تنبيهات FTD الأساسية الخاصة بوحدة المعالجة المركزية (CPU) عالية من عملية pruner.pl

مسألة

تقوم وحدة التحكم في إدارة الهيكل (FMC) بإنشاء تنبيهات لاستخدام وحدة المعالجة المركزية (CPU) بشكل متكرر وبمستوى عال للأجهزة المتعددة التي تتم إدارتها في برنامج الإرسال فائق السرعة (FTD)، كما تثير المخاوف حول أداء جدار الحماية واستقراره. وعلى وجه التحديد، تظهر مراقبة الصحة التابعة لـ FMC زيادات أساسية متكررة لوحدة المعالجة المركزية على مراكز معينة على مدى فترات ممتدة، حيث تستهلك عملية الخلفية Pruner.pl الداخلية بشكل مستمر وحدة المعالجة المركزية (CPU) الزائدة للمراكز المحددة. وعلى الرغم من ظهور تنبيهات وحدة المعالجة المركزية (CPU) الهامة هذه في وحدة التحكم في إدارة اللوحة الأساسية (FMC)، فإنه لا يتم ملاحظة أي تأثير حركة مرور مرئي للمستخدم، كما أن الاستقرار الكلي في برنامج الإرسال فائق السرعة (FTD) لا يزال غير متأثر.

البيئة

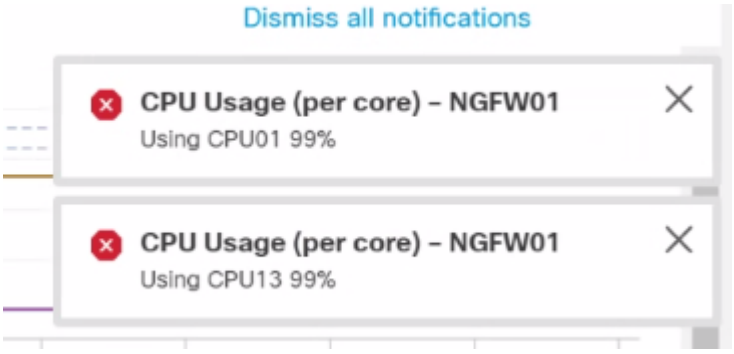
- إصدار برنامج FTD: 7-2-5 (تؤثر على كل من النماذج الافتراضية ونماذج الأجهزة في 7-2-6 وجميع الإصدارات الأقل من 7-2-6)
- الأجهزة التي تتم إدارتها بواسطة مركز إدارة FirePOWER (FMC)

قرار

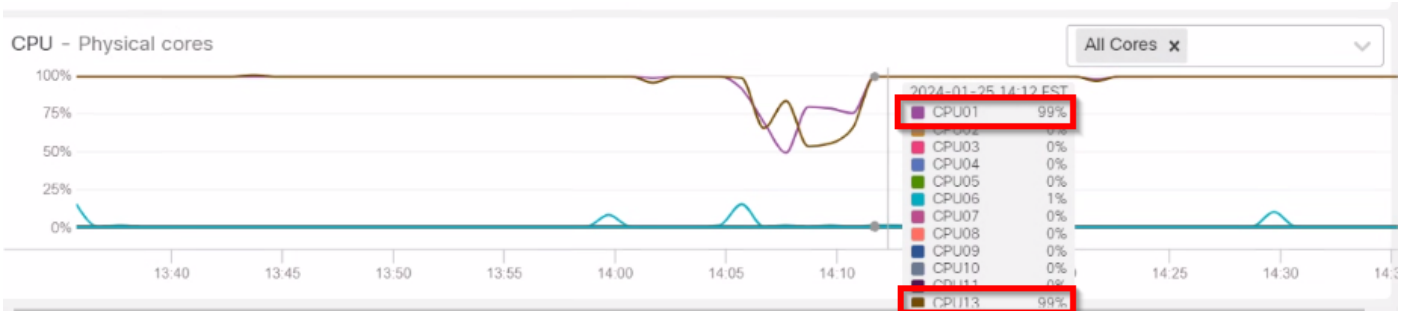
يتضمن الحل ترقية أجهزة FTD المتأثرة إلى إصدار برنامج يحتوي على الإصلاح للعيب المحدد.

