보안 엔드포인트 Linux 커넥터 장애 문제 해결 18

목차

소개

이 문서에서는 Secure Endpoint Linux 커넥터의 Fault 18에 대해 설명합니다.

결함 18: 커넥터 이벤트 모니터링이 오버로드되었습니다.

동작 보호 엔진은 시스템 활동에 대한 커넥터 가시성을 향상시킵니다. 이와 같이 가시성이 증가하면 커넥터의 시스템 활동 모니터링이 시스템의 활동량에 의해 압도될 가능성이 높아집니다. 이 경우 커넥터는 결함 18을 발생시키고 저하된 모드로 들어갑니다. 결함 18에 대한 자세한 내용은 Cisco Secure Endpoint Linux Connector 결함 문서를 참조하십시오. Linux 커넥터에서 `status` 이 명령을 Secure Endpoint Linux CLI에서 사용하여 커넥터가 성능 저하 모드에서 실행 중인지, 장애가 발생했는지 확인할 수 있습니다. 결함 18이 제기되면 `status` secure Endpoint Linux CLI의 명령은 가능한 두 심각도 중 하나로 결함을 표시합니다.

1. 주요 심각도의 결함 18

```
ampcli> status
Status:                  Connected
Mode:                    Degraded
Scan:                    Ready for scan
Last Scan:               2023-06-19 02:02:03 PM
Policy:                  Audit Policy for FireAMP Linux (#1)
Command-line:            Enabled
Orbital:                 Disabled
Behavioural Protection: Protect
Faults:                  1 Major
Fault IDs:      18
                ID 18 - Major: Connector event monitoring is overloaded. Investigate the most acti
```

2. 심각한 심각도의 결함 18

```
ampcli> status
Status:                  Connected
Mode:                    Degraded
Scan:                    Ready for scan
Last Scan:               2023-06-19 02:02:03 PM
Policy:                  Audit Policy for FireAMP Linux (#1)
Command-line:            Enabled
Orbital:                 Disabled
Behavioural Protection: Protect
Faults:                  1 Critical
Fault IDs:      18
                ID 18 - Critical: Connector event monitoring is overloaded. Investigate the most a
```

Connector Event Monitoring is Overloaded: 주요 심각도

결함 18이 주요 심각도로 제기될 경우, 이는 커넥터 이벤트 모니터링이 오버로드되지만 더 작은 시스템 이벤트 집합을 모니터링할 수 있음을 의미합니다. 이 커넥터는 주요 심각도로 전환되며 1.22.0 이전 커넥터에서 제공되었던 모니터링에 상응하는 이벤트는 적게 모니터링합니다. 시스템 이벤트의 플러드가 짧고 이벤트 모니터링 로드가 허용 가능한 범위로 다시 감소하면 결함 18이 지워지고 커넥터가 모든 시스템 이벤트 모니터링을 다시 시작합니다. 시스템 이벤트의 홍수가 더 심해지고 이벤트 모니터링 로드가 임계값으로 증가하면 장애 18이 심각한 심각도로 제기되고 커넥터가 심각한 심각도로 전환됩니다.

Connector Event Monitoring is Overloaded: Critical Severity

결함 18이 심각한 심각도로 제기될 경우 커넥터에 엄청난 시스템 이벤트가 발생하여 커넥터가 위험에 노출됩니다. 커넥터가 더 제한적인 심각한 심각도로 전환됩니다. 이 상태에서 커넥터는 중요 이벤트를 모니터링하여 커넥터가 정리하고 복구에 집중할 수 있도록 합니다. 이벤트의 홍수가 결국 더 허용 가능한 범위로 다시 감소하면 결함이 완전히 해결되고 커넥터가 모든 시스템 이벤트의 모니터링을 다시 시작합니다.

결함 조치 지침

커넥터에서 중대한 심각도 또는 중대한 심각도의 결함 18이 발생한 경우 문제를 조사하고 해결하기 위해 몇 가지 단계를 수행해야 합니다. 결함 18 해결 단계는 결함이 제기된 시기 및 이유에 따라 달라집니다.

1. Linux 커넥터를 새로 설치할 때 결함 18이 제기되었습니다.
2. 최근 운영 체제가 변경된 후 결함 18이 제기되었습니다.
3. 결함 18이 자발적으로 제기되었습니다.

4. Linux 커넥터가 이미 설치된 시스템을 다시 프로비저닝하거나 커넥터를 버전 1.22.0 이상으로 업데이트할 때 Fault 18이 제기되었습니다

사례 1: 신규 설치

Linux 커넥터를 새로 설치할 때 결함 18 및 저하된 모드가 관찰된 경우, 먼저 시스템이 최소 시스템

요구 사항을 충족하는지 확인해야 합니다. 요구 사항이 최소 요구 사항을 충족하거나 초과하는지 확인한 후, 결함이 지속되면 시스템에서 가장 활성화된 프로세스를 조사해야 합니다. Linux 시스템의 현재 활성 프로세스는 top 명령(또는 유사). CPU를 가장 많이 사용하는 프로세스가 안전한 것으로 알려진 경우 새 프로세스 제외를 생성하여 해당 프로세스를 모니터링에서 제외할 수 있습니다.

