

Splunk Enterprise Security - Les événements notables de l'examen des incidents sont affichés deux fois/dupliqués. Eventstats dans Splunk Server crée un nombre de résultats incohérent.

Applicabilité

Splunk Enterprise Splunk Enterprise Security

Description

Le problème a été signalé indépendamment sur les environnements Enterprise Security (principalement) et Distributed/Search Head Clustered Splunk Server (et non sur Splunk Server autonome) .

Sur la sécurité des entreprises

Doublons pour le tableau de bord de révision des incidents : Des événements notables sont apparus dans une situation où un plus grand nombre de nouveaux incidents de sécurité d'entreprise ont été créés en peu de temps, c'est-à-dire plusieurs milliers d'incidents en 24 heures.

Le bogue se produit également pour d'autres recherches de corrélation.

Sur le serveur Splunk (distribué ou en cluster)

Des nombres de résultats incohérents peuvent se produire sur le serveur Splunk lors de l'utilisation de eventstats.

Le comportement semble être lié à un environnement de serveur Splunk hiérarchisé/distribué/en cluster (recherche à distance) et n'est pas reproductible avec une autre instance autonome.

Enquête

Sur la sécurité des entreprises

Des messages d'erreur similaires à ceux-ci s'affichent dans l'en-tête de recherche dans le fichier 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
```

Sur le serveur Splunk (distribué ou en cluster)

Exemple :

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

Vérification du journal de recherche des exécutions sans et avec | eventstats, le message suivant s'affiche :

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

Résolution

La résolution pour les deux scénarios indépendants (Enterprise Security et Splunk Server) est la même.

Il s'agit d'un bogue connu :

Les statistiques d'événements SPL-16081 sur une recherche d'événement peuvent créer des événements en double dans certains scénarios

La solution de contournement du réglage :

```
phased_execution_mode=singlethreaded
```

dans limits.conf permettra à eventstats de générer correctement des rapports. La solution de contournement doit être utilisée jusqu'à ce qu'un correctif soit publié pour Splunk Server 7.1.x et 7.2.x.

Un correctif a été écrit et est actuellement en cours de test qui devrait être disponible dans un correctif futur.

Pour les versions de Splunk Server : 7.2.0, 7.2.1, 7.2.2, 7.2.3, vous rencontrerez un bogue connu avec le graphique (par exemple, les graphiques à secteurs).

SPL-165363 "phasé_execution_mode = monothread" cause un problème d'ordre des champs

Cette erreur est corrigée dans Splunk Server 7.2.4 et versions ultérieures. Elle n'affecte pas Splunk Server 7.1.x.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.