

Splunk Enterprise Security - Eventos notáveis na Revisão de incidentes são exibidos duas vezes/duplicados. O Eventstats no Splunk Server cria uma contagem de resultados inconsistente.

Aplicabilidade

Splunk Enterprise Splunk Enterprise Security

Descrição

O problema foi relatado de forma independente na Enterprise Security (principalmente) e em ambientes de servidores Splunk agrupados em cluster do Search Head/Distributed (não autônomo do Splunk Server) .

Sobre a segurança corporativa

Duplicatas para o painel de controle de revisão de incidentes: Eventos notáveis apareceram em uma situação em que um número maior de novos incidentes de segurança empresarial foi criado em um curto período de tempo, ou seja, vários milhares de incidentes em 24 horas. O bug também ocorre para outras pesquisas de correlação.

No Servidor Splunk (distribuído ou em cluster)

Contagens de resultados inconsistentes podem ocorrer no Servidor Splunk ao usar eventstats. O comportamento parece estar vinculado a um ambiente de servidor Splunk em camadas/distribuído/em cluster (pesquisa remota) e não pode ser reproduzido com uma instância autônoma diferente.

Investigação

Sobre a segurança corporativa

Mensagens de erro semelhantes às seguintes aparecerão no Cabeçalho de Pesquisa no arquivo 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
```

No Servidor Splunk (distribuído ou em cluster)

Exemplo:

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

Revisando o search.log para execuções sem e com | eventstats, a seguinte mensagem é exibida:

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

Resolução

A resolução para os dois cenários independentes (Segurança corporativa e Servidor Splunk) é a mesma.

Foi encontrado um bug conhecido:

SPL-160881 eventstats em uma pesquisa de eventos podem criar eventos duplicados em alguns cenários

A solução alternativa da configuração:

```
phased_execution_mode=singlethreaded
```

no limits.conf permitirá que eventstats reporte corretamente. A solução alternativa deve ser usada até que um patch seja liberado para o Splunk Server 7.1.x e 7.2.x.

Uma correção foi gravada e está sendo testada no momento e deve estar disponível em um patch

futuro.

Para versões do Servidor Splunk: 7.2.0, 7.2.1, 7.2.2, 7.2.3, você encontrará um Bug conhecido com gráficos (por exemplo, Gráficos de Pizza).

SPL-165363 "phased_execution_mode = singlethreaded" causa problemas com a ordenação de campos

Isso é corrigido no Servidor Splunk 7.2.4 e posterior. Ele não afeta o Splunk Server 7.1.x.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.