Avvisi FTD High CPU Core da Pruner.pl Process

Problema

FMC genera frequenti avvisi di elevato utilizzo della CPU per più dispositivi FTD gestiti e solleva preoccupazioni sulle prestazioni e la stabilità del firewall. In particolare, il monitoraggio dello stato del CCP mostra ripetuti picchi di core della CPU su core specifici per periodi prolungati, con il processo di background interno Pruner.pl che consuma costantemente una quantità eccessiva di CPU per i core specificati. Nonostante questi avvisi critici della CPU vengano visualizzati in FMC, non viene osservato alcun impatto sul traffico visibile all'utente e la stabilità complessiva del FTD rimane invariata.

Ambiente

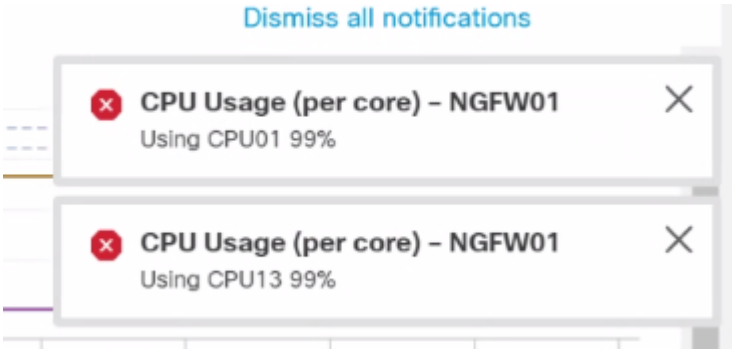
- Versione software FTD: 7.2.5 (riguarda sia i modelli virtuali che i modelli hardware in tutte le versioni precedenti alla 7.2.6)
- Dispositivi gestiti da Firepower Management Center (FMC)

Risoluzione

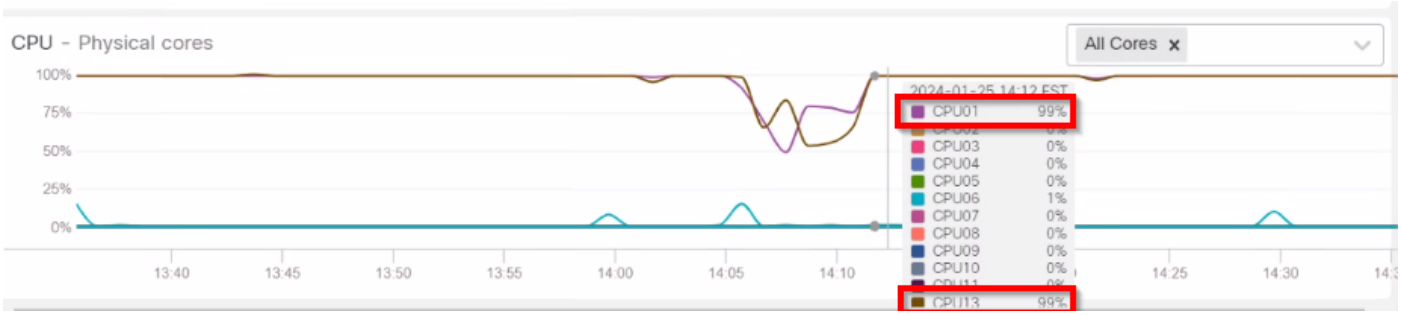
La risoluzione implica l'aggiornamento dei dispositivi FTD interessati a una versione software che contiene la correzione per il difetto identificato.

Fasi di risoluzione dei problemi e analisi

1: Esaminare i modelli di utilizzo della CPU nei grafici di Health Monitor FTD nel tempo per identificare l'ambito e i tempi del problema. L'analisi rivela i ripetuti picchi dei core della CPU su core specifici che si verificano, mentre l'utilizzo complessivo della CPU e della memoria è rimasto entro i normali intervalli operativi.



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: Analisi della CLI FTD e risoluzione dei problemi dei bundle dall'FTD interessato per identificare la causa principale dell'elevato utilizzo della CPU.

3: Esaminare i dati raccolti per identificare i processi che utilizzano risorse CPU eccessive. L'analisi dei file top.log ha confermato che il processo Pruner.pl utilizza sempre una CPU elevata su determinati core, con il modello di problema che inizia in un intervallo di tempo specifico.

```
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/
```

I log mostrano anche un numero elevato di file vuoti, 0-byte"*snort-unified.log" che sono la ragione principale per il funzionamento di Pruner.pl così spesso.

```
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
```

Soluzione di aggiornamento software

1: Aggiornare tutti i dispositivi FTD interessati a una versione software contenente la correzione per CSCwh79095. Le versioni minime consigliate sono:

- FTD 7.2.7 (versione minima fissa nel treno 7.2.x)
- FTD 7.4.1 o versione successiva (percorso di aggiornamento consigliato)

2: Dopo l'aggiornamento, monitorare gli avvisi di integrità di FMC per verificare che:

- L'utilizzo della CPU per core rimane stabile
- Non vengono generati nuovi allarmi critici per Pruner.pl o processi simili in background
- Allarmi CPU elevati per il processo Pruner.pl non si verificano più

Prevenzione e best practice

Implementare queste raccomandazioni per evitare problemi simili:

- Evitare di eseguire code train meno recenti a lungo termine e pianificare aggiornamenti periodici delle versioni consigliate per trarre vantaggio dalle correzioni dei bug e dagli aggiornamenti della sicurezza
- Prima di eseguire gli aggiornamenti principali, esaminare le note sulla versione di Cisco ed eseguire ricerche dei bug per rilevare i difetti noti sulle versioni corrente e di destinazione
- Continuare a monitorare gli avvisi di integrità FMC dopo gli aggiornamenti per garantire la stabilità del sistema
- Esaminare eventuali considerazioni speciali sull'aggiornamento documentate nelle note di rilascio

Causa

Gli alert elevati sulla CPU sono causati da un difetto del software in FTD 7.2.5 identificato come Cisco Bug ID CSCwh79095. Questo difetto è dovuto a file snort-unified.log vuoti e a 0 byte, che fanno sì che il processo in background Pruner.pl interno utilizzi una CPU eccessiva su core specifici. In questo modo vengono attivati gli allarmi persistenti relativi a CPU elevate in FMC. È importante sottolineare che questa condizione non influisce sull'inoltro del traffico del piano dati o sulla stabilità complessiva del dispositivo; genera solo avvisi critici sulla CPU nell'interfaccia di gestione. Il problema è dovuto a bug duplicati correlati, tra cui CSCwe66384 (Pruner.pl e gestione dischi con CPU elevata senza problemi evidenti) e CSCwf80946 (FTD: Eliminare i processi utilizzando core CPU di sistema eccessivi e generando avvisi HM di FMC).

Contenuto correlato

- Cisco Bug ID CSCwh79095 - Snort che genera un numero eccessivo di file di log unificati con zero byte (risolto in: 7.2.7, 7.4.1, 7.6.0)
- Cisco Bug ID CSCwf77994 - Falsi avvisi critici della CPU elevata per i core di sistema del dispositivo FTD con elevato utilizzo istantaneo (risolti in: 7.2.9, 7.4.1, 7.6.0)
- Note sulla release di FTD/FMC e documentazione sulle release consigliate
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).