目录

简介

针对最新的威胁和漏洞的漏洞研究小组(VRT)版本Sourcefire规则更新(SRU)。一新的SRU版本可能包含更新基本策略用于喷鼻息安装。本文解释漏洞研究小组使用的进程决定规则如何分配到每项策略。

用于的量度确定默认规则集

- 主要使用的度量是普通的漏洞配音录制系统(CVSS)分数分配到也许由规则包括的每个漏洞。
- 第二量度是临时基于并且关系到一个特定的漏洞的年龄。
- 最终量度是覆盖特定区域规则的。那么，当考虑为策略包括，例如， SQL射入规则认为足够重要有影响。

注意：在这些类别的规则包括的漏洞被认为重要，不管年龄。

在安全基础策略的连接

1. CVSS斯克尔必须是10

2. 漏洞的年龄

- 本年度(2014例如)
- 去年(2013在本例中)
- 在为时(2012前的年在本例中)

3. 规则类别

- 没使用此策略

平衡基本策略

注意：**平衡**策略是VRT规则集的默认交付状态开放源喷鼻息的。

1. CVSS斯克尔9或更加极大

2. 漏洞的年龄

   - 本年度(2014例如)
   - 去年(2013在本例中)
   - 在为时(2012前的年在本例中)

3. 规则类别

   - 恶意软件CnC
   - 黑名单
   - SQL射入
   - 检测安全漏洞代码工具包

在连接基础策略的安全

1. CVSS斯克尔8或更加极大

2. 漏洞的年龄

   - 本年度(2014例如)
   - 去年(2013在本例中)
   - 在为时(2012前的年在本例中)
   - 预先年(2011在本例中)

3. 规则类别

   - 恶意软件CnC
   - 黑名单
   - SQL射入
   - 检测安全漏洞代码工具包
   - APP检测

频率策略更新

所有新建的规则被放置到根据已确定标准的一个或很多基本策略。策略每年被再评价，并且从上一年度的规则，当漏洞老化，从策略删除保持策略兼容与选择标准。

如果规则移动在类别之间，他们的在策略的在线状态根据类别选择过程也决定。同样，应该由规则包括的一个特定的漏洞的CVSS分数更改，它是在根据CVSS量度的策略的在线状态也被再评价。

> **注意**：在列出的策略的规则在规则被评估由规则基本类型。将有更旧的一些规则，并且不在那上的标准在默认策略。以上是默认规则的选择标准，并且总是随时变化根据威胁横向。