أستكشاف أخطاء موصل نقطة النهاية الآمنة 18 وإصلاحها

المحتويات

المقدمة

يصف هذا المستند الخطأ 18 على موصل Secure Endpoint Linux.

الخطأ 18: تم تحميل مراقبة حدث الموصل بشكل زائد

يعمل محرك الحماية السلوكية على تحسين إمكانية رؤية الموصلات في نشاط النظام. مع ماظن ةردق يف ماظنلا يف ةطشنألا ددع قوفي نأ ديازتي لامتحا كانه ،ةيؤرلا يف ةدايزلا هذه الموصل على المراقبة. إذا حدث هذا، الموصل يرفع الخطأ 18 ويدخل في الوضع المخفض. ارجع إلى مقالة [أخطاء موصل نقطة النهاية الآمنة Cisco Secure Endpoint Linux] للحصول على تفاصيل حول الخطأ 18. في موصل لينوكس status يمكن إستخدام الأمر في واجهة سطر الأوامر (CLI) لنقطة النهاية الآمنة لنظام التشغيل Linux لمعرفة ما إذا كان الموصل يعمل في الوضع المخفض وما إذا كان قد تم رفع أي أخطاء. إذا كان الخطأ 18 مرفوعا، ثم يتم تشغيل status يعرض الأمر في واجهة سطر الأوامر (CLI) لنقطة النهاية الآمنة Secure Endpoint الخطأ بإحدى هاتين الحالتين المحتملتين:

1. الخطأ 18 ذو الخطورة الكبرى

```
ampcli> status
Status:                   Connected
Mode:                     Degraded
Scan:                     Ready for scan
Last Scan:                2023-06-19 02:02:03 PM
Policy:                   Audit Policy for FireAMP Linux (#1)
Command-line:             Enabled
Orbital:                  Disabled
Behavioural Protection:   Protect
Faults:                   1 Major
Fault IDs:        18
                  ID 18 - Major: Connector event monitoring is overloaded. Investigate the most acti
```

2. الخطأ 18 مع خطورة خطيرة

```
ampcli> status
Status:                  Connected
Mode:                    Degraded
Scan:                    Ready for scan
Last Scan:               2023-06-19 02:02:03 PM
Policy:                  Audit Policy for FireAMP Linux (#1)
Command-line:            Enabled
Orbital:                 Disabled
Behavioural Protection: Protect
Faults:                  1 Critical
Fault IDs:      18
                ID 18 - Critical: Connector event monitoring is overloaded. Investigate the most a
```

تم تحميل مراقبة حدث الموصل بشكل زائد: الخطورة الكبرى

عندما يتم رفع الخطأ 18 مع خطورة كبرى، فهذا يعني أن مراقبة حدث الموصل يتم تحميلها فوق طاقتها ولكنها ما زالت قادرة على مراقبة مجموعة أصغر من أحداث النظام. يتحول الموصل إلى مستوى خطورة كبير ويقوم بمراقبة الأحداث الأقل التي تواجي المراقبة التي كانت متوفرة في الموصلات الأقدم من 1.22.0. إذا كان فيض أحداث النظام قصيرا وتراجع حمل مراقبة الحدث مرة أخرى في نطاق مقبول، فيتم مسح الخطأ 18 ويواصل الموصل مراقبة جميع أحداث النظام. إذا أزداد فيض أحداث النظام سوءا وازدادت حمولة مراقبة الحدث إلى حد خطير، حينئذ يتم رفع الخطأ 18 بشدة شديدة ويحول الموصل إلى [خطورة حرجة](#).

تم تحميل مراقبة حدث الموصل بشكل زائد: الخطورة الحرجة

عندما يتم رفع الخطأ 18 مع خطورة بالغة، فهذا يعني أن الموصل يواجه قدرا هائلا من أحداث النظام التي تعرض الموصل للخطر. يتحول الموصل إلى خطورة حرجة أكثر تقييدا. في هذه الحالة، يراقب الموصل فقط الأحداث الهامة للسماح للموصل بالتنظيف والتركيز على الاسترداد. إذا تراجع فيض الأحداث في نهاية المطاف ليصل إلى نطاق أكثر قبولا، فسيتم مسح الخطأ بالكامل وسيستأنف الموصل مراقبة جميع أحداث النظام.

توجيه فعل الصدع

إذا كان الموصل قد تسبب في حدوث خطأ 18 إما بدرجة خطورة كبيرة أو خطيرة، فيجب إتخاذ بعض الخطوات للتحقيق في المشكلة وحلها. تختلف خطوات حل الخطأ 18 حسب الوقت والسبب الذي نشأ فيه الخطأ:

1. تم رفع خطأ 18 على تثبيت جديد لموصل ليونكس
2. حدث الخطأ 18 بعد التغييرات الأخيرة التي تم إجراؤها على نظام التشغيل
3. الصدع 18 نشأ تلقائيا

4. تم رفع الخطأ 18 عند إعادة إمداد جهاز بموصل Linux المثبت بالفعل أو تحديث الموصل إلى الإصدار 1.22.0+

الحالة 1: التثبيت الجديد

إذا تم مالحظة وجود عطل 18 والوضع المخفض خارج النظام من خالل التثبيت الجديد لموصل ليونكس، فيجب عليك أوال التأكد من أن النظام الذي يحوزتك في باحد الأدنى لمتطلبات النظام. بعد التحقق من استيفاء المتطلبات للحد الأدنى من المتطلبات أو تجاوزها، إذا استمر الخطأ، يجب عليك التحقيق في العمليات الأكثر نشاطا على النظام. يمكنك عرض العمليات النشطة الحالية على نظام ليونكس باستخدام top الأمر (أو ما شابه) في الوحدة الطرفية. إذا كان من المعروف أن العمليات التي تستهلك أعلى كمية من وحدة المعالجة المركزية حميدة، فيمكنك إنشاء استبعادات جديدة للعملية الستبعاد تلك العمليات من أن يتم مراقبتها.

