目录

简介

此条款讨论漏洞研究小组(VRT)如何确定默认入侵策略的规则状态和如何执行Sourcefire设备请确定新规则的适当的默认状态。

规则状态的确定默认策略的

每个规则有一个元数据字段，有零或更多政策价值的。当前有六可能的政策价值：

1. 安全IPS丢弃
2. 安全IPS警报
3. 平衡IPS丢弃
4. 平衡IPS警报
5. 连接IPS丢弃
6. 连接IPS警报

如果IPS策略下降Sourcefire提供了**平衡安全和连接**策略，受管理设备在轴向模式，并且规则有元数据政策价值平衡IPS丢弃，规则将设置下降和生成在您的IPS策略的事件。如果规则有政策价值仅安全IPS丢弃，在您的策略将禁用。

> **注意**：如果规则有指定的多项策略值，例如： 策略安全IPS丢弃，策略平衡IPS丢弃，在两项策略看起来。如果政策价值没有为一个给的规则指定，默认情况下在没有策略看起来。

如果受管理设备设置为被动模式，并且策略设置下降，这没有效果。设备生成警报。如果设备在轴向模式，并且政策价值设置下降，默认情况下规则丢弃数据包。如果其政策价值设置警告，只生成事件，无需丢弃。

最后，在大多数情况下，如果数据包丢弃，警报生成。除非警报抑制为一个给的规则，独立地配置这是真的。

如何执行Sourcefire请确定适当的默认状态，新规则的

规则的默认状态根据一定数量的要素。例如：

影响

注意事项

可能性有多大是它该尝试将做利用此漏洞，并且百分之几我们的用户(Sourcefire客户和更加清楚的喷鼻息社区)可能是易受攻击对此漏洞？

记住的事

与已知攻击的一个Internet Explorer漏洞在通配有更加高冲击比在Linux内核的一个无名的模块能有恶意使用的一个SAP数据库功能，当权限不正确地配置时，或者一次复杂拒绝服务攻击。VRT做开始与漏洞的CVSS分数的一个影响判断，如所需要调节它与我们可能拥有的所有其他信息。这是所有的最重要的量度，因为我们有时将启用规则不会否则获得启用的/没获得集下降，如果影响足够高。

性能

注意事项

是否期待此规则是快速或慢在“平均的”网络？

记住的事

当规则的速度依靠完全地检查时，使性能困难测量的流量，我们有一般想法什么构成正常的网络，并且一个给的规则如何在该正常的网络实行。我们也知道一个规则与，例如，相对长的单个内容匹配(6个或更多字节，典型地)，并且相对唯一(即“而不是obscureJavaScriptFunction()”，"|00 00 00 00|"或“GET/HTTP/1.1")比与复杂PCRE，一系列的byte_test并且/或者byte_jump子句的一个规则将评估快速等等。使用此知识我们能确定规则是否快速或慢并且考虑到那。

信心

注意事项

可能性有多大是此规则生成错误肯定？

记住的事

一些漏洞要求非常详细，容易地检测的情况是存在为了被使用，在我们可以非常确信情况下相关的规则任何时候射击，生活检测安全漏洞代码进展中。例如，如果有在有一个唯一魔术字符串在固定位置的协议的一缓冲区溢出，然后是远离该魔术字符串的一个已修复距离的一个指定的长度，我们可以是确信对我们的能力查找魔术字符串和根据一个已知值检查它问题。在某些情况下，问题是较不明确定义的;例如，某些DNS缓存毒化攻击可以由NXDOMAIN回复异常地大量到达自在某一时期的一个服务器的表示。在这种情况下， NXDOMAIN回复的仅仅出现就其本身不是检测安全漏洞代码的指示器;它在短时间内是指示问题一个非常大数目这样的回复的出现。因为该编号为不同的网络将是不同的， VRT被迫选择应该为多数网络工作和发布那的值;然而，当规则火，实际恶意活动发生时，我们不可以是100%确信那。

在最后但不是最不重要的，而其他要素可能时常设想如相关，影响当晚是国王-确保他们是很可能发现在通配是我们的最关心的我们的客户保护威胁。