# Pruner.pl 프로세스의 FTD 높은 CPU 코어 경고

## 문제

FMC는 관리되는 여러 FTD 디바이스에 대해 자주 높은 CPU 사용률 경고를 생성하며 방화벽 성능 및 안정성에 대한 우려를 제기합니다. 특히, FMC 상태 모니터는 특정 코어에서 오랜 기간 동안 CPU 코어 스파이크가 반복적으로 발생하는 것을 보여주며, 내부 Pruner.pl 백그라운드 프로세스는 지정된 코어에서 지속적으로 과도한 CPU를 소비합니다. FMC에 나타나는 이러한 중요한 CPU 경고에도 불구하고 사용자가 볼 수 있는 트래픽 영향은 관찰되지 않으며 전체적인 FTD 안정성은 영향을 받지 않습니다.

## 환경

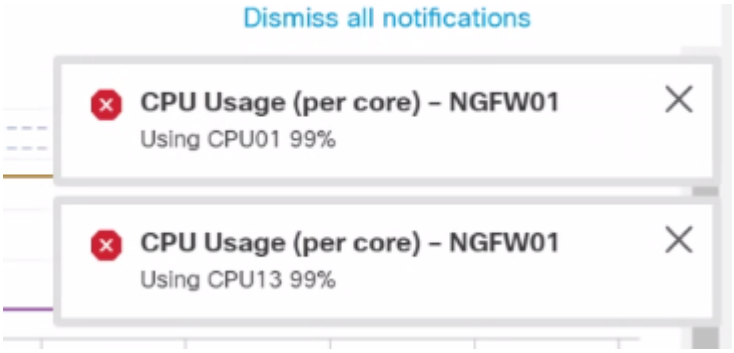
- FTD 소프트웨어 버전: 7.2.5(7.2.6 미만의 모든 버전에서 가상 및 하드웨어 모델에 모두 영향)
- FMC(Firepower 관리 센터)에서 관리되는 디바이스

## 해결

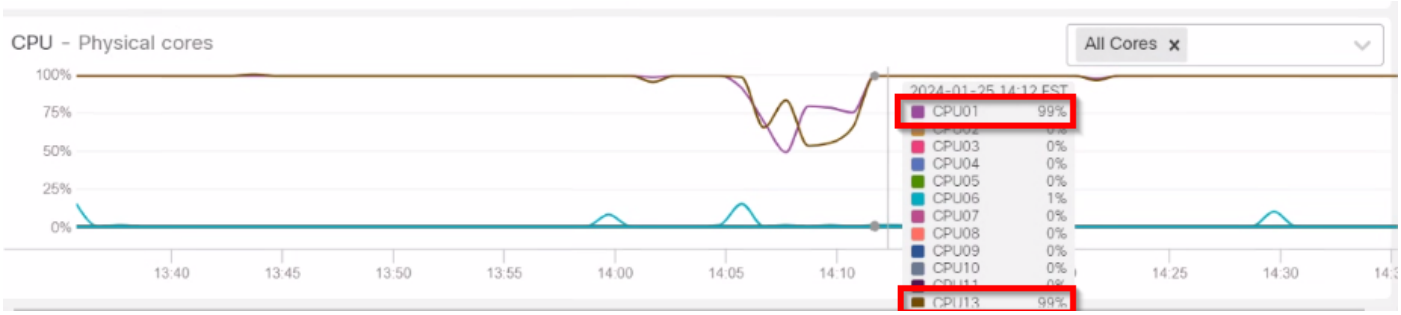
해결책에는 영향을 받는 FTD 디바이스를 확인된 결함에 대한 수정 사항이 포함된 소프트웨어 버전으로 업그레이드하는 작업이 포함됩니다.

