 版。有关迁移的详细信息，请参阅 《*Sourcefire 3D 系统迁移指南*》。

要在 X 系列设备上安装 5.3 版用于 X 系列的 Sourcefire 软件，必须卸载任何以前版本，并且移除任何现有的 Sourcefire 软件包。有关更新信息，请参阅 《*用于 X 系列的 Sourcefire 软件安装和配置指南*》。

要将至少运行 5.2.0.4 版 Sourcefire 3D 系统的所有其他设备更新到 5.3 版，请参阅第 12 页的更新设备中概述的操作步骤。

重要！ 您**必须**更新到最新补丁才可利用最新增强功能和安全修复程序。有关详细信息，请参阅该版本的 《*Sourcefire 3D 系统版本说明*》。

有关 5.3 版更新的详细信息，请参阅以下各节：

新增及更新的特性和功能

版本说明的本节概述了在 5.3 版 Sourcefire 3D 系统中新增及更新的特性和功能。

有关详细信息，请参阅 《*Sourcefire 3D 系统用户指南*》、《*安装指南*》、《*虚拟安装指南*》和 《*用于 X 系列的 Sourcefire 软件安装和配置指南*》。

高级恶意软件防护功能

文件捕获和存储

许可证：恶意软件
支持的设备：3 系列、虚拟、X 系列
支持的防御中心：除 DC500 之外的任何防御中心

文件捕获功能可以根据文件类型或文件性质自动从网络流量中提取感兴趣的文件。捕获后的文件可存储在本地 FirePOWER 设备中，或者自动提交以使用 Sourcefire 基于云的沙盒技术、动态分析进行其他恶意软件分析。

文件捕获配置为文件策略的一部分，每个文件都进行 SHA-256 计算，以唯一标识文件并减少文件存储中的重复项。捕获的文件存储在 FirePOWER 设备的主硬盘驱动器中。

您可以手动提交捕获的文件进行动态分析，或者通过事件表视图、网络文件轨迹功能和捕获的文件表视图从 FirePOWER 设备下载它们。

动态分析、威胁分数和摘要报告

许可证：恶意软件
支持的设备：3 系列、虚拟、 X 系列
支持的防御中心：除 DC500 之外的任何防御中心

5.3 版引入了动态分析，此功能使您能够使用基于云的技术最大程度地快速识别网络中新的零日恶意行为。配置后，您可以将性质未知、以前未见过的文件提交到 Sourcefire 云，以深入分析该文件的行为。根据该行为确定威胁分数并传回防御中心。威胁分数越高，文件就越可能是恶意的。然后，您可根据威胁分数级别采取相应的措施。

Sourcefire 还提供相关的动态分析摘要报告，列出分析的详细信息以及向该文件分配相应威胁分数的原因。此附加信息可帮助您识别恶意软件和微调检测功能。

您可以将系统配置为自动捕获并发送文件进行动态分析，也可以按需提交文件进行分析。有关文件捕获功能的详细信息，请参阅第 3 页的文件捕获和存储。

自定义检测

许可证：恶意软件
支持的设备：3 系列、虚拟、 X 系列
支持的防御中心：除 DC500 之外的任何防御中心

自定义文件检测可用于识别和阻止在网络中移动的任何文件，即使是 Sourcefire 尚未识别为恶意的文件。您无需云连接即可执行这些查找，因此，自定义文件检测非常适合于处理您拥有的任何类型的私有情报数据。

如果您识别出恶意文件，可以将该文件唯一的 SHA-256 值添加到自定义文件检测列表中，以自动阻止该文件。您可以将自定义检测列表和安全列表配合使用，将特定文件标记为安全。

自定义文件检测列表与清除列表配合使用，可帮助您自定义适合具体环境的恶意软件防护方法。默认情况下，每个文件策略都包含自定义文件检测列表和清除列表，但您可以根据具体策略选择不使用任一列表或两个列表。

Spero 引擎

许可证：恶意软件
支持的设备：3 系列、虚拟、X 系列
支持的防御中心：除 DC500 之外的任何防御中心

Spero 引擎功能提供另一种基于云的方法，利用大数据检测可执行文件中可疑和潜在的新恶意软件。Spero 根据可执行文件的结构信息、引用的动态链接库 (DLL) 以及可移植可执行文件 (PE) 头中的元数据创建文件签名。然后，此功能浏览机器已知的数据树进行分析，并确定文件是否包含恶意软件。系统综合考虑 Spero 分析结果与文件性质以生成该可执行文件的最终性质。

SMB 文件检测

许可证：保护
支持的设备：因功能而异
支持的防御中心：因功能而异

从 5.3 版开始，您可以检测、检查和阻止 NetBIOS-ssn 流量中传输的文件，包括通过服务器消息块 (SMB) 传输的文件。

AMP 云连接

许可证：恶意软件、 URL 过滤
支持的防御中心：除 DC500 之外的任何防御中心

在 5.3 版之前，要连接到 Sourcefire 云，您必须使用 TCP 端口 32137 以及从防御中心到云的直接连接。

5.3 版引入了代理支持，可连接到 Sourcefire 云以执行恶意软件检测和动态分析。以前，您必须使用 TCP 端口 32137，但现在已通过 TCP 端口 443 建立默认连接，允许更多公司连接和使用 Sourcefire 的高级恶意软件情报。端口 32137 仍然可以使用，但它已经不再是默认选项。

请注意，如果从 Sourcefire 3D 系统之前的版本更新到 5.3 版，默认情况下可以使用原端口 32137。如果在更新后要通过端口 443 连接，请取消选择 Cloud Services 页面 (**System > Local > Configuration > Cloud Services**) 上相应的复选框。

下一代入侵防御 (NGIPS) 功能

主机和事件关联危害表现 (IOC) 样式

许可证：FireSIGHT + 保护 或 FireAMP 订用
支持的设备：因功能而异
支持的防御中心：因功能而异

主机和事件关联能够准确找出网络中可能受到攻击的主机。主机和事件关联汇聚入侵事件、连接事件、安全情报事件和 FireAMP 事件的数据，帮助您快速诊断和控制网络中的安全漏洞。

此功能引入 Sourcefire 提供的危害表现 (IOC) 规则，可用于控制系统是否对特定类型的攻击生成危害表现事件并将这些事件与涉及的主机关联。生成事件时，系统在受该危害表现事件影响的主机上设置一个危害表现标记。来自独立检测源的关联危害表现事件最多的主机最有可能受到攻击。一旦解决安全漏洞，危害表现标记即会移除。危害表现事件和主机标记可在主机配置文件、网络映射、 Context Explorer、控制面板和事件查看器中查看。

增强的安全情报事件存储和视图

许可证：保护
支持的设备：3 系列、虚拟、 X 系列
支持的防御中心：除 DC500 之外的任何防御中心

如果系统配置为根据安全情报数据将流量列入黑名单或者监控列入黑名单的流量，您现在可以在控制面板以及 Context Explorer 中查看安全情报数据。虽然与连接事件类似，但安全情报事件分别进行存储和删除，并拥有各自的事件视图、工作流程和自定义分析控制面板构件的预设项。

