

Splunk Enterprise Security : インシデントレビューで注目すべきイベントは2回表示されるか、重複して表示されます。 SplunkサーバのEventStatsにより、矛盾した結果数が生成されます。

適用性

Splunk Enterprise Splunkエンタープライズセキュリティ

説明

この問題は、Enterprise Security (大部分) および分散/検索ヘッドのクラスタ化されたSplunkサーバ環境 (Splunkサーバのスタンドアロン環境ではありません) で個別に報告されています。

エンタープライズセキュリティ

インシデントレビューダッシュボードの重複 : 注目すべきイベントは、短時間で大量の新しいエンタープライズセキュリティインシデント (24時間に数千件のインシデント) が作成された状況で発生しました。

この不具合は、他の相関検索でも発生します。

Splunkサーバ (分散またはクラスタ化)

eventstatsの使用時に、Splunkサーバで一貫性のない結果数が発生する可能性があります。この動作は、階層化/分散/クラスタ化されたSplunkサーバ環境 (リモート検索) に関連付けられているようで、異なるスタンドアロンインスタンスでは再現できません。

調査

エンタープライズセキュリティ

検索ヘッドの splunkd.logファイルに、次のようなエラーメッセージが表示されます。

```
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
```

Splunkサーバ (分散またはクラスタ化)

例 :

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

search.logで | eventstatsを使用した実行と使用しない実行を確認すると、次のメッセージが表示されます。

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

解決方法

2つの独立したシナリオ (Enterprise SecurityとSplunk Server) の解決策は同じです。

これは既知の不具合であることが判明しています。

SPL-160881 イベント検索のeventstatsによって、一部のシナリオで重複イベントが作成される場合があります

設定の回避策 :

```
phased_execution_mode=singlethreaded
```

limits.confで、eventstatsが正しくレポートできるようになります。Splunkサーバ7.1.xおよび7.2.xのパッチがリリースされるまでは、回避策を使用する必要があります。

修正が作成され、将来のパッチで利用可能になる予定のテストを現在実施中です。

Splunk Serverのバージョン7.2.0、7.2.1、7.2.2、7.2.3では、グラフ作成に関する既知のバグ (円グラフなど) が発生します。

SPL-165363 「 phased_execution_mode = singlethreaded 」によりフィールドの順序に問題が発生

これは、Splunk Server 7.2.4以降で修正されています。 Splunk Server 7.1.xには影響しません。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。