ESA体验跳动(NDR)风暴

目录

简介

本文描述遇到的问题您的电子邮件安全工具(ESA)的地方体验跳动风暴并且提供解决方案对问题。

背景信息

跳动风暴是Joe工作或电子邮件垃圾邮件背景散射的副作用。

Joe工作

Joe工作是使用被伪装的发送方数据和目标败坏明显的发送方名誉并且/或者诱导收件人采取行动明显的发送方的垃圾邮件攻击。

背景散射

背景散射是的电子邮件垃圾邮件、病毒和蠕虫病毒副作用电子邮件服务器收到垃圾邮件和其他邮件发送信号反跳信息对无辜一方。因为原始消息信封发送方被伪造为了包含受害者的电子邮件地址，这发生。因为这些消息未由收件人恳求，彼此是充分地类似的和传送以大批数量，他们合格作为未经请求的大批电子邮件或垃圾邮件。同样地，生成电子邮件背景散射的系统可以变得列出在多种域名系统黑名单(DNSBLs)和是违反网络服务提供商服务条款。

问题

您的ESA体验有消息充盈被注入ESA的跳动风暴。在这样攻击期间的流入连接计数阻止。设备也许开发workqueue备份。为了验证，如果设备是受这样攻击支配，邮件为**从**地址的邮件记录的grep。跳动(无法投递报告-传送失败回执)有**从**地址的空信封邮件。

```
ironport.com> grep -e "From:" mail_logs
Mon Oct 20 14:40:55 2008 Info: MID 10 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 11 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 12 ICID 19 From: <>
```

是受跳动风暴支配的设备将有消息的多数与信封邮件的**从**'**<>**'地址。

解决方案

有一定数量的选项管理跳动风暴。

跳动验证

为了对付这些被误导的跳动攻击， AsyncOS包括思科跳动验证。 当启用，此功能通过ESA标记发送的消息的信封发送方地址。ESA接收的所有信号反跳信息的信封收件人然后被检查此标记出现。当合法信号反跳信息接收时，被添加到信封发送方地址删除的标记和跳动传送到收件人。不包含标记的信号反跳信息可以分开被处理。

AsyncOS考虑跳动，与空邮件的邮件**从**地址(**<>**)。是从地址例如mailer-daemon@example.com或postmaster@example.com的消息没有由系统认为跳动并且不是受跳动验证支配。

配置跳动验证地址标记密钥

跳动验证地址标记密钥列出显示您的当前密钥，并且unpurged的任何锁上您以前使用了。为了添加新密钥，请完成这些步骤：

1. 在**邮件策略>跳动验证**页，请点击**新密钥**。
2. 输入文本字符串并且单击**提交**。
3. 确认您的更改。

清除密钥

如果选择清除的一个规则从下拉菜单并且点击**清除，**您能清除您的旧有地址标记密钥**。**

配置思科跳动验证设置

跳动验证设置确定哪操作采取，当一次无效跳动接收时。

- 选择**邮件策略>跳动验证**。
- 单击 **Edit Settings**。
- 是否选择拒绝无效跳动或添加一个自定义报头到消息。如果想要添加报头，请输入报头名称和值。
- 随意地，请启用聪明的例外。(既使当单个监听程序使用两流入和流出的邮件)，此设置允许内部邮件服务器和信号反跳信息生成的流入的邮件消息自动地豁免从跳动验证处理。
- 提交并且确认您的更改。

配置思科与CLI的跳动验证

您能使用**bvconfig**和**destconfig** in命令CLI为了配置跳动验证。这些命令在思科AsyncOS CLI参考指南讨论。

思科跳动验证和集群配置

跳动验证在集群配置里工作，只要两个思科设备使用同一“跳动密钥”。当您使用同一密钥时，任一个系统应该能接受一合法bounceback。已修改报头标记/密钥不是特定对每个思科设备。

邮件筛选

如果不能使用跳动验证，因为您使用独立的设备收据和交付，您能设置消息过滤器为了阻塞有**从**地址的空邮件的消息。

邮件块

因为这些信号反跳信息很可能将有一个不存在的信封接收地址，您可无效的地址通过会话轻量级目录访问协议(LDAP)接收验证为了帮助更低影响的这样消息。