Falha no conector do Cisco Secure Endpoint Linux 18

Contents

Introdução

Este documento descreve a Falha 18 no conector Secure Endpoint Linux.

Falha 18: o Monitoramento de Eventos do Conector está Sobrecarregado

O mecanismo de Proteção comportamental melhora a visibilidade dos conectores na atividade do sistema. Com esse aumento na visibilidade, há uma maior possibilidade de que o monitoramento da atividade do sistema do conector possa ser sobrecarregado pela quantidade de atividade no sistema. Se isso acontecer, o conector elevará a falha 18 e entrará no modo degradado. Consulte o artigo Cisco Secure Endpoint Linux Connector Faults para obter detalhes sobre a falha 18. No conector Linux, o comando status pode ser usado na CLI do Secure Endpoint Linux para verificar se o conector está sendo executado em modo degradado e se alguma falha foi detectada. Se a falha 18 for acionada, então a execução da status no Secure Endpoint Linux CLI exibe a falha com uma das duas severidades possíveis:

1. Falha 18 com severidade maior

```
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. Falha 18 com severidade crítica

```
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
```

O Monitoramento de Eventos do Conector está Sobrecarregado: Gravidade Principal

Quando a falha 18 é gerada com severidade maior, isso significa que o monitoramento de eventos do conector está sobrecarregado, mas ainda pode monitorar um conjunto menor de eventos do sistema. O conector alterna para severidade maior e monitora menos eventos equivalentes ao monitoramento que estava disponível em conectores mais antigos que 1.22.0. Se a inundação de eventos do sistema for curta e a carga de monitoramento de eventos diminuir de volta para uma faixa aceitável, a falha 18 será eliminada e o conector retomará o monitoramento de todos os eventos do sistema. Se a inundação de eventos do sistema piorar e a carga de monitoramento de eventos aumentar para uma quantidade crítica, a falha 18 será elevada com severidade crítica e o conector mudará para severidade crítica.

O Monitoramento de Eventos do Conector está Sobrecarregado: Severidade Crítica

Quando a falha 18 é ocasionada com severidade crítica, isso significa que o conector está passando por uma quantidade enorme de eventos de sistema, o que coloca o conector em risco. O conector muda para uma severidade crítica mais restritiva. Nesse estado, o conector monitora apenas eventos críticos para permitir que o conector seja limpo e se concentre na recuperação. Se o fluxo de eventos eventualmente diminuir de volta para um intervalo mais aceitável, a falha será totalmente eliminada e o conector retomará o monitoramento de todos os eventos do sistema.

Diretrizes de ação de falha

Se o conector apresentar a falha 18 com severidade grave ou crítica, algumas etapas devem ser seguidas para investigar e resolver o problema. As etapas para resolver a falha 18 variam de acordo com quando e por que a falha foi gerada:

1. A falha 18 surgiu em uma nova instalação do conector Linux
2. A falha 18 foi gerada após alterações recentes no sistema operacional
3. A falha 18 foi acionada espontaneamente

4. A falha 18 ocorreu durante o reprovisionamento de uma máquina com o conector Linux já instalado ou na atualização do conector para a versão 1.22.0+

Caso 1: Instalação nova

Se for observada a falha 18 e o modo degradado fora de uma nova instalação do conector Linux, você deverá primeiro verificar se o sistema atende aos requisitos mínimos do sistema. Depois de verificar se os requisitos atendem ou excedem os requisitos mínimos, se a falha persistir, você deverá investigar os

processos mais ativos no sistema. Você pode exibir os processos ativos atuais em um sistema Linux usando o comando top (ou similar) no terminal. Se os processos que consomem a maior quantidade de CPU forem reconhecidamente benignos, você poderá criar novas exclusões de processos para impedir que esses processos sejam monitorados.

Cenário de exemplo:

Suponha que após uma nova instalação, a falha 18 e o modo degradado tenham sido exibidos pela CLI do Secure Endpoint Linux. Rexecutando o top em uma máquina Ubuntu exibia estes processos ativos:

```
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
```

Vemos que há um processo muito ativo, chamado trusted_process neste exemplo. Neste caso, estou familiarizado com este processo e confia nele, não há razão para eu desconfiar deste processo. Para limpar a falha 18, o processo confiável pode ser adicionado a uma exclusão de processo no Portal. Consulte o artigo Configure and Identify Cisco Secure Endpoint Exclusions para saber mais sobre as melhores práticas ao criar exclusões.

Caso 2: Alterações recentes

Se você tiver feito alterações recentes no sistema operacional, como a instalação de um novo programa, a falha 18 e o modo degradado poderão ser observados se essas novas alterações aumentarem a atividade do sistema. Use a mesma estratégia de remediação descrita na nova instalaçãocaso, no entanto, você deve procurar processos que estejam relacionados às alterações recentes, como um novo processo executado por um programa recém-instalado.

Caso 3: Atividade maliciosa

O mecanismo Proteção comportamental aumenta os tipos de atividade do sistema que são monitorados. Isso

fornece ao conector uma perspectiva mais ampla sobre o sistema e lhe dá a capacidade de detectar ataques comportamentais mais complexos. No entanto, monitorar uma quantidade maior de atividade do sistema também coloca o conector em um risco maior de ataques de negação de serviço (DoS). Se o conector ficar sobrecarregado com a atividade do sistema e entrar em modo degradado com falha 18, ele ainda continuará a monitorar eventos críticos do sistema até que a atividade geral do sistema seja reduzida. Essa perda na visibilidade de eventos do sistema reduz a capacidade do conector de proteger sua máquina. É essencial que você investigue o sistema imediatamente em busca de processos mal-intencionados. Use o `top` (ou semelhante) no sistema Linux para exibir os processos ativos atuais e tomar as medidas apropriadas para corrigir a situação se algum processo possivelmente mal-intencionado for identificado.

Caso 4: Requisitos do conector

O mecanismo de Proteção comportamental melhora a capacidade do conector de proteger a atividade da sua máquina, mas para fazer isso, ele deve consumir mais recursos do que nas versões anteriores. Se a falha 18 é levantada com frequência, não há processos benignos que estejam causando carga pesada e não parece haver nenhum processo mal-intencionado atuando na máquina, então você deve garantir que seu sistema atenda aos requisitos mínimos do sistema.

Consulte também

- Usar a CLI do Secure Endpoint para Mac/Linux
- Falhas do Conector Linux para Cisco Secure Endpoint
- Configurar e identificar exclusões do Cisco Secure Endpoint
- Guia do usuário do Secure Endpoint (PDF)

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.