来自Pruner.pl进程的FTD高CPU核心警报

问题

FMC会为多个受管FTD设备频繁生成高CPU使用率警报，并引发对防火墙性能和稳定性的担忧。具体而言，FMC运行状况监视器显示特定内核在较长时间内重复出现CPU核心峰值，内部Pruner.pl后台进程持续占用指定内核的过量CPU。尽管这些重要CPU警报出现在FMC中，但并未观察到用户可见的流量影响，整体FTD稳定性仍不受影响。

环境

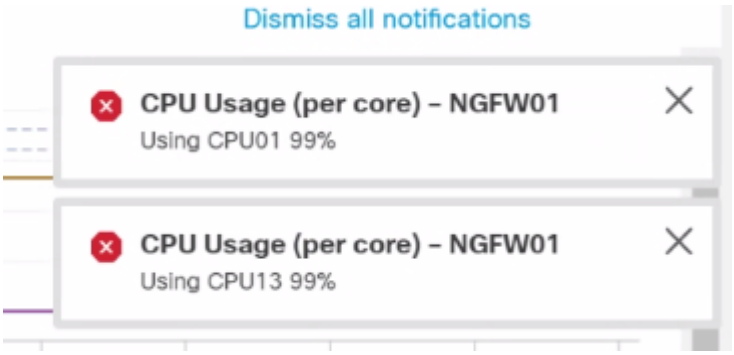
- FTD软件版本：7.2.5（影响所有低于7.2.6版本的虚拟和硬件型号）
- 由Firepower管理中心(FMC)管理的设备

分辨率

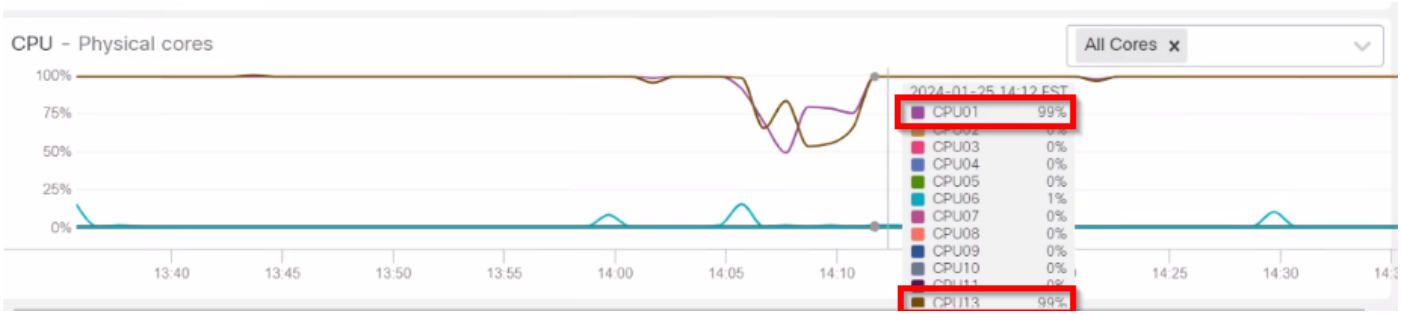
解决方法包括将受影响的FTD设备升级到包含已识别缺陷的修复程序的软件版本。

故障排除和分析步骤

1:检查FTD运行状况监控器图形中随时间变化的CPU使用率模式，以确定问题的范围和时间。分析显示特定内核上重复出现CPU核心峰值，而整体CPU和内存利用率保持在正常运行范围内。



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:分析FTD CLI并对来自受影响的FTD的捆绑包进行故障排除，以确定CPU使用率较高的根本原因。

3:查看收集的数据，确定哪些进程占用了过多的CPU资源。对top.log文件的分析证实，Pruner.pl进程在某些内核上持续使用高CPU，并且问题模式从某个特定的时间范围开始。

```
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/
```

日志还显示大量空的0字节“*snort-unified.log”文件，这是导致Pruner.pl如此频繁运行的主要原因。

```
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
```

软件升级解决方案

1:将所有受影响的FTD设备升级到包含CSCwh79095修复程序的软件版本。建议的最低版本为：

- FTD 7.2.7（7.2.x系列中的最低修复版本）
- FTD 7.4.1或更高版本（推荐的升级路径）

2:升级后，监控FMC运行状况警报以确认：

- 每个内核的CPU使用率保持稳定
- 没有为Pruner.pl或类似后台进程发出新的严重警报
- 不再发生Pruner.pl进程的高CPU警报

防御和最佳实践

实施以下建议以防止类似问题：

- 避免运行较旧的代码培训长期运行，并计划定期升级到推荐版本，以从漏洞修复和安全更新中获益
- 在主要升级之前，请查看思科版本说明并执行漏洞搜索，查找当前版本和目标版本上的已知缺陷
- 在升级后继续监控FMC运行状况警报，以确保系统稳定性
- 查看版本说明中记录的所有特殊升级注意事项

原因

高CPU警报是由FTD 7.2.5中识别为Cisco Bug ID CSCwh79095的软件缺陷引起的。此缺陷是由于空的0字节snort-unified.log文件导致内部Pruner.pl后台进程占用特定内核的过量CPU。这会触发FMC中的持续高CPU警报。重要的是，这种情况不会影响数据平面流量转发或整体设备稳定性；它仅在管理接口中生成关键CPU警报。此问题与CSCwe66384（Pruner.pl和磁盘管理器高CPU但没有明显的磁盘问题）和CSCwf80946(FTD:使用过多系统CPU核心并生成FMC HM警报的修剪器进程)。

相关内容

- Cisco Bug ID CSCwh79095（思科漏洞ID CSCwh） — Snort生成过多的零字节的snort-unified日志文件(已在以下位置修复：7.2.7，7.4.1，7.6.0)
- Cisco Bug ID CSCwf77994 — 运行瞬时高使用率的FTD设备系统内核的虚假严重CPU高CPU警报(修复于：7.2.9，7.4.1，7.6.0)
- FTD/FMC版本说明和推荐版本文档
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。