أستكشاف أخطاء معرف 11 وإصلاحها على نقطة نهاية SUSE Linux الآمنة

المحتويات

المقدمة

يصف هذا وثيقة العملية أن يحل Fault ID 11 من Secure Endpoint تشغيل SUSE Linux Enterprise 15 SP2 .

المتطلبات

واجهة سطر الأوامر (CLI) لكافة مستخدمي النظام، على الرغم من أن توفر بعض الأوامر يعتمد على تكوين النهج و/أو أذونات الجذر. والاوامر التي تعتمد عليها يكشف عنها في كل هذه المقالة.

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Linux Command Line
- Secure Endpoint

المكونات المستخدمة

أسست المعلومة يستعمل في الوثيقة على هذا برمجية صيغة:

- Secure Endpoint 1.20
- SUSE Linux Enterprise 15 SP2 Kernel الإصدار 5.3.18-24.96-default

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

تشغيل SUSE Linux Enterprise 15 Service Pack (SP) 2، مع إصدارات kernel الأكبر من أو تساوي 5.3.18، يستخدم الموصل eBPF وحدات مثالية لنظام الملفات في الوقت الفعلي ومراقبة الشبكة. يعرض الأمر eBPF الوحدات النمطية تحل محل لينكس Kernel الوحدات النمطية المستخدمة عند تشغيلها RHEL 6, RHEL 7, Oracle Linux 7 RHCK, Oracle Linux 7 UEK 5 وفي وقت سابق، و Amazon Linux 2 ولاة

4. 14 وأ ام لبق. نم لجأ Ubuntu رادصإلا 18.04 تارادصإلاو ةقحاللا، فضلا نع Debian 10 امو هدعب، eBPF تادحولا ةيلصألا.

قفاوتلل بسانملا، عقوملا عيمجتب ايئاقلت لصوملا موقي eBPF تادحولا ةيطمنلا يتلا نأ يجمربلا ليوحتلا اذه بلطتي .ماظنلا ىلع اهليغشتو اهليمحت لبق لصوملا اهمدختسي تقولا يف اهتيبثت مت kernel-devel يلاحلا عم قفاوتت يتلا kernel ريوطت سأر تافلم نوكت تادحولا eBPF عيمجتب لصوملا موقيو ،ةكبشلا ةبقارم نيكمت متيو filesystem يقيقحلا هذه نيكمت دنع يقيقحلا تقولا يف وأ لصوملا ليغشت اهيف متي ةرم لك يف ةيطمنلا تازيملا، كزجع نم ثيدحت جهنلا.

رفوتت ال :11 أطخلا فرعم لصوملا ديزي ،ةيلاحلا kernel-devel ةمزح ماظنلا دقتفي امدنع لمعت يتلا kernel ةاونل kernel-devel ةمزح تيبثتب مق .تافلملا ةبقارمو RealTime ةكبش ةلاح يف لمعي سكونيل لصوم نأ أطخلا اذه عم ةلكشملا .لصوملا ليغشت دعأ مث ايلاح أطخلا لح متي ىتح عقوتم وه امك لمعي ال هنأ ينعي ام ،ةروهدتم.

اهحالصإو ءاطخألا فاشكتسا

نإ نوكي أطخ 11 عفترم، دعب كلذ رهظي اذه أطخ لجس:

- ثحبلا نع روطس لجسلا يف لجس ماظنلا /var/log/messages ةهباشم هذهل:

init: cisco-amp pre-start: AMP kernel modules are not required on this kernel version '5.3.18-24.96-default'; skipping reinstalling kernel modules

ريشي لجسلا ىلإ نأ رادصإ kernel يلاحلا ىلع كيلمبمكويتر ال مدختسي تادحو kernel ل filesystem ةبقارمو ةكبشلا. يف تارادصإ kernel ربكألا نم وأ يواست 4.18، نإف filesystem متيو ةبقارم ةكبشلا مادختساب eBPF تادحولا ةيطمنلا.

