Falha no nível de kernel do Linux

Contents

Overview

No Red Hat Enterprise Linux (RHEL) 8 e suas variantes, Oracle Linux 8 Red Hat Compatible Kernel (RHCK), Oracle Linux 7 e 8, Unbreakable Enterprise Kernel (UEK) 6, bem como no Amazon Linux 2 executado em um kernel de sistema 4.19 ou mais recente, o conector do Cisco Secure Endpoint Linux não poderá monitorar movimentações de arquivos nem ativar a Correlação de Fluxo de Dispositivo (monitoramento de rede) quando o pacote kernel-devel, ou pacote kernel-uek-devel no Oracle Linux UEK, estiver ausente para o kernel atualmente em execução. O conector apontará o ID de falha 11 "O pacote kernel-devel necessário está ausente" nessa situação. Para Debian e Ubuntu esta falha pode ser levantada quando o pacote linux-headers estiver faltando.

Começando com o kernel RHEL 8, Oracle Linux 8 RHCK, Oracle Linux 7 e 8 UEK 6 e Amazon Linux 2 4.19 ou mais recente, o conector usará módulos eBPF para o monitoramento de rede e do sistema de arquivos em tempo real. Os módulos eBPF substituem os Linux Kernel Modules usados quando executados em RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 e anterior e o kernel Amazon Linux 2 4.14 ou anterior. Para o Ubuntu 18.04 e posterior, assim como para o Debian 10 e posterior, os módulos eBPF são nativos.

Para maior compatibilidade, o conector compilará automaticamente os módulos eBPF usados pelo conector antes de carregá-los e executá-los no sistema. Esta compilação requer que os arquivos de cabeçalho de desenvolvimento de kernel correspondentes ao kernel atualmente em execução sejam instalados. O conector tentará compilar e carregar os módulos eBPF cada vez que o conector for iniciado

Ocasionalmente, essa falha pode aparecer no Oracle Linux com o UEK instalado, apesar de os pacotes de desenvolvimento de kernel estarem presentes na máquina. Isso é causado por uma falha durante o processo de instalação em que o conector não pode configurar o SELinux para aceitar sondas eBPF usadas para monitorar a atividade no ponto final.

Aplicabilidade

A falha normalmente será gerada após uma nova instalação do conector Secure Endpoint Linux ou após a atualização do kernel do sistema.

Sistemas operacionais

- RHEL/CentOS/Rocky Linux/AlmaLinux 8
- Oracle Linux 8 RHCK
- Oracle Linux 7 e 8 UEK 5 e 6
- Ubuntu 18.04 e posterior
- Debian 10 e mais recente
- Amazon Linux 2

Versões do Conector

- Linux 1.13.0 e posterior

RHEL Linux

O pacote kernel-devel instala os arquivos de cabeçalho de desenvolvimento kernel necessários no diretório /usr/src/kernels, organizados de acordo com sua versão kernel.

Causas

O pacote em nível de kernel necessário para o sistema de arquivos em tempo real e o monitoramento de atividade de rede está ausente.

Resolução

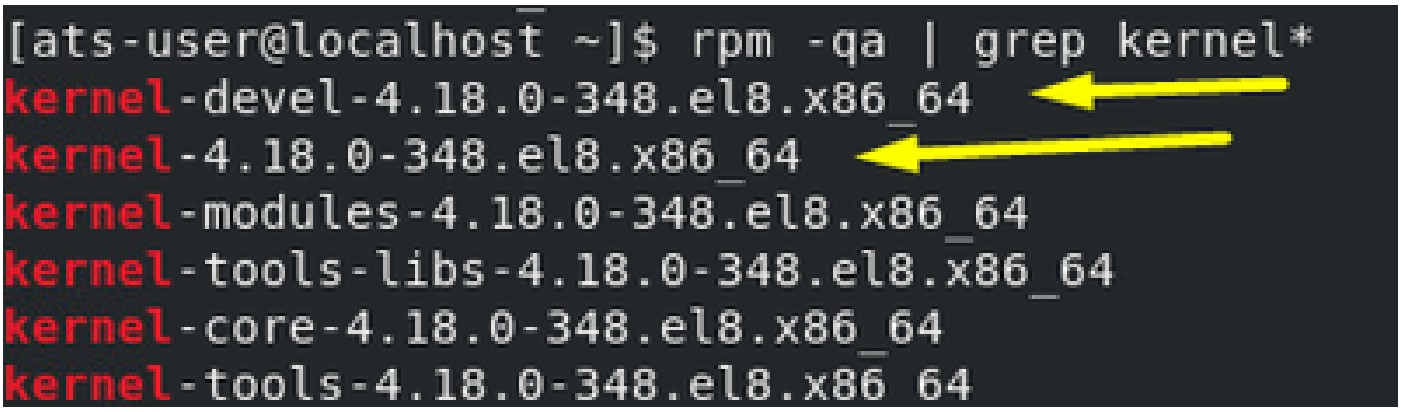
Instale o pacote `kernel-devel` que corresponda ao kernel em execução no momento.