### 문제 해결 및 분석 단계

1: 시간이 지남에 따라 FTD 상태 모니터 그래프의 CPU 사용률 패턴을 검사하여 문제의 범위와 타이밍을 식별합니다. 분석 결과, 특정 코어에서 반복적으로 CPU 코어 스파이크가 발생하는 반면, 전체 CPU 및 메모리 사용률은 정상 작동 범위 내에 머물러 있습니다.




inline_image_0.png




인라인 이미지_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: FTD CLI를 분석하고 영향받는 FTD에서 번들 문제를 해결하여 높은 CPU 사용률의 근본 원인을 파악합니다.

3: 수집된 데이터를 검토하여 어떤 프로세스에서 과도한 CPU 리소스를 사용하고 있는지 확인합니다. top.log 파일을 분석한 결과 Pruner.pl 프로세스가 특정 코어에서 높은 CPU를 지속적으로 사용하고 있었으며, 문제 패턴이 특정 기간 즈음에 시작되었다는 것이 확인되었습니다.

```
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/
```

또한 로그는 Pruner.pl이 자주 실행되는 주된 이유인 빈 0바이트"*snort-unified.log" 파일의 많은 수를 보여줍니다.

```
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
```

### 소프트웨어 업그레이드 솔루션

1: 영향을 받는 모든 FTD 장치를 CSCwh79095에 대한 수정 사항이 포함된 소프트웨어 버전으로 업그레이드합니다. 권장되는 최소 버전은 다음과 같습니다.

- FTD 7.2.7(7.2.x 기차의 최소 수정 버전)
- FTD 7.4.1 이상(권장 업그레이드 경로)

2: 업그레이드 후 FMC 상태 알림을 모니터링하여 다음을 확인합니다.

- 코어당 CPU 사용률이 안정적으로 유지됨
- Pruner.pl 또는 유사한 백그라운드 프로세스에 대해 새로운 중요 경보가 발생하지 않음
- Pruner.pl 프로세스에 대한 높은 CPU 알림이 더 이상 발생하지 않음

### 예방 및 모범 사례

유사한 문제를 방지하기 위해 다음 권장 사항을 구현합니다.

- 버그 수정 및 보안 업데이트의 이점을 얻기 위해 오래된 코드를 장기간 사용하지 않고 권장 릴리스로 정기적인 업그레이드를 계획합니다.
- 주요 업그레이드 전에 Cisco 릴리스 정보를 검토하고 현재 및 대상 버전에 대해 알려진 결함을 버그 검색합니다.
- 업그레이드 후 FMC 상태 경고를 계속 모니터링하여 시스템 안정성 보장
- 릴리스 노트에 문서화된 특별한 업그레이드 고려 사항 검토

## 원인

높은 CPU 경고는 Cisco Bug ID CSCwh79095으로 식별된 FTD 7.2.5의 소프트웨어 결함으로 인해 발생합니다. 이 결함은 비어 있는 0바이트 snort-unified.log 파일로 인해 내부 Pruner.pl 백그라운드 프로세스가 특정 코어에서 과도한 CPU를 소비하게 됩니다. 이렇게 하면 FMC에서 지속적인 CPU 사용량이 많은 경보가 트리거됩니다. 중요한 것은 이 조건은 데이터 플레인 트래픽 포워딩 또는 전반적인 디바이스 안정성에 영향을 미치지 않는다는 것입니다. 관리 인터페이스에서 중요한 CPU 알림만 생성합니다. 이 문제는 CSCwe66384(Pruner.pl 및 명백한 디스크 문제가 없는 디스크 관리자 높은 CPU) 및 CSCwf80946(FTD: 과도한 시스템 CPU 코어를 사용하고 FMC HM 알림을 생성하는 Pruner 프로세스).

## 관련 콘텐츠

- Cisco Bug ID CSCwh79095 - Snort가 0바이트의 과도한 수의 snort-unified 로그 파일을 생성합니다(수정됨: 7.2.7, 7.4.1, 7.6.0)
- Cisco 버그 ID CSCwf77994 - 높은 사용량이 즉시 실행되는 FTD 장치 시스템 코어에 대한 잘못된 중요 CPU 경고(수정됨: 7.2.9, 7.4.1, 7.6.0)
- FTD/FMC 릴리스 정보 및 권장 릴리스 문서
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.