

Splunk Enterprise Security - Opmerkelijke gebeurtenissen in de Incident Review worden twee keer weergegeven/gedupliceerd. Met Eventstats in Splunk Server wordt een inconsistente resultaattelling gemaakt.

toepasbaarheid

Splunk Enterprise Splunk Enterprise Security

Beschrijving

Het probleem is onafhankelijk gemeld in Enterprise Security (meestal) en in Splunk Server-omgevingen met gedistribueerde/zoekkopclusterde servers (niet Splunk Server standalone) .

Over bedrijfsbeveiliging

Duplicaten voor het Dashboard voor de beoordeling van incidenten: Opmerkelijke gebeurtenissen verschijnen in een situatie waarin in korte tijd een groter aantal nieuwe bedrijfsincidenten werd gemaakt, d.w.z. enkele duizenden incidenten in 24 uur.

De bug komt ook voor bij andere correlatiezoekopdrachten.

Op Splunk Server (gedistribueerd of geclusterd)

Er kunnen inconsistente resultaattellingen optreden op Splunk Server bij het gebruik van eventstats.

Het gedrag lijkt te zijn gekoppeld aan een gelaagde/gedistribueerde/geclusterde Splunk Server-omgeving (extern zoeken) en is niet reproduceerbaar met een andere standalone instantie.

onderzoek

Over bedrijfsbeveiliging

Foutberichten die vergelijkbaar zijn met de volgende worden weergegeven op de zoekkop in het bestand splunkd.log.

```
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
```

Op Splunk Server (gedistribueerd of geclusterd)

Voorbeeld:

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

Als u het search.log bekijkt voor executies zonder en met | eventstats, wordt het volgende bericht weergegeven:

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

resolutie

De resolutie voor de twee onafhankelijke scenario's (Enterprise Security en Splunk Server) is hetzelfde.

Het bleek een bekende bug te zijn:

SPL-160881 eventstats op een eventzoekopdracht kunnen in sommige scenario's dubbele gebeurtenissen maken

De workaround van het instellen:

```
phased_execution_mode=singlethreaded
```

In limits.conf kunnen eventstats correct rapporteren. De oplossing moet worden gebruikt totdat een patch is vrijgegeven voor Splunk Server 7.1.x en 7.2.x.

Er is een reparatie geschreven en momenteel worden tests uitgevoerd die beschikbaar moeten zijn in een toekomstige patch.

Voor versies van Splunk Server: 7.2.0, 7.2.1, 7.2.2, 7.2.3 komt u een bekende bug tegen met grafieken (bijv. cirkeldiagrammen).

SPL-165363 "phased_execution_mode = single threaded" veroorzaakt problemen met veldopdracht

Dit is vastgesteld in Splunk Server 7.2.4 en hoger. Het heeft geen invloed op Splunk Server 7.1.x.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.