

Splunk企业安全 — 事件审查中的值得注意的事件显示两次/重复。 Splunk Server中的eventstats创建不一致的结果计数。

适用范围

Splunk Enterprise Splunk Enterprise Security

描述

此问题已在企业安全（大部分）和分布式/搜索头群集Splunk服务器环境（不是Splunk服务器独立环境）上独立报告。

论企业安全

“事件审核”控制面板的重复项：值得注意的事件发生在短时间内产生较多新的企业安全事件，即24小时内产生数千起事件。
其他关联搜索也会出现Bug。

在Splunk服务器上（分布式或集群）

使用 eventstats时，Splunk服务器上可能会出现不一致的结果计数。
此行为似乎与分层/分布式/群集Splunk服务器环境（远程搜索）相关联，并且不能通过不同的独立实例进行复制。

调查

论企业安全

类似以下内容的错误消息将显示在文件splunkd.log的搜索头上。

```
11-28-2018 14:45:15.958 +0100 WARN TcpOutputProc - Possible duplication of events with c
|host::splsearchhead.company.corp|splunkd_ui_access|640056, streamId=0, offset=0 on host
```

在Splunk服务器上（分布式或集群）

示例：

```
index=foo filter" returns 6 resultsindex=foo <filter> | eventstats count(host)" 2 result
```

检查search.log中是否存在没有执行的执行，以及使用执行的执行 | eventstats，将显示以下消息：

```
10-23-2018 10:42:52.343 ERROR Timeliner - Ignored 4 events because they were after the c
```

分辨率

两个独立方案（企业安全和Splunk服务器）的分辨率相同。

发现它是已知Bug:

事件搜索上的SPL- 160881 eventstats在某些情况下可能会创建重复的事件

设置的解决方法：

```
phased_execution_mode=singlethreaded
```

在 limits.conf中，将使eventstats能够正确报告。在为Splunk Server 7.1.x和7.2.x发布补丁之前，应使用解决方法。

已编写修复程序，目前正在进行测试，应在未来的补丁中提供。

对于Splunk Server的版本： 7.2.0、7.2.1、7.2.2、7.2.3，您将遇到一个已知的Bug图表（例如饼图）。

SPL-165363“phased_execution_mode = singlethreaded”会导致字段排序问题

在Splunk Server 7.2.4及更高版本中修复了此问题。 它不会影响Splunk Server 7.1.x。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。