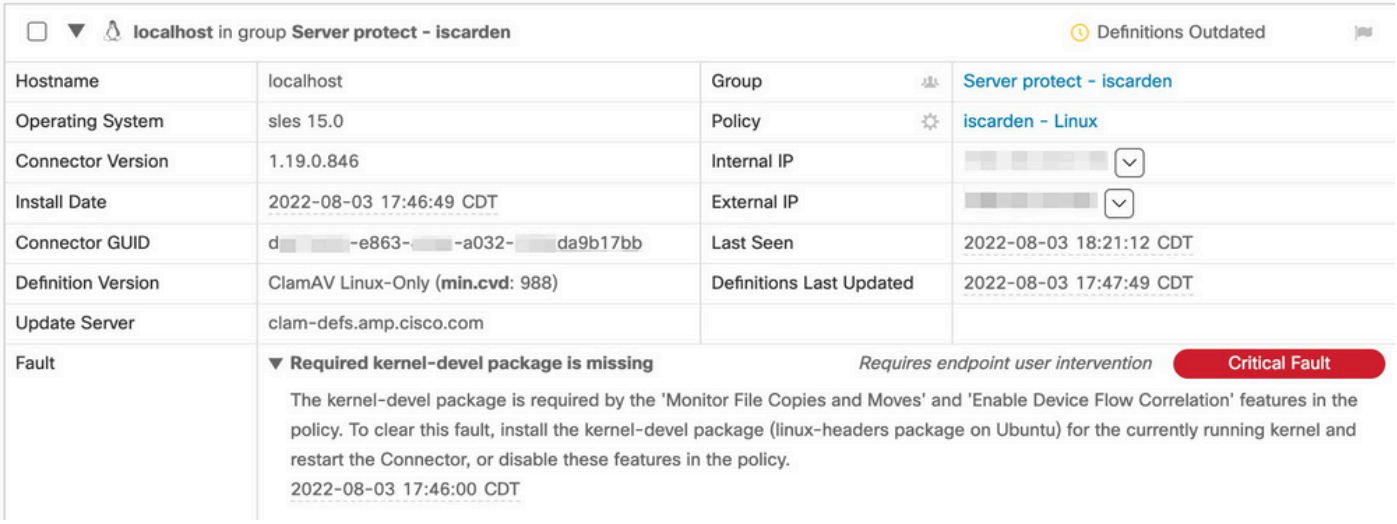
ةيفيك فيرعت سوؤر kernel ةبئاغلا

دنع ليغشت لصوملا ىلع زاهج كيلمبمكويتر نودب سوؤر kernel، Fault ID 11 (Realtime network and file monitoring is unavailable)، لصوملا لمعي يف ةلاح ةروهدتم نود filesystem وأ ةبقارم ةكبشلا. نكمي ذيفنت هذه تاوطخلا نم ةذفان ةيفرط ديدحتل ام اذإ ناك لصوملا kernel-header دوجوم وأ ال.

ةوطخلا 1. نم زاهجلا رثأتملا، دكأت نم نأ لصوملا هيدل Fault ID 11 :

```
# /opt/cisco/amp/bin/ampcli # status [logger] Set minimum reported log level to notice Trying to connect... Connected. Status: Connected Mode: Degraded Scan: Ready for scan Last Scan: 2022-08-03 06:31:42 PM Policy: iscarden - Linux (#22192) Command-line: Enabled Orbital: Disabled Faults: 1 Critical Fault IDs: 11           ID 11 - Critical: Realtime network and file monitoring is unavailable. Install the kernel-devel package for the currently running kernel, then, restart the Connector.
```

نم ةدحو مكحت ةطقن ةياهنلا ةنمآلا، رثعا ىلع زاهجلا رثأتملا عسوو ليصافتلا ققحتلل نم مسق "أطخلا".



الخطوة 2. تحقق من kernel الحالي باستخدام هذا الأمر:

$ uname -r 5.3.18-150200.24.115-default

الخطوة 3. للتحقق مما إذا كانت رؤوس الكبالت مثبتة أم ال:

zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//") # zypper se -s kernel-devel | grep $(uname -r | sed "s/-default//")

يجب أن يكون الإخراج كما يلي:

```
isaac@localhost:~> zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//")
i+ | kernel-default-devel | package | 5.3.18-24.96.1   | x86_64 | SLE-Module-Basesystem15-SP2-Updates
```

حيث يشير i+ إلى أن الحزمة مثبتة. إذا كان العمود الأيسر v وأ **فارغ**، يجب تثبيت الحزمة.

يعرض الأمر SUSE يناسب الكمبيوتر تثبيت رؤوس kernel إذا كانت جميع هذه العناوين صحيحة:

- يحتوي الموصل على معرف الخطأ 11.
- الحد الأدنى kernel الإصدار هو 5.3.18.
- يعرض الأمر kernel لم يتم تثبيت الرؤوس.

قرار

إذا SUSE لا يحتوي الجهاز على رؤوس kernel المطلوبة، ثم يمكن إستخدام هذا الإجراء لتثبيت رؤوس kernel المطلوبة على الجهاز.

الخطوة 1. تثبيت رؤوس kernel الضرورية:

sudo zypper install --oldpackage kernel-default-devel=$(uname -r | sed 's/-default//') # sudo zypper install --oldpackage kernel-devel=$(uname -r | sed 's/-default//')

الخطوة 2. أعد تشغيل الموصل:

sudo systemctl stop cisco-amp # sudo systemctl start cisco-amp

الخطوة 3. تأكد من مسح الخطأ:

```
# /opt/cisco/amp/bin/ampcli # status Trying to connect... Connected. ampcli> status Status: Connected Mode: Normal Scan: Ready for scan Last Scan: 2022-08-05 01:29:47 PM Policy: iscarden - Linux (#22201) Command-line: Enabled Orbital: Disabled Faults: None ampcli > quit
```

التحقق من الصحة

للتحقق من تثبيت رؤوس kernel الآن، قم بتشغيل الأوامر التالية:

```
# zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//") # zypper se -s kernel-devel | grep $(uname -r | sed "s/-default//")
```

قبل أن تقوم بالتبديل، كان لديك مخرجات مماثلة لهذا:

```
isaac@localhost:~> zypper se -s kernel-default-devel | grep $(uname -r | sed 's/
-default//') $ zypper se -s kernel-devel | grep $(uname -r | sed 's/-default//')
isaac@localhost:~>
```

بعد أن تقوم بالتبديل، يجب أن يكون المخرج مماثل لهذا:

```
isaac@localhost:~> zypper se -s kernel-default-devel | grep $(uname -r | sed "s/-default//")
i+ | kernel-default-devel | package | 5.3.18-24.96.1   | x86_64 | SLE-Module-Basesystem15-SP2-Updates
isaac@localhost:~> zypper se -s kernel-devel | grep $(uname -r | sed "s/-default//")
i | kernel-devel | package | 5.3.18-24.96.1   | noarch | SLE-Module-Basesystem15-SP2-Updates
isaac@localhost:~>
```

معلومات ذات صلة

- تحقق من توافق نظام تشغيل موصل Linux الآمن
- أخطاء Linux Kernel-Devel
- بناء الوحدات النمطية لنواة نقطة النهاية الآمنة Cisco Secure Endpoint Connector Linux Kernel Modules

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).