

# Splunk Enterprise Security — 「突發事件回顧」中的顯著事件顯示兩次/重複。 Splunk Server中的eventstats建立不一致的結果計數。

## 適用性

Splunk Enterprise Splunk Enterprise Security

## 說明

此問題已在企業安全（大部分）和分散式/搜尋頭群集Splunk伺服器環境（不是Splunk伺服器獨立環境）上獨立報告。

### 論企業安全

Incident Review Dashboard的副本：值得注意的是，在短時間內產生大量新的企業安全事件，即24小時內產生數千起事件。  
其他關聯搜尋也會發生錯誤。

在Splunk伺服器上（分散式或集群）

使用eventstats時，Splunk伺服器上可能會出現不一致的結果計數。  
此行為似乎與分層/分散式/群集的Splunk伺服器環境（遠端搜尋）相關，並且不能使用不同的獨立例項進行重現。

## 調查

### 論企業安全

splunkd.log檔案中的Search Head上將顯示類似以下內容的錯誤消息。

```
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伺服器上（分散式或集群）

範例：

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

檢查search.log中是否存在不帶和帶有執行 | eventstats，將顯示以下消息：

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

## 解析

兩個獨立方案（企業安全和Splunk伺服器）的解析度是相同的。

發現為已知錯誤：

事件搜尋上的SPL- 160881 eventstats在某些情況下可能會建立重複的事件

設定的解決方法：

```
phased_execution_mode=singlethreaded
```

在 limits.conf中，將啟用eventstats以正確報告。在為Splunk Server 7.1.x和7.2.x發佈修補程式之前，應使用解決方法。

已編寫修復程式，目前正在進行測試，應在將來的修補程式中使用。

對於Splunk Server版本： 7.2.0、7.2.1、7.2.2、7.2.3，您會遇到具有圖表（例如餅圖）的已知錯誤。

SPL-165363 "phased\_execution\_mode = singlethreaded"會導致欄位順序出現問題

在Splunk Server 7.2.4及更高版本中修復了此問題。 它不會影響Splunk Server 7.1.x。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。