简化的入侵策略变量管理

许可证：保护
支持的设备：任意
支持的防御中心：任意

增加变量集可简化和集中对象管理器的变量管理。您可以创建自定义变量集并且自定义默认变量集，以满足您的网络环境需求。默认变量集用作主密钥，其中包含 Sourcefire 提供的默认变量和用户创建的自定义变量，可用于填充自定义变量集。自定义该集中的变量会将更改传播到包含该变量的所有其他变量集。

从 5.2 版更新到 5.3 版会自动将现有变量转移到变量集中。现有系统级变量将成为默认变量集中的自定义变量。在入侵策略级配置的自定义变量根据入侵策略分组为新的自定义变量集。

下一代防火墙 (NGFW) 功能

地理定位和访问控制

许可证：FireSIGHT
支持的设备：3 系列、虚拟
支持的防御中心：除 DC500 之外的任何防御中心

5.3 版引入了按访问控制策略中的来源或目标国家/地区过滤流量的功能。要利用地理定位过滤，请指定单个国家/地区或者引用访问控制策略规则中的地理定位对象。

地理定位对象在对象管理器中配置，代表系统在监控网络的流量中识别的一个或多个国家/地区。创建地理定位对象以保存和组织自定义国家/地区组。

URL 过滤许可证变更

许可证：保护 + URL 过滤
支持的设备：3 系列、虚拟、 X 系列
支持的防御中心：除 DC500 之外的任何防御中心

Sourcefire 不再需要控制许可证来启用 URL 过滤，而仅需要保护许可证。第一次添加 URL 过滤许可证后，防御中心自动启用 URL 过滤和自动更新。

FirePOWER 设备功能

3 系列 FirePOWER 设备中的 8300 子系列

支持的设备：3D8350、 3D8360、 3D8370、 3D8390

5.3 版引入了 3 系列 FirePOWER 受管设备中功能强大的 8300 子系列。8300 子系列支持堆叠、集群、所有现有网络模块以及现有 3 系列 8000 子系列受管设备的所有其他功能。它们的功能不断提高，以便加快连接速度：3D8350 上为 15 Gbps，3D8360 上为 30 Gbps， 3D8370 上为 45 Gbps， 3D8390 上为 60 Gbps。

专用 AMP 设备

支持的设备：AMP7150 和 AMP8150

5.3 版还引入两台新的3 系列 FirePOWER 受管设备，这些设备设计有额外的处理能力，可最大化 Sourcefire 的 AMP 功能的性能。 AMP7150 是支持小型可插拔 (SFP) 收发器的 71xx 子系列设备，搭配 32 GB 的 RAM 和 120 GB 硬盘驱动器。AMP8150 是 81xx 子系列设备，具有 96 GB 的 RAM、 2 个 CPU、 24 个内核和 400 GB 硬盘驱动器。

磁盘管理器的改进

许可证：任意
支持的设备：2 系列、 3 系列、 X 系列
支持的防御中心：2 系列、 3 系列

在 5.3 版中， Sourcefire 改进了所有设备上的磁盘空间管理和文件删除功能。这些改进支持文件捕获功能，增强了整体性能。有关详细信息，请参阅第 3 页的文件捕获和存储。

恶意软件存储包

支持的设备：8000 系列

Sourcefire 现在支持安装 Sourcefire 提供的第二个硬盘驱动器或*恶意软件存储包*，用以在本地存储捕获的文件，在主硬盘驱动器上提供可用空间来存储事件和配置。您可以将恶意软件存储包添加到任何 8000 系列受管设备 （随附额外存储设备的 AMP8150 除外）。堆叠或集群的 8000 系列设备 （AMP8150 除外）上也支持恶意软件存储包。

兼容的受管设备释放主驱动器的空间，检测是否添加了恶意软件存储包，并且自动将现有文件捕获功能转移到添加的驱动器上。有关详细信息，请参阅第 3 页的文件捕获和存储。

警告！ 请**勿**尝试安装第三方硬盘驱动器。安装不支持的硬盘驱动器可能会损坏设备。

平台支持功能

用于 X 系列的 Sourcefire 软件

支持的设备：X 系列

运行 X 系列操作系统 (XOS) 9.7.2 版 （及更高版本）和 10.0 版 （及更高版本）的 X 系列设备目前支持 5.3 版 Sourcefire 3D 系统。如果您使用的是 XOS 的早期版本，请与 Blue Coat 系统支持部门联系。有关 X 系列的详细信息，请参阅《*用于 X 系列的 Sourcefire 软件安装和配置指南*》。

虚拟设备初始设置的改进

许可证：任意
支持的设备：虚拟、 X 系列
支持的防御中心：虚拟

从 5.3 版开始，您无需退出 VCloud 工作流程即可使用 vSphere Hypervisor 或 vCloud Director 在虚拟设备上执行初始设置。在初始设置过程中，您不再需要连接到虚拟设备控制台来更改默认密码、配置网络、设置初始检测模式和配置管理防御中心。这些配置步骤现在都可以在 vCloud 部署工作流程中执行。请注意，您仍可使用 ESXi 部署，但它需要在 VMware 控制台中进行其他设置。

更改的功能

以下列表介绍对 Sourcefire 3D 系统现有功能的更改：

- 您现在可以使用基于外壳的查询管理工具来查找和停止运行时间长的查询。该查询管理工具使您可以查找并停止运行时间超过指定分钟数的查询。当您停止查询时，该工具会将事件记录到审计日志和系统日志。

  请注意，仅在防御中心上具备外壳访问权限的管理用户才可使用此工具。有关详细信息，请在防御中心外壳上键入 `query_manager -h`，或者参阅《*Sourcefire 3D 系统用户指南*》中的“停止运行时间长的查询”。
- Sourcefire 现在将网络服务器引用的流量识别为所引用连接的网络应用。例如，如果通过 advertising.com 访问的通告实际上被 CNN.com 引用，则 Sourcefire 将 CNN.com 识别为网络应用。
- 您无法再配置包含以下任何端口条件的访问控制规则：`IP 0`、`IP-ENCAP 4`、`IPv6 41`、`IPv6-ROUTE 43`、`IPv6 FRAG 44`、`GRE 47`、或 `IPv6-OPTS 60`。

