

Splunk Enterprise Security - Wichtige Ereignisse in der Incident Review werden zweimal/dupliziert angezeigt. Eventstats im Splunk-Server erzeugen eine inkonsistente Ergebnisanzahl.

Geltungsbereich

Splunk Enterprise Splunk Enterprise Security

Beschreibung

Das Problem wurde unabhängig von Enterprise Security (meistens) und verteilten/Suchkopf-Cluster-Splunk-Server-Umgebungen (nicht Splunk-Server-Standalone) gemeldet .

bei Enterprise Security

Duplikate für das Incident Review Dashboard: Bemerkenswerte Ereignisse traten in einer Situation auf, in der eine größere Anzahl neuer Sicherheitsvorfälle innerhalb kurzer Zeit erstellt wurde, d. h. mehrere tausend Vorfälle innerhalb von 24 Stunden.

Der Fehler tritt auch bei anderen Korrelationssuchen auf.

Auf Splunk-Server (verteilt oder geclustert)

Inkonsistente Ergebniszähler können auf dem Splunk-Server auftreten, wenn Ereignisstatistiken verwendet werden.

Das Verhalten scheint mit einer gestuften/verteilten/geclusterten Splunk-Server-Umgebung (Remote-Suche) verknüpft zu sein und lässt sich nicht mit einer anderen eigenständigen Instanz reproduzieren.

Untersuchung

bei Enterprise Security

Fehlermeldungen wie die folgende werden im Suchkopf in der Datei splunkd.log angezeigt.

```
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
```

Auf Splunk-Server (verteilt oder geclustert)

Beispiel:

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

Überprüfen der Datei search.log auf Ausführungen ohne und mit | eventsStats erscheint die folgende Meldung:

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

Auflösung

Die Auflösung für die beiden unabhängigen Szenarien (Enterprise Security und Splunk Server) ist identisch.

Es wurde ein bekannter Bug gefunden:

SPL-16081-Ereignisstatistiken bei einer Ereignissuche können in einigen Szenarien zu doppelten Ereignissen führen.

Problemumgehung bei der Einstellung:

```
phased_execution_mode=singlethreaded
```

in limits.conf ermöglicht es eventstats, einen korrekten Bericht zu erstellen. Die Problemumgehung sollte angewendet werden, bis ein Patch für Splunk Server 7.1.x und 7.2.x veröffentlicht wird.

Ein Fix wurde geschrieben und wird derzeit getestet, der in einem zukünftigen Patch verfügbar sein sollte.

Für Versionen von Splunk Server: 7.2.0, 7.2.1, 7.2.2, 7.2.3, werden Sie einen bekannten Bug mit

Charting (z.B. Pie Charts) begegnen.

SPL-165363 "phased_execute_mode = singlethread" verursacht ein Problem mit der Feldreihenfolge

Dies wurde in Splunk Server 7.2.4 und höher behoben. Splunk Server 7.1.x ist davon nicht betroffen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.