시나리오 예:

새로 설치한 후 Secure Endpoint Linux CLI를 통해 결함 18 및 성능 저하 모드가 표시되었다고 가정해 보겠습니다. R실행 top ubuntu 시스템의 명령에서 다음 활성 프로세스를 표시했습니다.

```
Tasks: 223 total,   5 running, 218 sleeping,   0 stopped,   0 zombie
%Cpu(s): 29.4 us, 34.3 sy,  0.0 ni, 36.2 id,  0.0 wa,  0.0 hi,  0.1 si,  0.0 st
MiB Mem :   7943.0 total,   3273.9 free,   2357.6 used,   2311.5 buff/cache
MiB Swap:   2048.0 total,   2048.0 free,      0.0 used.   5141.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  34896 user1     20   0   18136   3292   3044 R  96.7   0.0   0:04.89 trusted_process
   4296 user1     20   0  823768  52020  38900 R  48.0   0.6   0:10.90 gnome-terminal-
    117 root      20   0       0      0      0 I  12.3   0.0   0:01.86 kworker/u64:6-events_unbound
  34827 root      20   0       0      0      0 I  10.3   0.0   0:00.47 kworker/u64:2-events_unbound
   1880 user1     20   0  353080 101600  70164 S   6.3   1.2   0:30.37 Xorg
  34576 root      20   0       0      0      0 R   6.3   0.0   0:01.46 kworker/u64:1-events_unbound
   2089 user1     20   0 3939120 251332 104008 S   3.0   3.1   0:23.25 gnome-shell
    132 root      20   0       0      0      0 I   1.3   0.0   0:02.67 kworker/2:2-events
   6951 root      20   0 1681560 213536  74588 S   1.3   2.6   0:41.30 ampdaemon
    741 root      20   0  253648  13352   9280 S   0.3   0.2   0:01.54 polkitd
    969 root      20   0  153600   3788   3512 S   0.3   0.0   0:00.36 prlshprint
   2291 user1     20   0  453636  29388  20060 S   0.3   0.4   0:03.75 prlcc
      1 root      20   0  169608  13116   8524 S   0.0   0.2   0:01.95 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
```

매우 활발한 프로세스가 있다는 것을 알 수 있습니다 trusted_process 살펴보겠습니다. 이 경우 나는 이 과정에 익숙하고 신뢰가 간다, 내가 이 과정에 대해 의심할 이유가 없다. 결함 18을 지우려면 포털의 프로세스 제외에 신뢰할 수 있는 프로세스를 추가할 수 있습니다. 제외를 생성할 때 모범 사례를 알아보려면 Configure and Identify Cisco Secure Endpoint Exclusions(Cisco 보안 엔드포인트 제외 구성 및 식별) 문서를 참조하십시오.

사례 2: 최근 변경 사항

운영 체제를 최근에 변경한 경우(예: 새 프로그램 설치), 이러한 새 변경 사항으로 시스템 활동이 증가하면 결함 18 및 저하된 모드가 관찰될 수 있습니다. 신규 설치에 설명된 것과 동일한 개선 전략을 사용합니다그러나 새로 설치된 프로그램에서 실행하는 새 프로세스 등 최근 변경 사항과 관련된 프로세스를 찾습니다.

사례 3: 악의적인 활동

동작 보호 엔진은 모니터링되는 시스템 활동의 유형을 늘립니다. 이를 통해 커넥터는 시스템에 대한 더 넓은 관점을 갖게 되며 더 복잡한 동작 공격을 탐지할 수 있습니다. 그러나 시스템 활동을 더 많이 모니터링하면 DoS(denial-of-service) 공격의 위험도 커집니다. 커넥터가 시스템 활동으로 인해 과중한 상태에 있고 결함 18로 성능이 저하된 모드로 전환되는 경우에도 전체 시스템 활동이 줄어들 때까지 계속해서 시스템의 중요 이벤트를 모니터링합니다. 이러한 시스템 이벤트 가시성 손실로 인해 커넥터가 시스템을 보호하는 기능이 저하됩니다. 악성 프로세스에 대해서는 시스템을 즉시 조사하는 것이 중요합니다. 이 `top` Linux 시스템에서 명령(또는 유사)을 실행하여 현재 활성 프로세스를 보고 악의적인 프로세스가 있을 수 있는 경우 적절한 조치를 취하여 상황을 해결합니다.

사례 4: 커넥터 요구 사항

동작 보호 엔진은 머신 활동을 보호하는 커넥터의 기능을 향상시키지만, 이를 위해서는 이전 버전보다 더 많은 리소스를 소비해야 합니다. 결함 18을 자주 제기하는 경우 부하가 큰 정상적인 프로세스가 없으며, 시스템에서 작동하는 악의적인 프로세스가 없는 것으로 나타나면 시스템이 최소 시스템 요구 사항을 충족하는지 확인해야 합니다.

관련 항목

- 보안 엔드포인트 Mac/Linux CLI 사용
- Cisco Secure Endpoint Linux Connector 결함
- Cisco Secure Endpoint Exclusions 구성 및 식별
- 보안 엔드포인트 사용 설명서(PDF)

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.