Linux Kernel-Devel-Fehler

Inhalt

Überblick

Unter Red Hat Enterprise Linux (RHEL) 8 und Varianten, Oracle Linux 8 Red Hat Compatible Kernel (RHCK), Oracle Linux 7 und 8 Unbreakable Enterprise Kernel (UEK) 6 sowie Amazon Linux 2, der auf einem 4.19 oder neueren System-Kernel ausgeführt wird, kann der Cisco Secure Endpoint Linux Connector nicht Dateiverschiebungen überwachen oder die Device Flow Correlation (Netzwerküberwachung) aktivieren, wenn der Kernel nel-devel-Paket oder kernel-uek-devel-Paket auf Oracle Linux UEK fehlt für den aktuell laufenden Kernel. Der Connector löst Fehler-ID 11 "Erforderliches Kernel-Paket fehlt" in dieser Situation aus. Für Debian und Ubuntu kann dieser Fehler ausgelöst werden, wenn das Linux-Headers-Paket fehlt.

Ab RHEL 8, Oracle Linux 8 RHCK, Oracle Linux 7 und 8 UEK 6 und Amazon Linux 2 Kernel 4.19 oder neuer verwendet der Connector eBPF-Module für die Echtzeit-Dateisystem- und Netzwerküberwachung. Die eBPF-Module ersetzen die Linux-Kernel-Module, die bei der Ausführung auf RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 und früher und Amazon Linux 2 Kernel 4.14 oder früher verwendet werden. Für Ubuntu 18.04 und höher sowie für Debian 10 und höher sind eBPF-Module nativ.

Aus Gründen der größtmöglichen Kompatibilität kompiliert der Anschluss automatisch die eBPF-Module, die vom Anschluss verwendet werden, bevor diese geladen und auf das System ausgeführt werden. Diese Kompilierung erfordert, dass die Headerdateien der Kernelentwicklung, die dem aktuell ausgeführten Kernel entsprechen, installiert werden. Wenn die Echtzeit-Dateisystem- und Netzwerküberwachung aktiviert ist, kompiliert der Connector die eBPF-Module jedes Mal, wenn der Connector gestartet wird, oder in Echtzeit, wenn diese Funktionen im Rahmen einer Richtlinienaktualisierung aktiviert werden.

Geltungsbereich

Der Fehler wird in der Regel nach der Installation eines neuen Secure Endpoint Linux-Connectors oder nach der Aktualisierung des System-Kernels ausgelöst.

Betriebssysteme

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

Connector-Versionen

- Linux 1.13.0 und höher

RHEL Linux

Das Kernel-devel-Paket installiert die benötigten Kernel-Entwicklungs-Header-Dateien im Verzeichnis /usr/src/kernels, organisiert entsprechend der Kernel-Version.

Ursachen

Das für die Überwachung des Dateisystems und der Netzwerkaktivität in Echtzeit erforderliche Kernel-Devel-Paket fehlt, und die Connector-Richtlinie hat entweder 'Monitor File Copies and Moves' oder 'Enable Device Flow Correlation' aktiviert.

Auflösung

Installieren Sie das Paket "kernel-devel", das dem aktuell laufenden Kernel entspricht.

Alternativ kann in der seltenen Situation, dass eine Überwachung des Dateisystems und des Netzwerks in Echtzeit nicht erforderlich ist, dieser Fehler durch Deaktivieren von 'Monitor File Copies and Moves' und 'Enable Device Flow Correlation' in der Richtlinie behoben werden. Beachten Sie, dass der Anschluss das System nicht in Echtzeit schützt, wenn diese Funktionen deaktiviert sind.

Vorgehensweise

Um das Kernel-Devel-Paket zu installieren, das dem aktuell laufenden Kernel entspricht, führen Sie folgendes aus.

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

Der Anschluss sollte den Fehler innerhalb einer Minute wiederherstellen und beheben. Wenn der

Fehler nicht innerhalb einer Minute behoben wird, starten Sie den Anschluss manuell neu. Der Fehler sollte dann innerhalb einer Minute nach dem Neustart behoben werden.

HINWEIS: Wenn der obige Befehl mit dem Fehler "Keine Übereinstimmung für Argument" fehlschlägt, ist es möglich, dass die aktuelle Kernel-Version nicht mehr unterstützt wird und der OS-Betreuer das Paket aus dem dnf-Repository entfernt hat. In diesem Fall kann das benötigte Paket für Kernel-devel .rpm manuell aus den Betriebssystemarchiven des Herstellers heruntergeladen und dann manuell installiert werden, oder der Kernel kann auf eine unterstützte Version aktualisiert werden und der obige Befehl erneut versucht werden.

Wenn beispielsweise die Verwendung von CentOS und die Aktualisierung des Kernels auf eine von der Distribution unterstützte Version nicht möglich ist, können alte RPM-Pakete für CentOS auf Kernelebene manuell von http://vault.centos.org heruntergeladen werden. Der Name der herunterzuladenden Datei wird durch die Ausgabe des folgenden Bash-Befehls angegeben.

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

Nach dem Herunterladen kann das Kernel-Devel-Paket installiert werden, indem der folgende bash-Befehl in dem Verzeichnis ausgeführt wird, in dem die heruntergeladene RPM-Datei gespeichert ist.

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

Oracle Linux

Oracle Linux verteilt sich mit zwei verschiedenen Kernel-Alternativen, RHCK und UEK. Die Pakete kernel-devel und kernel-uek-devel installieren die benötigten Kernelentwicklungs-Header-Dateien im Verzeichnis /usr/src/kernels auf RHCK bzw. UEK. Die Kernel-Entwicklungsdateien sind in /usr/src/kernels entsprechend ihrer Kernel-Version organisiert.

Oracle Linux-RHCK

Das Verfahren zum Identifizieren des fehlenden Kernelpakets und zum Lösen der Fehler-ID 11 auf Oracle Linux RHCK ist identisch mit dem von RHEL Linux. Weitere Informationen finden Sie im Abschnitt RHEL Linux oben.

Oracle Linux UEK

Das Verfahren zur Identifizierung des fehlenden Kernelpakets und zur Behebung der Fehler-ID 11 auf Oracle Linux UEK ist ähnlich, aber nicht identisch mit dem von RHEL Linux. Weitere Informationen finden Sie im Abschnitt RHEL Linux weiter oben. Ersetzen Sie jedoch alle Instanzen von "kernel-devel" durch "kernel-uek-devel". Um genau zu sein, `ersetzekernel-devel-$(uname -r) mit kernel-uek-devel-$(uname -r)` für jeden relevanten Befehl.

HINWEIS: Wenn das benötigte Paket kernel-uek-devel .rpm beim Versuch, aus dem dnf-Repository zu installieren, nicht gefunden wird, kann das Paket manuell heruntergeladen und aus den Oracle-Archiven unter https://yum.oracle.com/ installiert werden.

Debian/Ubuntu Linux

Das Paket linux-headers installiert die benötigten Headerdateien im Verzeichnis /usr/src, organisiert nach der Kernel-Version.

Ursachen

Das Linux-Header-Paket, das für die Überwachung von Dateisystemen und Netzwerkaktivitäten in Echtzeit erforderlich ist, fehlt, und die Connector-Richtlinie hat entweder 'Monitor File Copies and Moves' oder 'Enable Device Flow Correlation' aktiviert.

Auflösung

Das Linux-Headers-Paket kann mit dem folgenden Befehl installiert werden:

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