安全防火墙1010 FTD高内存导致流量影响(CSCwc82675)

目录

问题

用户在低端平台安全防火墙1010上遇到针对“关键数据平面内存”的运行状况监视器警告。这种高内存利用率会阻止用户连接到VPN。设备也可能因内存耗尽而无法访问并停止正常运行。

即使在重新启动后，即使FTD不处理流量，FTD内存也会立即恢复为高使用率。

<#root>

```
firepower# show memory

Free memory:          216990542 bytes ( 8%)

Used memory:         2487943528 bytes (92%)


-------------      ------------------
Total memory:        2704934070 bytes (100%)
```

内存使用情况详细信息显示DMA池中保留的大量内存。

<#root>

```
firepower# show memory detail

Heap Memory:
   Free Memory:
      Heapcache Pool:                       85289152 bytes (  3% )
      Global Shared Pool:                    1675200 bytes (  0% )
      Message Layer Pool:                   14495776 bytes (  1% )
      Message Layer HB Pool:                  197712 bytes (  0% )
      System:                              125170870 bytes (  5% )
   Used Memory:
      Heapcache Pool:                      684365632 bytes ( 25% )
      Global Shared Pool:                  123629632 bytes (  5% )
```

```
Reserved (Size of DMA Pool):        1073741824 bytes ( 40% )


      Reserved for messaging:                2019296 bytes (  0% )
      Reserved for HB messaging:               64432 bytes (  0% )
      MMAP usage:                           39073816 bytes (  1% )
      System Overhead:                     555472872 bytes ( 21% )
-----------------------------------     ----------------
   Total Memory:                         2704934070 bytes ( 100% )
```

ASP丢包输出还指示Snort预处理器执行多次递增丢包。

<#root>

```
firepower# show asp drop
.....

  Blocked or blacklisted by the firewall preprocessor (firewall)        14433080


  Blocked or blacklisted by the stream preprocessor (stream)               29325
  Blocked or blacklisted by the session preprocessor (session-preproc)       646
  Blocked or blacklisted by the IPS preprocessor (ips-preproc)                24
  Fragment reassembly failed (fragment-reassembly-failed)                    397
  Packet is blacklisted by snort (snort-blacklist)                       1812129
```

设备的running-config输出也可能指示多个AnyConnect软件包，它们有助于提高内存容量。

<#root>

```
firepower# show run | inc anyconnect

 anyconnect image disk0:/csm/cisco-secure-client-win-5.1.8.122-webdeploy-k9.pkg 1 regex "Windows"
 anyconnect image disk0:/csm/cisco-secure-client-macos-5.1.6.103-webdeploy-k9.pkg 2 regex "Mac OS"


 anyconnect profiles all-vpn disk0:/csm/all-vpn.xml
 anyconnect profiles iseposture disk0:/csm/ISEPosture.xml
 anyconnect enable
```

环境

- 产品:思科安全防火墙1010
- 已配置思科安全客户端(AnyConnect)

分辨率

缺陷Cisco Bug ID CSCwc82675已在Firepower版本10.0.0中永久解决。

解决方法

- 禁用Webvpn缓存
- 删除不需要的Anyconnect客户端软件包
- 将VPN协议从SSL/TLS更改为IPSec

原因

此特定问题是由缺陷Cisco Bug ID CSCwc82675引起的。Firepower 1010平台是运行安全客户端(AnyConnect)时具有已知限制的低端平台，因为其内存限制，在配置多个AnyConnect软件包(如Cisco Bug ID CSCwc82675中所述)后，可能导致高数据平面内存。Firepower 1010调配了8GB的总内存，并将3GB的总内存分配给LINA/ASA(DATAPATH)进行流量处理。这些设备通常显示更高的内存使用率，因为LINA为流量处理保留了一定量的内存，并且不会轻易将其释放到系统。此行为是出于设计目的，旨在获得更好的性能。使用VPN配置时，内存消耗显示约40%分配给DMA池，该池主要保留用于VPN操作。系统开销占内存使用总量。即使不处理流量，具有VPN配置的Firepower 1010平台也可以显示更高的内存使用率。一旦流量引入防火墙，此内存使用率可以达到最高水平。

相关内容

- 思科漏洞ID CSCwc82675

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）。