Linux 커널-장치 결함

목차

개요

RHEL(Red Hat Enterprise Linux) 8 및 변형, Oracle Linux 8 RHCK(Red Hat Compatible Kernel), Oracle Linux 7 및 8 UEK(Unbreakable Enterprise Kernel) 6 및 4.19 이상의 시스템 커널에서 실행되는 Amazon Linux 2의 경우, Cisco Secure Endpoint Linux 커넥터는 커널-Kernel-Device Flow Monitoring(네트워크 모니터링) 또는 파일 이동을 모니터링하지 못합니다. Oracle Linux UEK의 uek-devel 패키지가 현재 실행 중인 커널에 없습니다. 이 상황에서 커넥터에는 결함 ID 11 "필수 커널 장치 패키지가 없습니다"가 표시됩니다. Debian 및 Ubuntu의 경우 linux-headers 패키지가 누락될 때 이 결함이 발생할 수 있습니다.

RHEL 8, Oracle Linux 8 RHCK, Oracle Linux 7 및 8 UEK 6, Amazon Linux 2 커널 4.19 이상에서 커넥터는 실시간 파일 시스템 및 네트워크 모니터링에 eBPF 모듈을 사용합니다. eBPF 모듈은 RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 이하 및 Amazon Linux 2 커널 4.14 이하에서 실행할 때 사용되는 Linux 커널 모듈을 대체합니다. Ubuntu 18.04 이상과 Debian 10 이상에서는 eBPF 모듈이 기본 모듈입니다.

대부분의 호환성을 위해 커넥터는 시스템에서 해당 모듈을 로드하고 실행하기 전에 커넥터에서 사용하는 eBPF 모듈을 자동으로 컴파일합니다. 이 컴파일을 사용하려면 현재 실행 중인 커널에 해당하는 커널 개발 헤더 파일을 설치해야 합니다. 실시간 파일 시스템 및 네트워크 모니터링을 사용하도록 설정하면 커넥터는 커넥터가 시작될 때마다 eBPF 모듈을 컴파일하거나 정책 업데이트의 일부로 이 기능을 사용하도록 설정할 때 실시간으로 컴파일합니다.

적용 가능성

결함은 일반적으로 새로운 보안 엔드포인트 Linux 커넥터 설치 후 또는 시스템 커널을 업데이트한 후에 제기됩니다.

운영 체제

- RHEL/CentOS/Rocky Linux/AlmaLinux 8
- Oracle Linux 8 RHCK
- Oracle Linux 7 및 8 UEK 6
- Ubuntu 18.04 이상
- Debian 10 이상
- Amazon Linux 2

커넥터 버전

- Linux 1.13.0 이상

RHEL Linux

kernel-devel 패키지는 필요한 커널 개발 헤더 파일을 커널 버전에 따라 구성된 /usr/src/kernels 디렉토리에 설치합니다.

원인

실시간 파일 시스템 및 네트워크 활동 모니터링에 필요한 커널-디바이스 패키지가 누락되었으며 커넥터 정책에 '파일 복사 및 이동 모니터링' 또는 '디바이스 플로우 상관관계 활성화'가 활성화되어 있습니다.

해결

현재 실행 중인 커널과 일치하는 'kernel-devel' 패키지를 설치합니다.

또는 드문 경우이지만 실시간 파일 시스템 및 네트워크 모니터링이 필요하지 않을 경우 정책에서 '파일 복사 및 이동 모니터링' 및 '디바이스 플로우 상관관계 활성화'를 모두 비활성화하여 이 장애를 해결할 수 있습니다. 이러한 기능이 비활성화된 경우 커넥터는 시스템에 대한 실시간 보호를 제공하지 않습니다.

절차

현재 실행 중인 커널에 해당하는 커널-디바이스 패키지를 설치하려면 다음을 실행합니다.

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

커넥터는 1분 이내에 오류를 복구하여 지워야 합니다. 1분 내에 결함이 제거되지 않으면 커넥터를 수동으로 다시 시작합니다. 그런 다음 다시 시작한 후 1분 이내에 결함을 지워야 합니다.

참고: 위의 명령이 "인수와 일치하지 않음"이라는 오류 메시지와 함께 실패하면 현재 커널 버전이 더 이상 지원되지 않으며 OS 유지 관리자가 dnf 저장소에서 패키지를 제거할 수 있습니다. 이 경우 필요한 kernel-devel .rpm 패키지를 공급업체의 OS 아카이브에서 수동으로 다운로드한 다음 수동

으로 설치하거나, 커널을 지원되는 버전으로 업데이트하여 위 명령을 다시 시도할 수 있습니다.

예를 들어 CentOS를 사용하고 커널을 배포에서 지원하는 버전으로 업데이트할 수 없는 경우 http://vault.centos.org에서 CentOS용 이전 kernel-devel .rpm 패키지를 수동으로 다운로드할 수 있습니다. 다운로드할 파일의 이름은 다음 bash 명령의 출력에 의해 지정됩니다.

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

다운로드한 후에는 다운로드한 .rpm 파일이 저장된 디렉토리에서 다음 bash 명령을 실행하여 kernel-devel 패키지를 설치할 수 있습니다.

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

Oracle Linux

Oracle Linux는 RHCK와 UEK라는 두 가지 다른 커널 대안과 함께 배포됩니다. kernel-devel 및 kernel-uek-devel 패키지는 필요한 커널 개발 헤더 파일을 각각 RHCK 및 UEK의 /usr/src/kernels 디렉토리에 설치합니다. 커널 개발 파일은 커널 버전에 따라 /usr/src/kernel에서 구성됩니다.

Oracle Linux RHCK

Oracle Linux RHCK에서 누락된 커널 패키지를 식별하고 결함 ID 11을 확인하는 절차는 RHEL Linux와 동일합니다. 자세한 내용은 위의 RHEL Linux 섹션을 참조하십시오.

Oracle Linux UEK

Oracle Linux UEK에서 누락된 커널 패키지를 식별하고 결함 ID 11을 확인하는 절차는 비슷하지만 RHEL Linux와 동일하지는 않습니다. 자세한 내용은 위의 RHEL Linux 섹션을 참조하되 "kernel-devel"의 모든 인스턴스를 "kernel-uek-devel"로 바꾸십시오. 구체적으로 설명하려면 모든 관련 명령 `kernel-uek-devel-$(uname -r)`를 바꿉니다.

참고: dnf 저장소에서 설치를 시도할 때 필요한 kernel-uek-devel .rpm 패키지를 찾을 수 없는 경우 https://yum.oracle.com/의 Oracle 아카이브에서 패키지를 수동으로 다운로드하여 설치할 수 있습니다.

Debian/Ubuntu Linux

linux-headers 패키지는 필요한 헤더 파일을 커널 버전에 따라 구성된 /usr/src 디렉토리에 설치합니다.

원인

실시간 파일 시스템 및 네트워크 활동 모니터링에 필요한 Linux 헤더 패키지가 누락되었으며 커넥터 정책에 'Monitor File Copies and Moves' 또는 'Enable Device Flow Correlation' 중 하나가 활성화되어 있습니다.

해결

linux-headers 패키지는 다음 명령을 사용하여 설치할 수 있습니다.

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