  如果是从 Sourcefire 3D 系统的早期版本更新，访问控制策略规则编辑器使用警告来标记无效的规则，并且对象管理器将无效的端口对象值重置为 TCP。
- 如果您中断堆栈或集群，设备现在仍保留在主设备组中。在 5.3 版之前，系统将设备恢复到设备在加入堆栈或集群之前所属的组。
- 改进了 NetFlow 数据收集和日志记录的性能及稳定性。Sourcefire 还为启用 NetFlow 的设备所导出的连接新增了以下字段：**NetFlow Destination/Source Autonomous System**、 **NetFlow Destination/Source Prefix**、 **NetFlow Destination/Source TOS** 和 **NetFlow SNMP Input/Output**。
- 您现在可以使用 IPv6 地址创建身份验证对象。请注意，您不能使用带有 IPv6 地址的身份验证对象来验证外壳帐户。
- 您在 3 系列受管设备上创建 IPv6 快速路径规则时，现在可以识别唯一的**发起方**和**响应方** IP 地址。在 5.3 版之前，这些字段是固定的，被设置为 Any。
- 对于在 3 系列受管设备上全新安装的 5.3 版，默认启用自动应用旁路 (AAB) 功能。如果是从 Sourcefire 3D 系统旧版本进行更新， AAB 设置不受影响。请注意，仅当处理单一数据包花费了预设的时间量时， AAB 才激活。如果使用 AAB，则系统会终止所有受影响的 Snort 进程。
- 在更新到 5.3 版时，系统现在会存储您当前应用的访问控制策略以及最多 10 个已保存但尚未应用的访问控制策略修订，同时保留您的更改。
- 如果同时安排多项报告生成任务，系统将这些任务排队。您可以在 Task Status 页面 (**System > Monitoring > Task Status**) 中查看它们。
- 不可使用井号 (#) 命名安全区域对象。
- 现在可以使用 -1 作为入侵规则 `icode` 参数范围的最小值。选择 -1 作为最小值可以在范围中包括 ICMP 代码 0。
- 新增了 SMTP 预处理器告警来检测对 Cyrus SASL 身份验证的攻击。
- 系统现在包含 502 类型入侵事件的文件策略 UUID 元数据。

- 文件性质“中性”目前为“未知”。性质为“未知”的文件表示在恶意软件云分配性质之前已进行了云查找。
- 新增了多个 Snort 解码器规则来识别包含格式错误的身份验证报头的数据包。
- 您无法再根据连接摘要表的 **Ingress Interface**、 **Ingress Security Zone**、 **Egress Interface** 或 **Egress Security Zone** 字段配置自定义分析控制面板构件。
- 现在，如果您尝试安装系统上已经安装的 Sourcefire 地理定位数据库 (GeoDB) 版本，系统会发出告警。
- 您现在可以使用 **Application Protocol Category**、 **Client Category** 及 **Web Application Category** 条件创建关联规则。
- 从 5.3 版开始， LDAP 用户名区分大小写。在 5.3 版之前，用户名不区分大小写。

Sourcefire 文档的更新

在 5.3 版中，以下文档进行了更新，以反映功能的新增和更改，并解决报告的文档问题：

- *《Sourcefire 3D 系统用户指南》*
- *《Sourcefire 3D 系统联机帮助》*
- *《Sourcefire 3D 系统安装指南》*
- *《Sourcefire 3D 系统虚拟安装指南》*
- *《用于 X 系列的 Sourcefire 软件安装和配置指南》*
- *《Sourcefire 3D 系统 eStreamer 集成指南》*
- *《Sourcefire 3D 系统数据库访问指南》*
- *《Sourcefire 3D 系统恶意软件存储包指南》*
- *《Sourcefire 8000 系列设备快速入门指南》*

此外，随 5.3 版发布的 *《Sourcefire 3D 系统用户代理配置指南》*已面向 2.2 版代理进行更新。

您可以从 Sourcefire 支持站点下载所有更新的文档。

开始之前：重要更新和兼容性说明

在开始 5.3 版的更新过程之前，您应熟悉系统在更新过程中和更新后的行为，以及任何兼容性问题或更新前后需要的配置更改。

重要！ 如果配置包括自定义表，其中填充的数据来自**关联事件**表以及将 **Source IP** 选定为公共字段的**应用**表，则到 5.3 版的更新将会失败。如果配置包括此类型的自定义表，请删除该自定义表，在完成到 5.3 版的更新后重新创建该表。

警告！ Sourcefire **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

开始更新之前， Sourcefire **强烈**建议您删除或移动设备上的所有备份文件，然后将当前事件和配置数据备份到外部位置。

使用防御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 《*Sourcefire 3D 系统用户指南*》。

重要！ 防御中心清除之前更新的备份。要保留存档的备份，请将备份存储到外部。

更新期间的流量和检查

更新过程重新启动受管设备。根据设备的配置和部署方式，以下功能受到影响：

- 流量检查，包括应用感知和控制、 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，在更新集群的设备时，系统每次更新一台设备以避免流量中断。

流量检查和链路状态

在内联部署中，受管设备 （根据型号而定）可通过应用控制、用户控制、 URL 过滤、安全情报和入侵防御以及交换、路由、 NAT 和 VPN 来影响流量。在被动部署中，您可以执行入侵检测和收集发现数据，而不影响网络流量。有关设备功能的详细信息，请参阅 《*Sourcefire 3D 系统安装指南*》。

下表提供流量、检查和链路状态在更新时会受到何种影响 （取决于部署）的详细信息。请注意，无论如何配置任何内联集，在更新过程中都**不会**执行交换、路由、NAT 和 VPN。

网络流量中断

部署	网络流量已中断？
与可配置旁路内联 （为内联集启用 **Configurable bypass** 选项）	网络流量在更新过程中的两个时间点中断： • 在更新过程开始时，流量在链路下降和上升 （摆动）以及网卡切换到硬件旁路时会短暂中断。硬件旁路期间不检查流量。 • 在更新完成后，当链路摆动和网卡离开旁路时，流量会再次短暂中断。在终端重新连接并且与传感器接口重新建立链路后，将再次检查流量。 **重要！** 虚拟设备、 8000 系列设备上的非旁路网络模块或者 71xx 子系列设备上的 SFP 收发器**不**支持可配置旁路选项。
内联	网络流量在整个更新过程中被阻止。
被动	在更新过程中网络流量不会中断，但也不检查网络流量。

交换和路由

受管设备在更新过程中**不**执行交换、路由、 NAT、 VPN 或相关功能。如果已将设备配置为仅执行交换和路由，则在更新过程中会阻止网络流量。

更新过程中的审计日志记录

在更新具有网络界面的设备时， Sourcefire 3D 系统完成其更新前任务之后，简化的更新界面页面显示出来。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计日志中。

产品兼容性

您必须至少使用 5.3 版的防御中心来管理运行 5.3 版的设备。

运行 5.3 版的防御中心可以管理运行 5.2.0.4 版或更高版本的物理和虚拟设备，以及运行 5.3 版的设备。

网络浏览器兼容性

Sourcefire 3D 系统 5.3 版的网络界面经过测试，可兼容下表所列的浏览器。

网络浏览器兼容性

浏览器	需要启用的选项和设置
Chrome 30	JavaScript、 Cookie
Firefox 24	JavaScript、 Cookie、安全套接字层 (SSL) v3
Microsoft Internet Explorer 9 和 10	JavaScript、 Cookie、安全套接字层 (SSL) v3、 128 位加密、 **Active scripting** 安全设置、兼容性视图、将 **Check for newer versions of stored pages** 设置为 **Automatically**