خطوات أستكشاف الأخطاء وإصلاحها والتحليل

1: فحص أنماط إستخدام وحدة المعالجة المركزية (CPU) في الرسومات البيانية ل "مراقبة سلامة برنامج FTD" عبر الوقت لتحديد نطاق المشكلة وتوقيتها. ويكشف التحليل عن زيادات أساسية متكررة لوحدة المعالجة المركزية (CPU) على نوى محددة، بينما ظل إستخدام وحدة المعالجة المركزية (CPU) والذاكرة بشكل عام ضمن نطاقات التشغيل العادية.



inline_image_0.png



inline_image_1.png

```
Health Monitor Alert | Time: Mon Jul 24 06:34:20 2023 UTC | Severity: critical | Module: CPU Usage (per
Health Monitor Alert | Time: Mon Jul 24 04:24:20 2023 UTC | Severity: critical | Module: CPU Usage (per
```

2: تحليل واجهة سطر الأوامر (CLI) الخاصة ب FTD واستكشاف أخطاء حزم FTD المتأثرة وإصلاحها لتحديد السبب الرئيسي لاستخدام وحدة المعالجة المركزية (CPU) بشكل كبير.

3: مراجعة البيانات المجمعة لتحديد العمليات التي تستهلك موارد وحدة المعالجة المركزية (CPU) الزائدة. أكد تحليل ملفات top.log أن عملية pruner.pl كانت تستخدم CPU مرتفع بشكل ثابت على مراكز معينة، مع بداية نمط الإصدار حول إطار زمني محدد.

```
                                                root@FTDdevice:/home/admin# cd /ngfw/var/log/
        root@FTDdevice:/ngfw/var/log# grep "Pruner.pl --persistent" top.log | grep -v "S   0.0"
12341 root      20   0  458920 437816  10056 R 100.0   0.2   9452:10 /usr/bin/perl /ngfw/usr/local/sf/
12341 root      20   0  437124 416148  10056 R 100.0   0.2   9453:13 /usr/bin/perl /ngfw/usr/local/sf/
12341 root      20   0  437124 416148  10056 R 100.0   0.2   9454:13 /usr/bin/perl /ngfw/usr/local/sf/
12341 root      20   0  437124 416148  10056 R  94.1   0.2   9455:15 /usr/bin/perl /ngfw/usr/local/sf/
12341 root      20   0  437124 416148  10056 R 100.0   0.2   9456:18 /usr/bin/perl /ngfw/usr/local/sf/
```

كما تظهر السجلات عددا كبيرا من الملفات الفارغة ذات 0 بايت"*snort-unified.log" التي هي السبب الرئيسي لتشغيل pruner.pl بشكل متكرر.

```
root@FTDdevice:/home/admin# cd /ngfw/var/sf/detection_engines/FTD-UUID/
root@FTDdevice:/ngfw/var/sf/detection_engines/FTD-UUID# ls -l instance-* | grep -ri "root       0.snor
-rw-r--r--  1 root    root        0 Nov 12 19:47 snort-unified.log.1699818430
-rw-r--r--  1 root    root        0 Nov 12 19:41 snort-unified.log.1699818093
-rw-r--r--  1 root    root        0 Nov 12 19:35 snort-unified.log.1699817758
-rw-r--r--  1 root    root        0 Nov 12 17:13 snort-unified.log.1699809226
-rw-r--r--  1 root    root        0 Nov 12 17:08 snort-unified.log.1699808890
-rw-r--r--  1 root    root        0 Nov 12 17:02 snort-unified.log.1699808554
```