Procedimento

O pacote 'kernel-devel' precisa corresponder ao kernel em execução no momento. Para verificar se o pacote 'kernel-level' está instalado e/ou ausente, execute o seguinte procedimento:

```
rpm -qa | grep kernel*
```

Este é um exemplo de saída que ilustra o pacote 'kernel-devel' correspondente ao kernel em execução no momento.



Para instalar o pacote kernel-devel correspondente ao kernel atualmente em execução, execute o seguinte.

```
dnf install -y kernel-devel-$(uname -r)
```

O conector deve se recuperar e eliminar a falha em um minuto. Se a falha não desaparecer em um minuto, reinicie manualmente o conector. A falha deve ser eliminada dentro de um minuto após a reinicialização.

OBSERVAÇÃO: se o comando acima falhar com o erro "No match for arguments", é possível que a versão atual do kernel não seja mais suportada e o mantenedor do sistema operacional tenha removido o pacote do repositório dnf. Nesse caso, o pacote .rpm de desenvolvimento do kernel necessário pode ser baixado manualmente dos arquivos do sistema operacional do fornecedor e, em seguida, instalado manualmente, ou o kernel pode ser atualizado para uma versão compatível e o comando acima pode ser tentado novamente.

Por exemplo, se o uso do CentOS e a atualização do kernel para uma versão suportada pela distribuição não for possível, os pacotes .rpm antigos em nível de kernel do CentOS podem ser baixados manualmente de http://vault.centos.org. O nome do arquivo a ser baixado é fornecido pela saída do seguinte comando bash.

```
echo kernel-devel-$(uname -r).rpm
```

Após o download, o pacote kernel-devel pode ser instalado executando o seguinte comando bash no diretório onde o arquivo .rpm baixado é salvo.

```
dnf install -y kernel-devel-$(uname -r).rpm
```

Linux Oracle

O Oracle Linux distribui com duas alternativas de kernel diferentes, RHCK e UEK. Os pacotes kernel-devel e kernel-uek-devel instalam os arquivos de cabeçalho de desenvolvimento do kernel necessários no diretório /usr/src/kernels em RHCK e UEK, respectivamente. Os arquivos de desenvolvimento do kernel são organizados em /usr/src/kernels de acordo com sua versão do kernel.

RHCK do Oracle Linux

O procedimento para identificar o pacote de kernel ausente e resolver o ID de falha 11 no RHCK do Oracle Linux é idêntico ao do RHEL Linux. Consulte a seção RHEL Linux acima para obter mais informações.

Oracle Linux UEK

O procedimento para identificar o pacote de kernel ausente e resolver o ID de falha 11 no Oracle Linux UEK é semelhante, mas não idêntico ao do RHEL Linux. Consulte a seção RHEL Linux acima para obter mais informações, mas substitua cada instância de "kernel-devel" por "kernel-uek-devel". Para ser específico, `substitua kernel-devel-$(uname -r)` por kernel-uek-devel-$(uname -r)para cada comando relevante.

OBSERVAÇÃO: se o pacote kernel-uek-devel .rpm necessário não for encontrado durante a tentativa de instalação a partir do repositório dnf, o pacote poderá ser baixado manualmente e instalado a partir dos arquivos Oracle em https://yum.oracle.com/.

Linux Debian/Ubuntu

O pacote linux-headers instala os arquivos de cabeçalho necessários no diretório /usr/src, organizados de acordo com a versão do kernel.

Causas

O pacote linux-headers necessário para monitoração em tempo real do sistema de arquivos e da atividade de rede está ausente.

Você pode confirmar os cabeçalhos instalados no diretório /usr/src.

Resolução

O pacote linux-headers pode ser instalado com o seguinte comando:

```
sudo apt install linux-headers-$(uname -r)
```

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.