屏幕分辨率兼容性

Sourcefire 建议选择至少 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。

恢复到前一版本

如果您因某种原因而需要将设备恢复到 Sourcefire 3D 系统的之前版本，请联系 Sourcefire 支持部门以了解详细信息。

更新设备

您**无法**将运行 4.10.x 版的 Sourcefire 3D 系统直接更新到 5.3 版，您必须重新映像物理设备，并且重新创建虚拟设备。请注意，重新映像会丢失设备上的几乎**全部**配置和事件数据。有关重新映像和重新创建设备的详细信息，请参阅 《*Sourcefire 3D 系统安装指南*》。

提示！ 如果要保留重要的配置和事件数据，可以执行从 4.10.3.x 版 （补丁 4.10.3.5 或更高版本）到 5.2.0.x 版的有限迁移，然后将迁移的部署更新到 5.3 版。有关详细信息，请参阅 《*Sourcefire 3D 系统迁移指南*》。

要在 X 系列设备上安装 5.3 版用于 X 系列的 Sourcefire 软件，必须卸载任何以前版本，并且移除任何现有的 Sourcefire 软件包。有关更新信息，请参阅 《*用于 X 系列的 Sourcefire 软件安装和配置指南*》。

要将至少运行 5.2.0.4 版 Sourcefire 3D 系统的所有其他设备更新到 5.3 版，请参阅下文概述的操作步骤。以下各节帮助您准备和安装 5.3 版更新：

- 第 13 页的计划更新
- 第 16 页的更新防御中心
- 第 18 页的更新受管设备
- 第 20 页的使用外壳执行更新

警告！ 在更新期间**不要**重新启动或关闭设备，直至看到登录提示符。系统在更新的预先检查过程中可能会看起来处于非活动状态；这是预期行为，不需要重新启动或关闭设备。

提示！ 系统可能会生成无关的 **Module Disk Usage: Frequent drain...** 运行状况告警。如果在更新到 5.3 版的过程中看到该告警，可以放心地忽略。

计划更新

开始更新之前，必须仔细阅读并理解这些版本说明，特别是第 10 页的开始之前：重要更新和兼容性说明。为确保更新过程顺利，您还必须阅读以下各节。

Sourcefire 3D 系统版本要求

要更新到 5.3 版，设备必须至少运行 5.2.0.4 版。如果运行的是早期版本，可从 Sourcefire 支持站点获取更新

防御中心必须至少运行 5.3 版才可将其受管设备更新到 5.3 版。

设备的当前版本与本发行版 （5.3 版）越接近，更新所需的时间就越少。

操作系统要求

您可以在以下托管环境中托管 64 位 Sourcefire 虚拟设备：

- VMware vSphere Hypervisor/VMware ESXi 5.0
- VMware vSphere Hypervisor/VMware ESXi 5.1
- VMware vCloud Director 5.1

有关详细信息，请参阅 《*Sourcefire 3D 系统虚拟安装指南*》。

您可以在运行 XOS 9.7.2 版和更高版本以及 10.0 版和更高版本的 X 系列设备上运行用于 X 系列的 Sourcefire 软件。有关详细信息，请参阅 《*用于 X 系列的 Sourcefire 软件安装和配置指南*》。

时间和磁盘空间方面的要求

下表提供 5.3 版更新的磁盘空间和时间指导原则。请注意，使用防御中心更新受管设备时，防御中心需要其 /Volume 分区有额外的磁盘空间。

在更新过程中的任何时候都不**要**重新开始更新或重新启动设备。 Sourcefire 提供的时间预估仅供参考，实际更新时间根据设备型号、部署和配置而有所不同。请注意，系统在更新的预先检查部分和重新启动后可能显示为非活动；这是预期行为。

提示！ 更新的重新启动部分包括数据库检查。如果在数据库中检查期间找到错误，更新需要更长时间来完成。与数据库交互的系统守护程序在数据库检查和修复期间**不会**运行。

如果遇到更新进度方面的问题，请联系 Sourcefire 支持部门。

时间和磁盘空间方面的要求

设备	/ 上的空间	/Volume 上的空间	管理器中 /Volume 上的空间	时间
2 系列防御中心	50 MB	5.5 GB	不适用	40-55 分钟
2 系列受管设备	40 MB	2.2 GB	268 MB	45-60 分钟
3 系列防御中心	150 MB	4.3 GB	不适用	50-65 分钟
3 系列受管设备	50 MB	3 GB	388 MB	30-45 分钟
3D9900 受管设备	75 MB	2 GB	388 MB	55-70 分钟
虚拟防御中心	150 MB	388 MB	不适用	硬件相关
虚拟受管设备	50 MB	3 GB	388 MB	硬件相关

配置和事件备份准则

开始更新之前， Sourcefire **强烈**建议您删除或移动设备上的所有备份文件，然后将当前事件和配置数据备份到外部位置。

您可以使用防御中心备份自身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 《*Sourcefire 3D 系统用户指南*》。

何时执行更新

由于更新过程可能影响流量检查、流量和链路状态，因此 Sourcefire **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。

安装方法

使用防御中心的网络界面执行更新。先更新防御中心，然后用它更新其管理的设备。

您**无法**将运行 4.10.x 版的 X 系列设备更新到 5.3 版。而必须先卸载旧版本，然后安装 5.3 版。有关详细说明，请参阅《*用于 X 系列的 Sourcefire 软件安装和配置指南*》。

安装顺序

必须先更新防御中心，然后才可更新其管理的设备。

在成对的防御中心上安装更新

开始更新高可用性对中的一个防御中心时，如果它尚未就绪，另一个防御中心将会变为主防御中心。此外，成对防御中心将会停止共享配置信息；成对防御中心在常规同步过程中**不会**接收软件更新。

为确保操作的连续性，请**勿**同时更新成对防御中心。先完成辅助防御中心的更新操作步骤，再更新主防御中心。

在集群设备上安装更新

在集群设备上安装更新时，系统每次对一台设备执行更新。更新开始时，系统首先将更新应用到辅助设备；此时，辅助设备会进入维护模式，当有必要的进程重新启动后，设备会再次处理流量。然后，系统将更新应用到主设备，过程与辅助设备上的更新相同。

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，设备恢复正常运行。请注意：

- 如果主设备*先于*所有辅助设备完成更新，在所有设备完成更新之前，堆栈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，堆栈在主设备完成更新后恢复正常运行。

X 系列设备

您**无法**将运行 4.10.x 版的 X 系列设备更新到 5.3 版。而必须先卸载旧版本，然后安装 5.3 版。有关详细说明，请参阅《*用于 X 系列的 Sourcefire 软件安装和配置指南*》。

安装后

在防御中心或受管设备上执行更新后，**必须**重新应用设备配置和访问控制策略。应用访问控制策略可能会造成短暂停止流量流动和处理，还可能会导致一些数据包不经检查即被传输。有关详细信息，请参阅《*Sourcefire 3D 系统用户指南*》。

您还应执行另外一些更新后步骤来确保部署正常执行。其中包括：

- 验证更新已成功
- 确保部署中的所有设备都能够成功通信
- 更新到 5.3 版的最新补丁 （如果有），以利用最新的增强功能和安全修复程序
- 按需要更新入侵规则和漏洞数据库 (VDB)

