排除RHEL CentOS Oracle Linux上的Linux连接器兼容性故障

目录

简介

环境

- 连接器版本
- 操作系统
- 内核版本

问题

- 症状

分辨率

- 连接器升级

相关内容

- Linux操作系统兼容性
- Linux用户指南

简介

本文档介绍Cisco Secure Endpoint Linux连接器版本1.12.4及更低版本之间的不兼容性。

环境

在这些平台上，连接器看起来可以正常运行，但无法检测文件重命名和网络事件、Red Hat Enterprise Linux、CentOS和Oracle Linux 7.8。请升级到连接器版本1.12.5或更高版本，以恢复完整的事件检测。

此问题适用于以下各节中描述的连接器版本、操作系统和内核版本。

连接器版本

受影响的连接器版本为：

- 1.12.4及更低版本

操作系统

受影响的操作系统包括：

- Red Hat Enterprise Linux 7.8
- CentOS 7.8
- Oracle Linux 7.8(RHCK)

注意：连接器版本1.18.0及更高版本支持Oracle Unbreakable Enterprise Kernel(UEK)。

内核版本

受影响的内核版本为：

- 3.10.0-1127.el7.x86_64或更高版本

问题

在内核版本为3.10.0-1127.el7.x86_64或更高版本的Red Hat Enterprise Linux、CentOS和Oracle Linux 7.8上，Cisco Secure Endpoint Linux连接器版本1.12.4及更低版本不检测文件重命名和网络事件。

症状

使用以下症状确认问题：

- 在Cisco Secure Endpoint Console中，连接器不检测文件重命名和网络事件，并且不会显示在设备轨迹中。
- 在终端窗口中，运行命令sudo cat /var/log/messages | grep "kernel:ampnetworkflow:<info>_msg_send_offset:peer disconnected”。 该命令返回多个结果，指示连接器使用的ampnetworkflow内核模块出现故障。

```
sudo cat /var/log/messages | grep "kernel: ampnetworkflow:
```

```
_msg_send_offset: peer disconnected"
```

分辨率

连接器升级

完成以下步骤以确认问题、升级连接器并确认修复：

1. 确认终端上安装的连接器版本。如果连接器版本为1.12.4或更低版本，请继续执行下一步。
2. 确认运行的内核版本：

   在终端窗口中，运行命令uname -r。

   ```
   uname -r
   ```

   此命令返回3.10.0-1127.el7.x86_64或更高内核版本。如果命令返回此版本或更高版本，请继续执行下一步。

3. 将Cisco Secure Endpoint Linux连接器升级到版本1.12.5或更高版本。
4. 升级后，确认再次检测到File Rename和Network Events并显示在Device Trajectory中。
5. 确认ampnetworkflow错误不再出现在系统日志中：

   ```
   sudo cat /var/log/messages | grep "kernel: ampnetworkflow:

           _msg_send_offset: peer disconnected"
   ```

相关内容

Linux操作系统兼容性

- 打开Cisco Secure Endpoint Linux Connector OS兼容性文档

Linux用户指南

- 打开Cisco Secure Endpoint Linux Connector用户指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。