

Splunk Enterprise Security - Incident Review에서 눈에 띄는 이벤트는 두 번/중복 표시됩니다.

Splunk Server의 Eventstats에서 일관성 없는 결과 수가 생성됩니다.

적용 가능성

Splunk Enterprise Splunk Enterprise Security

설명

이 문제는 엔터프라이즈 보안(대부분) 및 분산/검색 헤드 클러스터 Splunk 서버 환경(Splunk Server 독립형 아님)에서 독립적으로 보고되었습니다 .

엔터프라이즈 보안

Incident Review Dashboard의 중복 항목: 주목할 만한 이벤트는 짧은 시간에 더 많은 수의 새로운 엔터프라이즈 보안 사고가 생성된 경우(예: 24시간 동안 수천 건의 사고)에 나타났습니다. 다른 상관관계 검색에도 버그가 발생합니다.

Splunk 서버(분산 또는 클러스터형)

eventstats를 사용하는 경우 Splunk Server에서 일관성 없는 결과 수가 발생할 수 있습니다. 이 동작은 계층형/분산/클러스터링된 Splunk Server 환경(원격 검색)에 연결된 것으로 보이며, 다른 독립형 인스턴스로 재현할 수 없습니다.

조사

엔터프라이즈 보안

다음과 유사한 오류 메시지가 splunkd .log 파일의 Search Head에 나타납니다.

```
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
```

Splunk 서버(분산 또는 클러스터형)

예:

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

search.log에서 및 와 함께 실행되지 않는 실행 검토 | eventstats, 다음 메시지가 나타납니다.

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

해결

두 가지 독립 시나리오(엔터프라이즈 보안 및 Splunk Server)의 해결 방법은 동일합니다.

알려진 버그로 확인되었습니다.

SPL-16081 이벤트 검색의 통계는 일부 시나리오에서 중복 이벤트를 생성할 수 있습니다

설정의 해결 방법:

```
phased_execution_mode=singlethreaded
```

in limits.conf는 eventstats가 올바르게 보고할 수 있도록 합니다. 해결 방법은 Splunk Server 7.1.x 및 7.2.x에 대한 패치가 릴리스될 때까지 사용해야 합니다.

수정 사항이 작성되었으며 현재 향후 패치에 사용할 수 있는 테스트가 진행 중입니다.

Splunk Server 버전의 경우: 7.2.0, 7.2.1, 7.2.2, 7.2.3에서는 알려진 버그(예: 파이 차트)가 차트에 표시됩니다.

SPL-165363 " phased_execution_mode = singlethreaded"로 인해 필드 순서 지정 문제가 발생합니다.

이는 Splunk Server 7.2.4 이상에서 수정됩니다. Splunk Server 7.1.x에는 영향을 미치지 않습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.