重要！ 在完成系统软件更新后，将 VDB 内部版本 156 或更高版本安装到防御中心并重新应用访问控制策略。

- 根据第 2 页的新增及更新的特性和功能中的信息进行任何必要的配置更改。

以下各节不仅包括执行更新的详细说明，而且包括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。

更新防御中心

按照本节所述的操作步骤更新防御中心，包括虚拟防御中心。对于 5.3 版更新，防御中心会重新启动。

警告！ 在更新防御中心之前，请将访问控制策略重新应用到任何受管设备。否则，对受管设备的最终更新可能会失败。

警告！ 在更新期间**不要**重新启动或关闭设备，直至看到登录提示符。系统在更新的预先检查部分可能显示为非活动；这是预期行为，不需要重新启动或关闭设备。

重要！ 将防御中心更新到 5.3 版会从设备中移除现有的卸载程序。

要更新防御中心，请执行以下操作：

1. 阅读这些版本说明并完成必要的更新前任务。

   有关详细信息，请参阅第 10 页的开始之前：重要更新和兼容性说明和第 13 页的计划更新。

2. 从 Sourcefire 支持站点下载更新：
   - 对于 2 系列防御中心：
     `Sourcefire_3D_Defense_Center_Upgrade-5.3.0-XXX.sh`
   - 对于 3 系列和虚拟防御中心：
     `Sourcefire_3D_Defense_Center_S3_Upgrade-5.3.0-XXX.sh`

重要！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。

3. 选择 **System > Updates**，然后在 **Product Updates** 选项卡中点击 **Upload Update**，将更新上传到防御中心。浏览到更新并点击 **Upload**。

   更新成功上传到防御中心。

4. 确保部署中的设备能够成功通信，并且运行状况监视器未报告任何问题。

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

   正在运行的任务会在更新开始时停止，成为失败的任务，并且不能恢复；必须在更新完成后手动将这些任务从任务队列中删除。任务队列每 10 秒钟自动刷新一次。**必须**等到所有长时间运行的任务都完成后，才能开始更新。

6. 选择 **System > Updates**。

   系统将显示 Product Updates 选项卡。

7. 点击上传的更新旁边的安装图标。

   系统将显示 Install Update 页面。

8. 选择防御中心并点击 **Install**。确认要安装更新并重新启动防御中心。

   更新过程开始。可以开始在任务队列 (**System > Monitoring > Task Status**) 中监控更新进度。但是，在防御中心完成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详细信息。

   如果出于任何原因导致更新失败，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**勿**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**勿**重新开始更新，而应联系支持部门。

   更新完成后，防御中心显示成功消息并重新启动。

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

10. 登录到防御中心。

11. 审核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。

12. 选择 **Help > About** 并确认所列软件版本是否正确：5.3.0 版。另请注意防御中心上的规则更新和 VDB 的版本；稍后需要使用这些信息。

13. 确认部署中的设备能够成功通信，并且运行状况监视器未报告任何问题。

14. 如果支持站点上的可用规则更新比防御中心上的规则新，请导入最新的规则。

    有关规则更新的详细信息，请参阅《*Sourcefire 3D 系统用户指南*》。

15. 如果支持站点上的可用 VDB 比防御中心上的 VDB 新，请安装最新的 VDB。

    安装 VDB 更新会导致短暂停止流量流动和处理，还可能会导致遗漏检查一些数据包。有关详细信息，请参阅《*Sourcefire 3D 系统用户指南*》。

16. 将设备配置重新应用到所有受管设备。

    提示！ 要重新激活灰显的 **Apply** 按钮，请在设备配置中编辑任何接口，然后点击 **Save** 而不进行更改。

17. 将访问控制策略重新应用到所有受管设备。

    警告！ 请勿单独重新应用入侵策略；必须完全重新应用所有访问控制策略。

    应用访问控制策略可能会造成短暂停止流量流动和处理，还可能会导致遗漏检查一些数据包。有关详细信息，请参阅《*Sourcefire 3D 系统用户指南*》。

18. 如果支持站点可以提供 5.3 版的补丁，请按该版本的《*Sourcefire 3D 系统版本说明*》所述应用该补丁。您**必须**更新到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

在将防御中心更新到 5.3 版后，使用它们来更新其管理的设备。

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载到管理防御中心。接着，安装软件。一次可以更新多台设备，但必须全部使用同一个更新文件。

对于 5.3 版更新，所有设备都会重新启动。受管设备在更新过程中**不**执行流量检查、交换、路由、 NAT、 VPN 或相关功能。根据设备的配置和部署，更新过程还可能影响流量和链路状态。有关详细信息，请参阅第 10 页的更新期间的流量和检查。

警告！ 在更新受管设备之前，请使用其管理防御中心将适当的访问控制策略重新应用到受管设备。否则，受管设备更新可能失败。

警告！ 在更新期间**不要**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显示为非活动；这是预期行为，不需要重新启动或关闭设备。

要更新受管设备，请执行以下操作：

1. 阅读这些版本说明并完成必要的更新前任务。

   有关详细信息，请参阅第 10 页的开始之前：重要更新和兼容性说明和第 13 页的计划更新。

2. 更新设备的管理防御中心上的 Sourcefire 软件；请参阅第 16 页的更新防御中心。

3. 从 Sourcefire 支持站点下载更新：

   - 对于 2 系列受管设备：
     `Sourcefire_3D_Device_Upgrade-5.3.0-XXX.sh`
   - 对于 3 系列受管设备：
     `Sourcefire_3D_Device_S3_Upgrade-5.3.0-XXX.sh`
   - 对于 3D9900 受管设备：
     `Sourcefire_3D_Device_x900_Upgrade-5.3.0-XXX.sh`
   - 对于虚拟受管设备：
     `Sourcefire_3D_Device_Virtual64_VMware_Upgrade-5.3.0-XXX.sh`

   重要！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。

4. 选择 **System > Updates**，然后在 **Product Updates** 选项卡中点击 **Upload Update**，将更新上传到防御中心。浏览到更新并点击 **Upload**。

   更新成功上传到防御中心。

5. 确保部署中的设备能够成功通信，并且运行状况监视器未报告任何问题。

6. 点击要安装的更新旁边的安装图标。

   系统将显示 Install Update 页面。

7. 选择要安装更新的设备。

   如果您正在更新堆叠对，选择该对中的一个成员时会自动选择另一个成员。您必须同时更新堆叠对中的所有成员。

8. 点击 **Install**。确认要安装更新并重新启动设备。

   更新过程开始。可在防御中心的任务队列 (**System > Monitoring > Task Status**) 中监控更新进度。

   请注意，在更新过程中，受管设备可能会重新启动两次；这是预期行为。

   警告！如果更新遇到问题 （例如，如果任务队列指示更新失败，或者手动刷新任务队列后几分钟不显示进度），请**勿**重新开始更新，而应联系支持部门。

9. 选择 **Devices > Device Management**，并确认更新的设备是否具有正确的软件版本：5.3.0 版。
10. 确认部署中的设备能够成功通信，并且运行状况监视器未报告任何问题。
11. 将设备配置重新应用到所有受管设备。

