FTD High CPU Core Warnungen von Pruner.pl Prozess

Problem

FMC generiert häufige Warnmeldungen bezüglich der CPU-Auslastung für mehrere verwaltete FTD-Geräte und gibt Anlass zu Bedenken hinsichtlich der Leistung und Stabilität der Firewall. Insbesondere zeigt der FMC-Integritätsmonitor wiederholte CPU-Core-Spitzen auf bestimmten Cores über längere Zeiträume an, wobei der interne Hintergrundprozess von Pruner.pl ständig übermäßig viel CPU für die angegebenen Cores verbraucht. Trotz dieser kritischen CPU-Warnungen, die in FMC angezeigt werden, wurden keine Auswirkungen auf den vom Benutzer sichtbaren Datenverkehr beobachtet, und die FTD-Stabilität bleibt insgesamt unbeeinträchtigt.

Umwelt

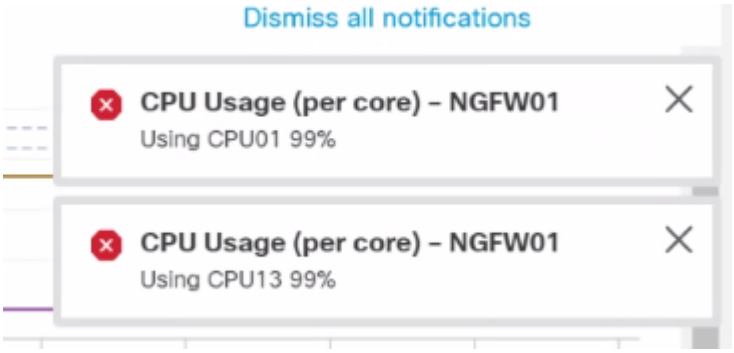
- FTD-Softwareversion: 7.2.5 (betrifft sowohl virtuelle als auch Hardwaremodelle in allen Versionen unter 7.2.6)
- Vom FirePOWER Management Center (FMC) verwaltete Geräte

Auflösung

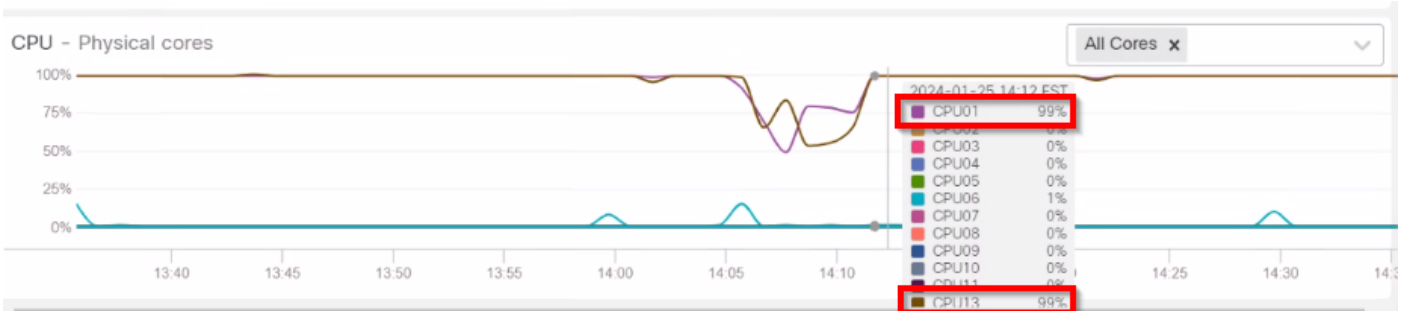
Die Lösung beinhaltet die Aktualisierung der betroffenen FTD-Geräte auf eine Softwareversion, die die Behebung des identifizierten Fehlers enthält.

Schritte zur Fehlerbehebung und Analyse

1: Untersuchen Sie die CPU-Auslastungsmuster in den FTD Health Monitor-Diagrammen im Laufe der Zeit, um den Umfang und das Timing des Problems zu identifizieren. Die Analyse zeigt wiederholte CPU-Core-Spitzen auf bestimmten Cores, während die CPU- und Speichernutzung insgesamt innerhalb normaler Betriebsbereiche blieb.



