Fehlerbehebung: Secure Endpoint Linux Connector Fault 18

Inhalt

Einleitung

In diesem Dokument wird Fehler 18 des Secure Endpoint Linux-Connectors beschrieben.

Fehler 18: Connector-Ereignisüberwachung ist überlastet

Die Verhaltensschutz-Engine verbessert die Transparenz der Connectors für die Systemaktivität. Durch diese erhöhte Transparenz steigt die Wahrscheinlichkeit, dass die Überwachung der Systemaktivität des Connectors durch die Systemaktivität überlastet wird. In diesem Fall löst der Steckverbinder den Fehler 18 aus und wechselt in den degradierten Modus. Details zu Fehler 18 finden Sie im Artikel Cisco Secure Endpoint Linux Connector Faults (Linux-Connectorfehler). Auf dem Linux-Connector status kann in der Secure Endpoint Linux CLI verwendet werden, um festzustellen, ob der Connector im heruntergestuften Modus ausgeführt wird und ob Fehler aufgetreten sind. Wird der Fehler 18 ausgelöst, so wird der status in der Secure Endpoint Linux CLI den Fehler mit einem der beiden möglichen Schweregrade anzeigt:

1. Fehler 18 mit großem Schweregrad

```
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. Fehler 18 mit kritischem Schweregrad

```
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-Ereignisüberwachung ist überlastet: Schweregrad schwerwiegend

Wenn der Fehler 18 mit großem Schweregrad ausgelöst wird, bedeutet dies, dass die Steckerereignisüberwachung überlastet ist, aber dennoch in der Lage ist, eine kleinere Anzahl von Systemereignissen zu überwachen. Der Connector wechselt in den Schweregrad "Major" (Schweregrad) und überwacht weniger Ereignisse, die der Überwachung entsprechen, die für ältere Connectors als 1.22.0 verfügbar war. Wenn die Flut von Systemereignissen kurz ist und die Ereignisüberwachungslast wieder in einen akzeptablen Bereich zurückgeht, wird Fehler 18 behoben und der Stecker übernimmt die Überwachung aller Systemereignisse. Wenn sich die Flut von Systemereignissen verschlimmert und die Ereignisüberwachungslast auf einen kritischen Wert ansteigt, wird der Fehler 18 mit kritischem Schweregrad ausgelöst, und der Stecker wechselt in den kritischen Schweregrad.

Connector-Ereignisüberwachung ist überlastet: kritischer Schweregrad

Wenn der Fehler 18 mit kritischem Schweregrad ausgelöst wird, bedeutet dies, dass eine überwältigende Anzahl von Systemereignissen auf dem Steckverbinder auftritt, die ihn gefährden. Der Connector wechselt in einen restriktiveren kritischen Schweregrad. In diesem Zustand überwacht der Connector nur kritische Ereignisse, damit der Connector bereinigen und sich auf die Wiederherstellung konzentrieren kann. Wenn die Ereignisflut schließlich wieder in einen akzeptableren Bereich zurückgeht, wird der Fehler vollständig behoben, und der Connector überwacht erneut alle Systemereignisse.

Leitfaden zur Fehlerbehebung

Wenn der Steckverbinder den Fehler 18 jemals mit einem schweren oder kritischen Schweregrad verursacht, müssen einige Schritte unternommen werden, um das Problem zu untersuchen und zu beheben. Die Schritte zur Behebung von Fehler 18 variieren je nach dem Zeitpunkt und dem Grund der Fehlerbehebung:

1. Fehler 18 wurde bei einer Neuinstallation des Linux-Connectors ausgelöst.
2. Fehler 18 wurde nach den letzten Änderungen am Betriebssystem ausgelöst.
3. Fehler 18 wurde spontan ausgelöst

4. Fehler 18 wurde ausgelöst, als ein Computer, auf dem der Linux-Anschluss bereits installiert war, erneut bereitgestellt oder der Anschluss auf Version 1.22.0+ aktualisiert wurde

Fall 1: Neuinstallation

Wenn bei einer Neuinstallation des Linux-Anschlusses Fehler 18 und ein herabgesetzter Modus festgestellt werden, müssen Sie zunächst sicherstellen, dass Ihr System die minimalen Systemanforderungen erfüllt. Nachdem Sie überprüft haben, ob die Anforderungen die Mindestanforderungen erfüllen oder übertreffen, müssen Sie, falls der Fehler weiterhin besteht, die aktivsten Prozesse im System untersuchen. Sie können die

aktuellen aktiven Prozesse auf einem Linux-System anzeigen, indem Sie top -Kommando (oder Ähnliches) im Terminal. Wenn bekannt ist, dass die Prozesse, die die höchste CPU-Auslastung aufweisen, harmlos sind, können Sie neue Prozessausschlüsse erstellen, um diese Prozesse von der Überwachung auszuschließen.