> **提示！** 要重新激活灰显的 **Apply** 按钮，请在设备配置中编辑任何接口，然后点击 **Save** 而不进行更改。

12. 将访问控制策略重新应用到所有受管设备。

    应用访问控制策略可能会造成短暂停止流量流动和处理，还可能会导致遗漏检查一些数据包。有关详细信息，请参阅《*Sourcefire 3D 系统用户指南*》。
13. 如果支持站点可以提供 5.3 版的补丁，请按该版本的《*Sourcefire 3D 系统版本说明*》所述应用该补丁。您**必须**更新到最新补丁才可利用最新增强功能和安全修复程序。

使用外壳执行更新

虽然 Sourcefire 建议您在防御中心上使用网络界面执行更新，但偶尔可能需要您使用 bash 外壳更新设备。

对于 5.3 版更新，所有设备都会重新启动。受管设备在更新过程中**不**执行流量检查、交换、路由、 NAT、 VPN 或相关功能。根据设备的配置和部署，更新过程还可能影响流量和链路状态。有关详细信息，请参阅第 10 页的更新期间的流量和检查。

Sourcefire 已了解特定情况下的失败，计划在即将发布的补丁中纠正它们。如果您看到错误消息

要使用外壳安装更新，请执行以下操作：

1. 阅读这些版本说明并完成必要的更新前任务。

   有关详细信息，请参阅第 10 页的开始之前：重要更新和兼容性说明和第 13 页的计划更新。
2. 从 Sourcefire 支持站点下载适当的更新：
   - 对于 2 系列防御中心：
     `Sourcefire_3D_Defense_Center_Upgrade-5.3.0-XXX.sh`
   - 对于 3 系列和虚拟防御中心：
     `Sourcefire_3D_Defense_Center_S3_Upgrade-5.3.0-XXX.sh`
   - 对于 2 系列受管设备：
     `Sourcefire_3D_Device_Upgrade-5.3.0-XXX.sh`
   - 对于 3 系列受管设备：
     `Sourcefire_3D_Device_S3_Upgrade-5.3.0-XXX.sh`

- 对于 3D9900 受管设备：
  `Sourcefire_3D_Device_x900_Upgrade-5.3.0-XXX.sh`
- 对于虚拟受管设备：
  `Sourcefire_3D_Device_Virtual64_VMware_Upgrade-5.3.0-XXX.sh`

重要！ 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。

3. 使用具有管理员权限的帐户登录到设备的外壳。

   对于虚拟设备，使用 VMware vSphere 客户端中的虚拟控制台登录。请注意，在 3 系列或虚拟受管设备上，必须键入 expert 以显示外壳提示符。

4. 在提示符后，以根用户身份运行更新，按提示提供密码。

   `sudo install_update.pl /var/sf/updates/`*`update_name`*

   其中 *`update_name`* 是您之前下载的更新的文件名。

   更新过程开始。

5. 在更新完成后，设备将重新启动。您可以监控更新，并按照以下各节所述完成所有更新后步骤：
   - 第 16 页的更新防御中心
   - 第 18 页的更新受管设备

在 5.3 版中解决的问题

以下问题在 5.3 版中解决：

- 改进了 VPN 的性能和稳定性。（116996、 119698、 123636）
- 解决了以下问题：修改集群堆叠中的设备配置并立即应用更改时，会导致应用失败并且系统在任务状态队列中显示错误消息。 (121625)
- 解决了以下问题：在某些情况下，安装新的入侵规则更新时，会导致关联规则引用的自定义入侵规则分类恢复为预定义分类。 (122163)
- 解决了以下问题：在某些情况下，如果您应用受相同区域和网络 （被配置为发现主机、用户和应用的不同组合）约束的两个或多个网络发现规则，网络发现策略的作用达不到预期。 (122853)
- 解决了以下问题：如果网络环境中用于 LDAP 服务器主机名和 IP 地址的 DNS 条目不匹配，则 LDAP 身份验证可能会失败。 (123447)
- 解决了以下问题：在 3 系列设备上更新 Sourcefire 3D 系统，需要花三个多小时。 (124148)
- 解决了以下问题：在某些情况下，如果设备组包含非活动的受管设备，便无法对设备组进行编辑。 (124286)

- 现在，当系统已在运行 Sourcefire 3D 系统的更新时，如果您尝试安装入侵规则更新，系统会生成错误消息。 (124290)
- 解决了以下问题：在极少数情况下，防御中心没有将事件备份到远程存储。 (124350)
- 解决了以下问题：在某些情况下系统将显示 **Please wait, loading...** 错误消息。 (124918)
- 改进了 Nmap 扫描的性能。 (124999)
- 解决了以下问题：系统不彻底终止失败的入侵规则更新。 (125368)
- 解决了以下问题：系统对 SMTP 预处理器规则 124:1、 124:3 或 124:10 生成误报告警。 (125449)
- 安全问题 解决了多个数据包显示问题。（125531、 132258）
- 改进了敏感数据分析性能。（125588、 126167）
- 解决了以下问题：即使您使用的补救措施禁用了 **Scan from reporting device**，系统也会从设备运行 Nmap 扫描。 (125608)
- 解决了以下问题：如果启用任何自动检测 DCE/RPC 预处理器选项，系统会在重组流量中生成误报告警。 (125737)
- 解决了以下问题：在导入新的入侵规则更新后，入侵策略中的导入的规则数与导入日志中的规则数不匹配。 (125900)
- 安全问题解决了以下问题：系统向具备有限用户角色的用户授予不正确的访问权限。（126016、 127428、 127779）
- 解决了有关集群、堆叠以及集群和堆叠配置中受管设备的多个同步问题。（126106、 128724）
- 改进了向系统日志发送连接事件时系统日志告警响应的稳定性。 (127682)
- 解决了以下问题：当您启用 TCP 数据流预处理器选项 **Require TCP 3-Way Handshake** 并且配置基于速率的攻击防御预处理器来限制过多同步连接时，系统对未完成 （仅限 SYN）连接生成入侵规则 135:2 相关事件。 (127803)
- 解决了以下问题：如果您将流量量变曲线和关联规则配置为在流量峰值达到或超过两个标准偏差时触发，系统并不会生成关联事件。 (128107)
- 解决了以下问题：系统对入侵规则 1:24490 生成误报告警。 (128304)
- 解决了以下硬件问题：在极少数情况下， 3D8120、 3D8130、 3D8140 和 3D8250 出现系统问题而需要重新启动。 (128689)
- 解决了以下问题：如果您使用网络发现策略禁用 LDAP 流量用户检测，防御中心停止记录用户代理登录数据。 (128741)
- 解决了以下问题：在某些情况下，如果您安排了自动 LDAP 用户数据检索，则无法按需执行用户数据检索和下载。 (128962)
- 安全问题 解决了对象管理器和规则编辑器中的跨站点脚本 (XSS) 漏洞。（129052、 132023）