مثال سيناريو:

لنفترض أنه بعد التركيب الجديد، تم عرض الخطأ 18 والوضع المخفض عبر واجهة سطر الأوامر لنقطة النهاية الآمنة Linux. Rإزالة top يعرض الأمر في جهاز Ubuntu هذه العمليات النشطة:

```
Tasks: 223 total,   5 running, 218 sleeping,   0 stopped,   0 zombie
%Cpu(s): 29.4 us, 34.3 sy,  0.0 ni, 36.2 id,  0.0 wa,  0.0 hi,  0.1 si,  0.0 st
MiB Mem :   7943.0 total,   3273.9 free,   2357.6 used,   2311.5 buff/cache
MiB Swap:   2048.0 total,   2048.0 free,      0.0 used.   5141.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  34896 user1     20   0   18136   3292   3044 R  96.7   0.0   0:04.89 trusted_process
   4296 user1     20   0  823768  52020  38900 R  48.0   0.6   0:10.90 gnome-terminal-
    117 root      20   0       0      0      0 I  12.3   0.0   0:01.86 kworker/u64:6-events_unbound
  34827 root      20   0       0      0      0 I  10.3   0.0   0:00.47 kworker/u64:2-events_unbound
   1880 user1     20   0  353080 101600  70164 S   6.3   1.2   0:30.37 Xorg
  34576 root      20   0       0      0      0 R   6.3   0.0   0:01.46 kworker/u64:1-events_unbound
   2089 user1     20   0 3939120 251332 104008 S   3.0   3.1   0:23.25 gnome-shell
    132 root      20   0       0      0      0 I   1.3   0.0   0:02.67 kworker/2:2-events
   6951 root      20   0 1681560 213536  74588 S   1.3   2.6   0:41.30 ampdaemon
    741 root      20   0  253648  13352   9280 S   0.3   0.2   0:01.54 polkitd
    969 root      20   0  153600   3788   3512 S   0.3   0.0   0:00.36 prlshprint
   2291 user1     20   0  453636  29388  20060 S   0.3   0.4   0:03.75 prlcc
      1 root      20   0  169608  13116   8524 S   0.0   0.2   0:01.95 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
```

نرى أنه هناك عملية نشطة جدا تسمى trusted_process في هذا المثال. في هذه الحالة أنا على دراية بهذه العملية وهي موثوق بها، ال يوجد سبب للشك في هذه العملية. لمسح الخطأ 18، يمكن إضافة العملية الموثوق بها إلى إستثناء عملية في المدخل. ارجع إلى مقالة تكوين استثناءات نطاق نهاية المأمن من Cisco والتعرف عليها للتعرف على أفضل الممارسات عند إنشاء االستثناءات.

الحالة 2: التغييرات الأخيرة

إذا قمت بإجراء تغييرات حديثة على نظام التشغيل الخاص بك، مثل تثبيت برنامج جديد، يمكن ملاحظة وجود خطأ 18 ووضع مخفض إذا أدت هذه التغييرات الجديدة إلى زيادة نشاط النظام. أستخدم نفس إستراتيجية المعالجة الموضحة في التثبيت الجديد مع ذلك، ابحث في الحالة عن العمليات المرتبطة بالتغييرات الأخيرة، مثل عملية جديدة تم تشغيلها بواسطة برنامج مثبت حديثا.

الحالة 3: نشاط ضار

يزيد محرك الحماية السلوكية أنواع نشاط النظام الذي تم مراقبته. وهذا يوفر للموصل وعي أوسع حول النظام ويمنحه القدرة على اكتشاف الهجمات السلوكية الأكثر تعقيدا. ومع ذلك، فإن مراقبة مقدار أكبر من نشاط النظام يعرض الموصل لخطر أكبر لهجمات رفض الخدمة (DoS). إذا كان الموصل مثقل بنشاط النظام ودخل في وضع متدني مع حدوث الخطأ 18، فإنه يستمر في مراقبة الأحداث الحرجة للنظام حتى يتم تقليل نشاط النظام الكلي. يؤدي هذه الفقدان في رؤية أحداث النظام إلى تقليل قدرة الموصل على حماية النظام بشكل فعال. من المهم للغاية أن تتحقق من النظام بحثا عن العمليات الضارة. أستخدم top وقم بتشغيل (أو ما شابه) على نظام لينوكس لعرض العمليات النشطة الحالية، وقم باتخاذ الإجراء المناسب لتصحيح الوضع إذا تم التعرف على أي عمليات قد تكون ضارة.

القضية 4: متطلبات الموصل

يحسن محرك الحماية السلوكية من قدرة الموصل على حماية نشاط الجهاز، ولكن للقيام بذلك، يجب أن يستهلك موارد أكثر من الإصدارات السابقة. إذا كان الخطأ 18 يتم رفعه بشكل متكرر، فلا توجد عمليات حميدة تتسبب في حمل ثقيل، ولا يبدو أنه هناك أي عمليات ضارة تعمل على الجهاز، ثم يجب عليك التأكد من أن النظام الخاص بك في الحد الأدنى لمتطلبات النظام.

اطّلع أيضاً على

- استخدام واجهة سطر الأوامر (CLI) الخاصة بنقطة النهاية الآمنة Mac/Linux
- أخطاء موصل Cisco Secure Endpoint Linux
- تكوين استيعابات نقاط النهاية الآمنة من Cisco والتعرف عليها
- دليل مستخدم نقطة النهاية الآمنة (PDF)

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).