Beispielszenario:

Angenommen, nach der Neuinstallation werden Fehler 18 und der herabgesetzte Modus über die Secure Endpoint Linux-CLI angezeigt. RAusführen des top -Befehl auf einem Ubuntu-Computer die folgenden aktiven Prozesse angezeigt:

```
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
```

Wir sehen, dass es einen sehr aktiven Prozess gibt, der trusted_process in diesem Beispiel. In diesem Fall bin ich mit diesem Prozess vertraut und es gibt keinen Grund für mich, diesem Prozess misstrauisch zu sein. Zum Löschen des Fehlers 18 kann der vertrauenswürdige Prozess einem Prozessausschluss im Portal hinzugefügt werden. Im Artikel Configure and Identify Cisco Secure Endpoint Exclusions erfahren Sie mehr über die Best Practices beim Erstellen von Ausschlüssen.

Fall 2: Kürzlich vorgenommene Änderungen

Wenn Sie kürzlich Änderungen an Ihrem Betriebssystem vorgenommen haben, z. B. die Installation eines neuen Programms, können Fehler 18 und der herabgesetzte Modus festgestellt werden, wenn diese neuen Änderungen die Systemaktivität erhöhen. Verwenden Sie die gleiche Behebungsstrategie wie in der neuen Installation beschrieben.Suchen Sie jedoch nach Prozessen, die mit den jüngsten Änderungen zusammenhängen, z. B. nach einem neuen Prozess, der von einem neu installierten Programm ausgeführt wird.

Fall 3: Schädliche Aktivitäten

Die Engine für den Verhaltensschutz erhöht die Art der Systemaktivität, die überwacht wird. Dadurch erhält der Connector eine umfassendere Perspektive auf das System und kann komplexere Verhaltensangriffe erkennen. Die Überwachung einer größeren Anzahl von Systemaktivitäten erhöht jedoch auch das Risiko von Denial-of-Service (DoS)-Angriffen. Wenn der Connector durch die Systemaktivität überlastet ist und mit Fehler 18 in den degradierten Modus wechselt, überwacht er weiterhin systemkritische Ereignisse, bis die Systemaktivität insgesamt reduziert wird. Dieser Verlust an Systemereignistransparenz verringert die Fähigkeit des Steckverbinders, Ihre Maschine zu schützen. Es ist wichtig, dass Sie das System sofort auf schädliche Prozesse untersuchen. Verwenden Sie `top` -Befehl (oder Ähnliches) auf Ihrem Linux-System, um die aktuellen aktiven Prozesse anzuzeigen und geeignete Maßnahmen zu ergreifen, um die Situation zu beheben, wenn möglicherweise schädliche Prozesse identifiziert werden.

Fall 4: Verbindungsanforderungen

Die Behavioral Protection Engine verbessert die Fähigkeit des Connectors, Ihre Computeraktivität zu schützen. Hierzu müssen jedoch mehr Ressourcen verbraucht werden als bei früheren Versionen. Wenn Fehler 18 häufig ausgelöst wird, es keine harmlosen Prozesse gibt, die eine hohe Auslastung verursachen, und es scheint, als würden keine bösartigen Prozesse auf dem Computer wirken, dann müssen Sie sicherstellen, dass Ihr System die minimalen Systemanforderungen erfüllt.

Siehe auch

- Verwenden der Secure Endpoint Mac/Linux CLI
- Cisco Secure Endpoint Linux-Connector-Fehler
- Konfigurieren und Identifizieren von Cisco Secure Endpoint-Ausschlüssen
- Benutzerhandbuch zu Secure Endpoints (PDF)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.