- 解决了以下问题：在某些情况下，如果您看到已审核的入侵事件并向下钻取到数据包视图，但却看不到任何事件，并且已审核的约束已移除。 (129257)
- 解决了以下问题：在某些情况下，如果 SMTP 服务器以连接错误进行响应，系统会错误识别 SMTP 流量并生成缺少应用信息的连接事件。 (130085)
- 解决了高可用性配置中防御中心上的访问控制策略同步问题。 (130475)
- 解决了以下问题：在极少数情况下，系统生成包含无法破译的消息的严重运行状况告警邮件。 (130518)
- 解决了对象管理器中安全区域页面上的多个显示问题。（130569、 130631、 130632）
- 解决了以下问题：在自定义工作流程中向下钻取时，会将您重定向至入侵事件的不正确数据包视图页面。 (130620)
- 解决了以下问题：在某些情况下，即使您选择 **Physical Serial Port** 作为远程控制台访问选项，系统恢复启动选项也不输出到受管设备的串行端口。 (130772)
- 改进了集群受管设备在硬件发生故障后进行故障转移时的稳定性。（130811、 130812、 131031、 133088、 130602）
- 解决了集群受管设备上的故障转移同步问题。 (130829)
- 改进了系统在处理文件传输协议 (FTP) 流量时的恶意软件分析和阻止功能。（130888、 133134）
- 解决了以下问题：在极少数情况下，入侵策略页面无法显示。 (131181)
- 解决了以下问题：在极少数情况下，服务器的表视图 (**Analysis > Hosts > Servers**) 重复列出服务器并产生不准确的服务器计数。 (131329)
- 解决了以下问题：在某些情况下，如果按照知识库文章 000001950 所述配置静态路由，并对网络配置进行后续更改，则系统会丢弃这些静态路由，直到系统下次重新启动为止。 (131646)
- 改进了在三堆栈中堆叠三台受管设备的稳定性。（131836、 131896）
- 解决了以下问题：系统在更新到 Sourcefire 3D 系统的主要版本后，错误放置用户帐户的主目录文件。 (132503)
- 解决了以下问题：禁用入侵策略中的 **Quoted-Printable Decoding Depth** 高级选项不会阻止系统对入侵规则 124:11 生成事件。 (132538)

已知问题

5.3 版中报告了以下已知的问题：

- 如果系统生成将 **Destination Port/ICMP Code** 设置为 0 的事件，则 Intrusion Event Statistics 页面 (**Overview > Summary > Intrusion Event Statistics**) 的 Top 10 Destination Ports 部分会在显示中忽略端口号。 (125581)
- 防御中心本地配置 (**System > Local > Configuration**) 在高可用性对等体之间**不**同步。必须在所有防御中心 （而不仅仅是主要设备）上编辑和应用更改。（130612、 130652）
- 在极少数情况下，配置在层 （与另一个入侵策略共享）中包含本地入侵规则的入侵策略时，可能导致入侵策略导出失败。一种解决方案是为每个共享层创建一个备份副本，并且从入侵策略移除共享层，然后再导出。在导出完成后，将共享层重新添加到入侵策略中。 (132312)
- 在某些情况下，如果在系统开始删除之前磁盘空间使用率超过磁盘空间阈值，则大型系统备份可能会失败。 (132501)
- 在极少数情况下，如果任何入侵策略规则包含敏感数据规则分类，则 Snort 可能会停止处理数据包。 (132600)
- 在某些情况下，使用 RunQuery 工具执行 a `SHOW TABLES` 命令可能会导致查询失败。为避免查询失败，请仅使用 RunQuery 应用以交互方式运行此查询。 (132685)
- 如果在 Sourcefire 3D 系统更新失败后重新启动3 系列 受管设备，则即使您解决了原来的问题，后续更新也可能失败。 (132700)
- 如果删除以前导入的本地入侵规则，则无法重新导入删除的规则。 (132865)
- 在极少数情况下，系统可能不为入侵规则 141:7 或 142:7 生成事件。 (132973)
- 在极少数情况下，如果您创建和应用具有以下规则的访问控制策略， Snort 耗尽系统资源：指定非常大的端口范围，并且包含会导致防御中心以扩展形式将其发送到设备的其他规则条件。 (132998)
- 在某些情况下，受管设备的远程备份包括无关的统一文件，在防御中心上生成大型备份文件。 (133040)
- 访问控制策略的 Security Intelligence 页面无法显示超过 100 个可用的安全区域。 (133418)
- 在某些情况下，将代理服务器配置为通过 Message Digest 5 (MD5) 身份验证进行验证会导致与防御中心的通信出现问题。一种解决方案是配置基本或 NLTM 身份验证。（133727、 135041、 135076）
- 必须使用设备的 CLI 或外壳在受管设备上编辑最大传输单元 (MTU)。您无法通过用户界面在受管设备上编辑 MTU。 (133802)

- 如果在高可用性配置中使用命令行界面 (CLI) 将 3 系列或虚拟受管设备注册到防御中心，设备注册对于第二个防御中心将会失败。一种解决方案是从受管设备的外壳运行 `add_manager.pl` 脚本以将其注册到防御中心。 (133825)
- 如果在 URL 中创建带星号 (*) 的 URL 对象，系统不会为包含引用该对象的规则的访问控制策略生成被抢占的规则警告。请**勿**在 URL 对象 URL 中使用星号 (*)。（134095、 134097）
- 在单个受管设备上重新应用任何入侵策略 （重新应用单个或部分访问控制策略）总计达到 4096 次或更多次数会导致系统问题。 (134231)
- 如果将入侵策略配置为生成入侵事件系统日志告警，由启用了预处理器选项的入侵规则生成的入侵事件系统日志告警消息是 **Snort 告警**，而不是自定义消息。 (134270)
- 在极少数情况下，系统生成无关的 **Module Disk Usage: Frequent drain of Connection Events** 运行状况告警。如果在更新到 5.3 版的过程中看到该运行状况告警，可以放心地忽略。（134355、 137660）
- Sourcefire 文档错误地说明您可以使用用于 X 系列的 Sourcefire 软件在访问控制策略中执行基于地理定位的流量过滤。**不**能在 X 系列的访问控制策略中执行基于地理定位的流量过滤。 (134400)
- 如果堆栈中的辅助设备生成入侵事件，系统不会使用安全区域数据填充入侵事件的表视图。 (134402)
- Sourcefire 文档并未反映：除非用户组以前在流量中出现过并且进入了缓存，否则系统不会匹配流量或者对引用该用户组的访问控制规则生成事件。如果访问控制策略默认操作设置为 **Block All Traffic**，则当允许的用户组中的用户产生的流量第一次出现在网络中时，系统可能会阻止该用户组。 (134440)
- 如果安装某个版本的漏洞数据库 (VDB)，并且您以前已在访问控制策略中启用 NAVL 检测器，系统可能不会将访问控制策略标记为过时。要在防御中心和受管设备之间同步 NAVL 检测器，请在安装 VDB 的新版本后完全重新应用访问控制策略。 (134458)
- 如果配置启用了 **Fast Port Scan** 选项的 Nmap 扫描补救， Nmap 补救将会失败。一种解决方案是禁用 **Fast Port Scan** 选项。 (134499)
- 如果根据连接事件表保存的搜索生成包含连接事件摘要数据的报告，关于该表的报告中未填充任何数据。 (134541)
- 安排和运行同步系统备份任务对系统性能有负面影响。一种解决方案是错开已计划的任务，每次仅运行一个备份。 (134575)
- 如果格林尼治标准时间 （GMT，也称为 UTC）不是您本地的时区，已计划的地理定位更新可能会失败。如果您本地的时区与 GMT 差 +X 小时，请将地理定位更新安排在 X:00 或以后的时间。如果您本地的时区与 GMT 相差 -X 小时，请将地理定位更新安排在 (24:00 - X) 或之前的时间。例如，如果您本地的时区为 UTC-5，请将更新安排在本地时间 19:00 之前。 (134742)