حل ترقية البرامج

1: ترقية جميع أجهزة FTD المتأثرة إلى إصدار برنامج يحتوي على الإصلاح ل CSCwh79095. أقل الإصدارات الموصى بها هي:

- برنامج FTD 7. 2. 7 (الحد الأدنى لإصدار الإصلاح في قطار 7. 2.x)
- FTD 7.4.1 أو إصدار أحدث (مسار ترقية مستحسن)

2: بعد الترقية، قم بمراقبة تنبيهات حماية FMC لتأكيد ما يلي:

- ظل إستخدام وحدة المعالجة المركزية (CPU) لكل مركز ثابتا
- لم يتم رفع أي تنبيهات حرجة جديدة لعمليات Pruner.pl أو الخلفية المماثلة
- لم تعد تنبيهات وحدة المعالجة المركزية (CPU) عالية لعملية Pruner.pl تحدث

الوقاية وأفضل الممارسات

تنفيذ هذه التوصيات لمنع حدوث مشاكل مماثلة:

- تجنب تشغيل الشفرة القديمة التي تدرب الترقيات طويلة المدى وتخطط للترقيات الدورية للإصدارات الموصى بها للاستفادة من إصلاح الأخطاء وتحديثات الأمان
- قبل الترقيات الرئيسية، راجع ملاحظات إصدار Cisco وأجرى عمليات بحث عن الأخطاء المعروفة في الإصدارات الحالية والهدف
- متابعة مراقبة تنبيهات الحماية من FMC بعد إجراء عمليات الترقية لضمان إستقرار النظام

- مراجعة أي اعتبارات خاصة للترقية تم توثيقها في ملاحظات الإصدار

السبب

تحدث تنبيهات وحدة المعالجة المركزية (CPU) العالية بسبب عيب في البرنامج في FTD. هذا العيب ناتج عن خطأ من Cisco. يرجع السبب في هذه المشكلة إلى معرف تصحيح الأخطاء من Cisco CSCwh79095 لمعرف باسم 7.2.5 إلى ملفات snort-unified.log الفارغة ذات 0 بايت التي تتسبب في إستهلاك عملية الخلفية ل Pruner.pl الداخلية لوحدة المعالجة المركزية (CPU) الزائدة على نوى محددة. وهذا يؤدي إلى تشغيل تنبيهات مستمرة لوحدة المعالجة المركزية (CPU) في FMC. المهم، ال يؤثر هذا الشرط على إعادة توجيه حركة مرور مستوى البيانات أو الاستقرار العام للجهاز؛ فهو يقوم بإنشاء تنبيهات وحدة المعالجة المركزية (CPU) العالية فقط في واجهة الإدارة. المشكلة هي أخطاء متكررة ذات صلة بما في ذلك CSCwe66384 (Pruner.pl و Disk Manager high CPU بدون مشاكل واضحة في القرص) و CSCwf80946 (FTD: عملية تقليم باستخدام مراكز وحدات المعالجة المركزية (CPU) المفرطة في النظام وتوليد تنبيهات FMC HM).

المحتوى ذي الصلة

- معرف تصحيح الأخطاء من Cisco CSCwh79095 - Snort الذي يقوم بإنشاء عدد مفرط من ملفات السجل الموحدة التي لا توجد بها أية وحدات بايت (ثابت في: 7.6.0 و 7.4.1 و 7.2.7)
- معرف تصحيح الأخطاء من Cisco CSCwf77994 - تنبيهات وحدة المعالجة المركزية (CPU) العالية الخاطئة الحرجة لمراكز أنظمة أجهزة FTD التي تقوم بتشغيل الاستخدام العالي للفوري (ثابت في: 7.6.0 و 7.4.1 و 7.2.9)
- ملاحظات إصدار FTD/FMC ووثائق الإصدارات الموصى بها
- [الدعم الفني والتنزيلات من Cisco]

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).