

Splunk Enterprise Security: los eventos importantes de la revisión de incidentes se muestran dos veces o duplicados. Las estadísticas de eventos en Splunk Server crean un recuento de resultados incoherente.

Aplicabilidad

Splunk Enterprise Splunk Enterprise Security

Descripción

El problema se ha notificado de forma independiente en los entornos de Enterprise Security (principalmente) y Distributed/Search Head Clustered Splunk Server (no Splunk Server independiente) .

Sobre seguridad empresarial

Duplicados para el panel de revisión de incidentes: Sucesos notables se produjeron en una situación en la que se creó un mayor número de nuevos incidentes de seguridad empresarial en poco tiempo, es decir, varios miles de incidentes en 24 horas. El error también ocurre para otras búsquedas de correlación.

En servidor Splunk (distribuido o en clúster)

Pueden producirse recuentos de resultados incoherentes en Splunk Server cuando se utilizan eventstats.

El comportamiento parece estar vinculado a un entorno de Splunk Server distribuido/por niveles (búsqueda remota) y no se puede reproducir con una instancia independiente diferente.

Investigación

Sobre seguridad empresarial

En el encabezado de búsqueda del archivo splunkd.log aparecerán mensajes de error similares a los siguientes.

```
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
```

En servidor Splunk (distribuido o en clúster)

Ejemplo:

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

Revisión del archivo search.log para las ejecuciones sin y con | eventstats, aparece el siguiente mensaje:

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

Resolución

La resolución para los dos escenarios independientes (Enterprise Security y Splunk Server) es la misma.

Se descubrió que era un error conocido:

SPL-16081 eventstats en una búsqueda de eventos puede crear eventos duplicados en algunos escenarios

La solución alternativa a la configuración:

```
phased_execution_mode=singlethreaded
```

en limits.conf permitirá que eventstats informe correctamente. Se debe utilizar la solución alternativa hasta que se libere un parche para Splunk Server 7.1.x y 7.2.x.

Se ha escrito una corrección que se está probando y que debería estar disponible en un futuro parche.

Para versiones de Splunk Server: 7.2.0, 7.2.1, 7.2.2, 7.2.3, encontrará un error de funcionamiento conocido con gráficos circulares (por ejemplo, gráficos circulares).

SPL-165363 " phase_execution_mode = single thread" causa problemas con el orden de los campos

Esto se corrige en Splunk Server 7.2.4 y versiones posteriores. No afecta a Splunk Server 7.1.x.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).