

Splunk Enterprise Security - Gli eventi di rilievo nella revisione degli incidenti vengono visualizzati due volte/duplicati. Eventstats in Splunk Server crea un conteggio dei risultati incoerente.

Applicabilità

Splunk Enterprise Splunk Enterprise Security

Descrizione

Il problema è stato segnalato in modo indipendente in ambienti Enterprise Security (per lo più) e Splunk Server in cluster con testa di ricerca/distribuita (non Splunk Server standalone) .

Sulla sicurezza aziendale

Duplicati per il pannello di controllo Revisione incidente: In una situazione in cui è stato creato in breve tempo un numero maggiore di nuovi incidenti di sicurezza aziendale, ovvero diverse migliaia di incidenti in 24 ore, sono apparsi eventi degni di nota.

Il bug si verifica anche per altre ricerche di correlazioni.

Su server di splunk (distribuito o in cluster)

Conteggi dei risultati incoerenti possono verificarsi su Splunk Server quando si utilizzano eventstats.

Il comportamento sembra essere legato a un ambiente Splunk Server di livello/distribuito/cluster (ricerca remota) e non è riproducibile con un'istanza standalone diversa.

Indagine

Sulla sicurezza aziendale

I messaggi di errore simili a quelli riportati di seguito verranno visualizzati nella testa di ricerca nel file 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
```

Su server di splunk (distribuito o in cluster)

Esempio:

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

Esame del file search.log per le esecuzioni senza e con | eventstats, viene visualizzato il seguente messaggio:

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

Risoluzione

La risoluzione per i due scenari indipendenti (Enterprise Security e Splunk Server) è la stessa.

Si è scoperto che si trattava di un bug noto:

Gli stati degli eventi SPL-160881 in una ricerca di eventi possono creare eventi duplicati in alcuni scenari

Soluzione per l'impostazione:

```
phased_execution_mode=singlethreaded
```

in limits.conf consente la corretta segnalazione degli eventi stats. La soluzione alternativa deve essere utilizzata fino al rilascio di una patch per Splunk Server 7.1.x e 7.2.x.

È stata scritta una correzione, attualmente in fase di test, che dovrebbe essere disponibile in una

patch futura.

Per le versioni di Splunk Server: 7.2.0, 7.2.1, 7.2.2, 7.2.3: viene rilevato un bug noto con grafici (ad esempio, grafici a torta).

SPL-165363 "phased_execution_mode = singlethreaded" causa problemi nell'ordinamento dei campi

Questa condizione viene risolta in Splunk Server 7.2.4 e versioni successive. Non influisce su Splunk Server 7.1.x.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).