- 查询数据库时，无法使用 application_host_map 表中的 **host_id** 或 **application_tag_id** 字段进行加入。 (134791)
- 如果编辑以前已配置、其中启用了用户和组访问控制参数的 LDAP 连接，则点击 **Fetch Groups** 不会填充 Available Groups 框。在编辑 LDAP 连接以提取可用组时，必须重新输入密码。 (134872)
- 在某些情况下，如果在 Event View Settings 页面的 **Event Preferences** 部分启用 **Resolve IP Addresses**，则与 IPv6 地址相关的主机名在控制面板或事件视图中可能无法正常解析。（135182）
- 在创建 LDAP 身份验证对象时，在 **Base Filter** 字段中不能输入超过 450 个字符。（135314）
- 在某些情况下，如果在执行夏令时 (DST) 时安排任务，则在您未执行 DST 的时段不运行该任务。一种解决方案是在 Time Zone Preference 页面 (**Admin > User Preferences**) 中选择 **Europe, London** 作为您本地的时区，并且在未执行 DST 的时段重新创建任务。（135480）
- 由于数据库检查，系统需要额外的时间来重新启动运行 5.3 版或更高版本的设备。如果在数据库检查过程中发现错误，重新启动需要额外的时间来修复数据库。（135564、 136439）
- 在某些情况下，系统可能对 SSH 预处理器规则 128:1 生成误报。（135567）
- 如果应用其中包含规则 （已启用 **Extract Original Client IP Address** HTTP 预处理器选项）的入侵策略，当流量通过专用代理服务器时，系统可能会使用 **Original Client IP** 字段中使用不正确的数据填充入侵事件。（135651）
- 如果您将受管设备从 5.1.1.x 版更新到 5.2.x 版，然后更新到 5.3 版，系统将对 **high unmanaged disk usage** 生成无关的运行状况告警。（135689）
- 如果将自定义表配置为用 **Correlation Events** 表和 **Applications** 表中的数据进行填充，然后将 **Source IP** 选定为公共字段，则到 5.3 版的更新将会失败。一种解决方案是删除该自定义表，并在更新到 5.3 版后重新创建。（135735）
- 如果将设备从 5.2.x 版更新到 5.3 版，然后创建备份，则在重新映像到 5.3 版的设备上**无法**恢复备份。（135869）
- 在某些情况下，如果您配置具有“监控”规则 （强制记录连接结束的日志）和启用了 **Log at Beginning of Connection** 的“信任”规则的访问控制策略，则系统无法为匹配的 SSH 加密流量生成连接结束事件。一种解决方案是如上所述配置规则，然后在“信任”规则上直接添加“允许”规则。将“允许”规则配置为具有与“信任”规则相同的条件，启用 **Log at Beginning of Connection** 和 **Log at End of Connection**，并且包含与 SSH 加密流量匹配的应用条件。（135952）
- 在某些情况下，系统限制在物理受管设备上访问 User Management 页面 (**System > Local > User Management**)。一种解决方案是手动输入 URL `https://`*`appliance`*`/admin/user/view/cgi` （其中 *appliance* 是设备的 IP 地址或名称），以管理员用户的身份访问 User Management 页面。（136079）

- 如果将访问控制策略应用到多台设备，防御中心将在网络界面的 Task Status 页面、Access Control policy 页面和 Device Management 页面中以不同方式显示任务状态。 Device Management 页面 (**Devices > Device Management**) 中的状态正确。（136364、 136614）
- 在某些情况下，如果根据运行状况事件表创建自定义工作流程，防御中心将在事件查看器中显示冲突的数据。（136419）
- 如果将自定义入侵规则作为 `.rtf` 文件导入，系统不会发出不支持 `.rtf` 文件类型的告警。（136500）
- 如果禁用物理接口，与其关联的逻辑接口也会禁用，但对于该受管设备，在设备编辑器的 Interfaces 选项卡中逻辑接口仍显示为绿色。（136560）
- 记录到系统日志或 SNMP 陷阱服务器的连接事件可能有不正确的 **URL Reputation** 值。 (138504)
- 在访问控制策略中，系统会在实施策略的安全情报黑名单之前处理某些“信任”规则。在第一个“监控”规则之前或者具有应用、 URL、用户或者基于地理定位的网络条件的规则之前放置的“信任”规则，将在黑名单之前处理。也就是说，靠近访问控制策略 （编号小的规则）顶部附近或者在简单策略中使用的“信任”规则允许本应列入黑名单的流量通过而不受检查。（138743、 139017）
- 如果在入侵策略中禁用 **Drop When Inline**，内联标准化停止修改流量中发现的数据包，并且系统不指示要修改哪些流量。在某些情况下，网络中的其他设备或应用在您重新启用 **Drop When Inline** 后可能改变运作方式。（139174、139177）
- 安全问题 Sourcefire 非常了解智能平台管理接口 (IPMI) 标准 (CVE-2013-4786) 中固有的漏洞。在设备上启用无人值守管理 (LOM) 会暴露此漏洞。要减小漏洞，请在仅供受信任用户访问的安全管理网络中部署设备，并且使用复杂、不基于词典的 20 字节密码。如果启用 LOM 并暴露此漏洞，请每三个月更改一次复杂的密码。为防止暴露此漏洞，请勿启用 LOM。（139286、140953）

获得帮助

如果您是新客户，感谢您选择 Sourcefire。请访问 https://support.sourcefire.com/ 来下载 Sourcefire 支持欢迎套件，此文档可帮助您开始使用 Sourcefire 支持和设置客户中心帐户。

如果对 Sourcefire 防御中心或受管设备有任何疑问或需要帮助，请联系 Sourcefire 支持部门：

- 访问 Sourcefire 支持站点 https://support.sourcefire.com/。
- 发邮件给 Sourcefire 支持部门，邮箱为：support@sourcefire.com。
- 致电 Sourcefire 支持部门，号码为：410.423.1901 或 1.800.917.4134。

如果对 X 系列平台有任何疑问或需要帮助，请访问 Blue Coat 支持站点：https://www.bluecoat.com/support/contactsupport/。

感谢您使用 Sourcefire 产品。

法律声明

免责声明