

# Errore di sviluppo del kernel Linux

## Sommario

---

## Panoramica

Su Red Hat Enterprise Linux (RHEL) 8 e versioni successive, Oracle Linux 8 Red Hat Compatible Kernel (RHCK), Oracle Linux 7 e 8, Unbreakable Enterprise Kernel (UEK) 6, nonché Amazon Linux 2 in esecuzione su un kernel di sistema 4.19 o più recente, il connettore Cisco Secure Endpoint Linux non sarà in grado di monitorare gli spostamenti di file o abilitare Device Flow Correlation (monitoraggio della rete) quando il pacchetto kernel-devel, o kernel-uek-devel su Oracle Linux UEK, risulta mancante per il kernel attualmente in esecuzione. In questa situazione, il connettore genererà l'ID errore 11 "Pacchetto di sviluppo del kernel richiesto mancante". Per Debian e Ubuntu questo errore può essere sollevato quando manca il pacchetto linux-headers.

A partire da RHEL 8, Oracle Linux 8 RHCK, Oracle Linux 7 e 8 UEK 6 e il kernel Amazon Linux 2 4.19 o versione successiva, il connettore utilizzerà i moduli eBPF per il monitoraggio in tempo reale del file system e della rete. I moduli eBPF sostituiscono i moduli kernel Linux utilizzati quando vengono eseguiti su RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 e versioni precedenti e il kernel Amazon Linux 2 4.14 o versioni precedenti. Per Ubuntu 18.04 e versioni successive, nonché per Debian 10 e versioni successive, i moduli eBPF sono nativi.

Per garantire la massima compatibilità, il connettore compila automaticamente i moduli eBPF utilizzati dal connettore prima di caricarli ed eseguirli sul sistema. Questa compilazione richiede l'installazione dei file di intestazione per lo sviluppo del kernel corrispondenti al kernel attualmente in esecuzione. Il connettore tenterà di compilare e caricare i moduli eBPF a ogni avvio del connettore

Occasionalmente, questo errore può apparire su Oracle Linux con UEK installato nonostante i pacchetti di sviluppo del kernel siano presenti sul computer. Ciò è causato da un errore durante il processo di installazione in cui il connettore non è in grado di configurare SELinux per accettare le sonde eBPF utilizzate per monitorare l'attività sull'endpoint.

## Applicabilità

L'errore viene in genere generato dopo l'installazione di un nuovo connettore Secure Endpoint Linux o dopo l'aggiornamento del kernel del sistema.

## Sistemi operativi

- RHEL/CentOS/Rocky Linux/AlmaLinux 8

- RHCK per Oracle Linux 8
- Oracle Linux 7 e 8 UEK 5 e 6
- Ubuntu 18.04 e versioni successive
- Debian 10 e versioni successive
- Amazon Linux 2

## Versioni connettore

- Linux 1.13.0 e versioni successive

## RHEL Linux

Il pacchetto `kernel-devel` installa i file di intestazione per lo sviluppo del kernel necessari nella directory `/usr/src/kernels`, organizzati in base alla versione del kernel.

### Cause

Manca il pacchetto di sviluppo del kernel necessario per il monitoraggio in tempo reale del file system e dell'attività di rete.

### Risoluzione

Installare il pacchetto `kernel-devel` corrispondente al kernel attualmente in esecuzione.

### Procedura

Il pacchetto `kernel-devel` deve corrispondere al kernel attualmente in esecuzione. Per verificare se il pacchetto `kernel-devel` corrente è installato e/o mancante, eseguire quanto segue:

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

Di seguito è riportato un output di esempio che illustra il pacchetto `kernel-devel` corrispondente al kernel attualmente in esecuzione.

```
[ats-user@localhost ~]$ rpm -qa | grep kernel*
kernel-devel-4.18.0-348.el8.x86_64
kernel-4.18.0-348.el8.x86_64
kernel-modules-4.18.0-348.el8.x86_64
kernel-tools-libs-4.18.0-348.el8.x86_64
kernel-core-4.18.0-348.el8.x86_64
kernel-tools-4.18.0-348.el8.x86_64
```

Per installare il pacchetto di sviluppo del kernel corrispondente al kernel attualmente in esecuzione, eseguire quanto segue.

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

Il connettore dovrebbe essere ripristinato e cancellare il guasto entro un minuto. Se il problema non viene risolto entro un minuto, riavviare manualmente il connettore. Il guasto deve essere quindi risolto entro un minuto dal riavvio.

**NOTA:** se il comando precedente non riesce e viene visualizzato l'errore "Nessuna corrispondenza per l'argomento", è possibile che la versione corrente del kernel non sia più supportata e che il gestore del sistema operativo abbia rimosso il pacchetto dal repository dnf. In questo caso, il pacchetto .rpm per lo sviluppo del kernel necessario può essere scaricato manualmente dagli archivi del sistema operativo del fornitore e quindi installato manualmente, oppure può essere aggiornato a una versione supportata e il comando di cui sopra ha tentato di nuovo.

Ad esempio, se non è possibile utilizzare CentOS e aggiornare il kernel a una versione supportata dalla distribuzione, i vecchi pacchetti .rpm per CentOS possono essere scaricati manualmente da <http://vault.centos.org>. Il nome del file da scaricare è fornito dall'output del seguente comando bash.

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

Una volta scaricato, il pacchetto kernel-devel può essere installato eseguendo il seguente comando bash nella directory in cui viene salvato il file .rpm scaricato.

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

# Oracle Linux

Oracle Linux distribuisce con due diverse alternative di kernel, RHCK e UEK. I pacchetti kernel-devel e kernel-uek-devel installano i file di intestazione di sviluppo del kernel necessari nella directory /usr/src/kernels su RHCK e UEK, rispettivamente. I file di sviluppo del kernel sono organizzati in /usr/src/kernel in base alla versione del kernel.

## Oracle Linux RHCK

La procedura per identificare il package del kernel mancante e risolvere l'ID errore 11 su Oracle Linux RHCK è identica a quella di RHEL Linux. Per ulteriori informazioni, fare riferimento alla sezione Linux di RHEL riportata sopra.

## Oracle Linux UEK

La procedura per identificare il pacchetto del kernel mancante e risolvere l'ID errore 11 su Oracle Linux UEK è simile, ma non identica, a quella di RHEL Linux. Fare riferimento alla sezione Linux di RHEL sopra per ulteriori informazioni ma sostituire ogni istanza di "kernel-devel" con "kernel-uek-devel". Per essere specifici, replacekernel-devel-\$(uname -r) withkernel-uek-devel-\$(uname -r)per ogni comando pertinente.

**NOTA:** se non è possibile trovare il package .rpm kernel-ek-devel necessario durante il tentativo di installazione dal repository dnf, il package può essere scaricato manualmente e installato dagli archivi Oracle all'indirizzo <https://yum.oracle.com/>.

# Debian/Ubuntu Linux

Il pacchetto linux-headers installa i file di intestazione necessari nella directory /usr/src, organizzati in base alla versione del kernel.

## Cause

Manca il pacchetto linux-headers necessario per il monitoraggio in tempo reale del file system e dell'attività di rete.

È possibile confermare le intestazioni installate nella directory /usr/src.

## Risoluzione

Il pacchetto linux-headers può essere installato con il seguente comando:

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

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).