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: Analyse der FTD-CLI und Fehlerbehebung bei Paketen der betroffenen FTD, um die Ursache für eine hohe CPU-Auslastung zu ermitteln.

3: Überprüfen Sie die erfassten Daten, um festzustellen, welche Prozesse zu viele CPU-Ressourcen verbrauchen. Die Analyse der top.log Dateien bestätigte, dass der Pruner.pl Prozess konsistent hohe CPU auf bestimmten Cores verwendet, wobei das Problem Muster um einen bestimmten Zeitraum begann.

```
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/
```

Die Protokolle zeigen auch eine hohe Anzahl von leeren, 0-Byte"*snort-unified.log" Dateien, die der Hauptgrund für die so oft laufende Pruner.pl sind.

```
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
```

Software-Upgrade-Lösung

1: Führen Sie für alle betroffenen FTD-Geräte ein Upgrade auf eine Softwareversion durch, die den Fix für CSCwh79095 enthält. Die empfohlenen Mindestversionen sind:

- FTD 7.2.7 (Mindestversion für Fehlerbehebung in 7.2.x Train)
- FTD 7.4.1 oder höher (empfohlener Upgrade-Pfad)

2: Überwachen Sie nach dem Upgrade die FMC-Integritätswarnungen, um Folgendes zu bestätigen:

- CPU-Auslastung pro Core bleibt stabil
- Für Pruner.pl oder ähnliche Hintergrundprozesse werden keine neuen kritischen Alarme ausgelöst
- Hohe CPU-Warnungen für den Pruner.pl-Prozess treten nicht mehr auf

Prävention und Best Practices

Implementieren Sie diese Empfehlungen, um ähnliche Probleme zu vermeiden:

- Vermeidung der langfristigen Ausführung älterer Code-Schulungen und Planung regelmäßiger Upgrades auf empfohlene Versionen, um von Bugfixes und Sicherheits-Updates zu profitieren
- Überprüfen Sie vor größeren Upgrades die Versionshinweise von Cisco, und suchen Sie bei aktuellen und Zielversionen nach bekannten Fehlern.
- Weitere Überwachung von FMC-Integritätswarnungen nach Upgrades zur Gewährleistung der Systemstabilität
- Lesen Sie die Versionshinweise unter "Spezielle Überlegungen zu Upgrades".

Ursache

Die hohen CPU-Warnungen werden durch einen Softwarefehler in FTD 7.2.5 verursacht, der als Cisco Bug-ID CSCwh79095 identifiziert wurde. Dieser Fehler ist auf leere, 0-Byte-Datei "snort-unified.log" zurückzuführen, die bewirkt, dass der interne Hintergrundprozess "Pruner.pl" übermäßig viel CPU auf bestimmten Cores verbraucht. Dies löst anhaltende CPU-intensive Alarme in FMC aus. Wichtig ist, dass dieser Zustand die Weiterleitung des Datenverkehrs auf Datenebene und die Stabilität der gesamten Geräte nicht beeinträchtigt. Es werden nur kritische CPU-Warnungen in der Management-Schnittstelle generiert. Das Problem ist mit doppelten Bugs verbunden, einschließlich CSCwe66384 (Pruner.pl und hohe CPU des Festplattenmanagers ohne offensichtliche Probleme mit der Festplatte) und CSCwf80946 (FTD: Pruner-Prozess mit übermäßig hohen System-CPU-Kernen und Generierung von FMC (HM-Warnungen).

Verwandte Inhalte

- Cisco Bug-ID CSCwh79095 - Snort erzeugt eine übermäßige Anzahl von snort-einheitlichen Protokolldateien mit null Bytes (Behoben in: 7.2.7, 7.4.1, 7.6.0)
- Cisco Bug-ID CSCwf77994 - Falsch kritische CPU-Warnungen für FTD-Gerätesystemkerne mit sofortiger hoher Auslastung (behoben in: 7.2.9, 7.4.1, 7.6.0)
- FTD/FMC Versionshinweise und empfohlene Versionen Dokumentation
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.