

Erschöpfung des FTD-Speicherblocks der sicheren Firewall verursacht Datenverlust

Inhalt

Problem

Bei einer sicheren Firewall 2110 FTD mit Enhanced Interior Gateway Routing Protocol (EIGRP) treten zeitweilige Datenverluste und Routing-Unterbrechungen auf. Dies führt zu einem Verlust der Adjazenz und des Internetzugangs. Die Symptome korrelieren mit der Erschöpfung des Speicherblocks (Blockgröße 80 und 9472) und resultieren in Paketverlusten im Datenpfad und Auswirkungen auf die Kontrollebene. Darüber hinaus wird keine Absturz- oder Core-Datei für das Problem generiert, da kein Neustart ausgelöst wird.

Die Erschöpfung der Speicherblöcke bewirkt, dass die FTD-Einheit den Datenverkehr nicht mehr verarbeitet.

<#root>

firepower#

show blocks

SIZE	MAX	LOW	CNT	FAILED
0	2700	2650	2700	0
4	200	199	200	0

80 24000 0 0 2200668

256	6072	3011	3178	0
1550	7386	4013	4719	0
2048	600	572	600	0
2560	900	889	900	0
4096	100	100	100	0
8192	100	97	100	0

9472 10000 0 2668 1

16384	100	100	100	0
65664	16	16	16	0

ASP-Drops auf dem FTD zeigten große Zähler für "Dispatch queue tail drops (dispatch-queue-limit)" drops:

<#root>

firepower#

show asp drop

Frame drop:

First TCP packet not SYN (tcp-not-syn)	12357166
Packet is blacklisted by snort (snort-blacklist)	1159498
Fragment reassembly failed (fragment-reassembly-failed)	53865

Dispatch queue tail drops (dispatch-queue-limit)	1582611
---	----------------

Es gibt auch eine Menge Zeitüberschreitungen bei der Fragmentzusammenstellung:

<#root>

firepower#

show fragment

Interface: outside

Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
Run-time stats: Queue: 0, Full assembly: 1916508

Drops:

Size overflow: 0,

Timeout: 6217,

Chain overflow: 0, Fragment queue threshold exceeded: 47611,
Small fragments: 0, Invalid IP len: 0,
Reassembly overlap: 0, Fraghead alloc failed: 0,
SGT mismatch: 0, Block alloc failed: 0,
Invalid IPV6 header: 0, Passenger flow assembly failed: 0
Cluster reinsert collision: 0

Die zugewiesenen Blöcke zeigen alle die gleiche Zuweisung an und zeigen die Auswirkung des Cisco Fehlers CSCws19823 an. (Führen Sie den Befehl `terminal pager 20` aus, bevor Sie ausführen, um die Ausgabe zu begrenzen.)

<#root>

firepower#

show blocks assigned

Class size 2, size 80

Block	allocd_by	freed_by	data size	alloccnt	dup_cnt	oper loc
0xa800000100058c80	0x000000aaad8556ac	0x000000aaad2cefb8	183	17310	0	

alloc cvmx_api_pdts_send_to_host

0xa800000100059400	0x000000aaad8556ac	0x000000aaad2cefb8	183	3748	0	
--------------------	--------------------	--------------------	-----	------	---	--

alloc cvmx_api_pdts_send_to_host

0xa800000100059b80	0x000000aaad8556ac	0x000000aaad2cefb8	182	74639	0	
--------------------	--------------------	--------------------	-----	-------	---	--

alloc cvmx_api_pdts_send_to_host

0xa80000010005a300	0x000000aaad8556ac	0x000000aaad7cf0e8	183	23610	0	
--------------------	--------------------	--------------------	-----	-------	---	--

alloc cvmx_api_pdts_send_to_host

0xa80000010005aa80	0x000000aaad8556ac	0x000000aaad2cefb8	183	40731	0	
--------------------	--------------------	--------------------	-----	-------	---	--

alloc cvmx_api_pdts_send_to_host

Eine Überprüfung der Verbindungen auf der FTD bestätigt, dass die meisten eingehenden Verbindungen SMB-Datenverkehr (TCP/445) auf der FTD-Schnittstelle sind. (Führen Sie `Terminal Pager 20` aus, bevor Sie ausführen, um die Ausgabe zu begrenzen.)

<#root>

firepower#

show conn detail

TCP outside: 10.X.X.49/55970 inside: 10.X.X.73/

445

,
flags UIO N1, idle 1m13s, uptime 1h52m, timeout 1h0m, bytes 163283, xlate id 0xffe0384b00, flow id
Initiator: 10.X.X.49, Responder: 10.X.X.73
Connection lookup keyid: 3616633230
TCP outside: 10.X.X.72/57775 inside: 10.X.X.214/

445

,
flags UIO N1, idle 5s, uptime 2h6m, timeout 1h0m, bytes 182005, xlate id 0xffe0384b00, flow id 2202
Initiator: 10.X.X.72, Responder: 10.X.X.214
Connection lookup keyid: 3661674758
TCP outside: 10.X.X.131/54313 inside: 10.X.X.71/

445

,
flags UIO N1, idle 29s, uptime 9m35s, timeout 1h0m, bytes 26205, xlate id 0xffe0384b00, flow id 224
Initiator: 10.X.X.131, Responder: 10.X.X.71
Connection lookup keyid: 1202806582

Umwelt

- Cisco Secure Firewall FPR2110-NGFW-K9 Firewall Threat Defense (FTD) Version 7.4.3 (zuerst gesehen)
- Von der Firewall überprüft SMB-Datenverkehr (TCP/445)

Auflösung

Sofortige Lösung

1. Konfigurieren Sie eine Vorfilterrichtlinie, um die Prüfung des SMB-Datenverkehrs an allen relevanten Schnittstellen zu umgehen, insbesondere an der FTD-Schnittstelle, an der der SMB-Datenverkehr in die Firewall eintritt.

```
access-list CSM_FW_ACL_ line 4 remark rule-id 268459032: PREFILTER POLICY: FTD Prefilter Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268459032: RULE: SMB-FastPath
access-list CSM_FW_ACL_ line 6 advanced trust tcp ifc outside any any eq 445 rule-id 268459032 eve
```

2. Vorhandene SMB-Verbindungen löschen und Blockzähler zurücksetzen

```
clear conn port 445 all
clear blocks
```

3. Führen Sie diesen Befehl aus, um die Blockinkremente auf Fehler zu überwachen:

```
show blocks
```

Permanente Fehlerbehebung

1. Führen Sie ein Upgrade auf Cisco Secure Firewall Threat Defense 7.0.9, 7.2.11, 7.4.4 oder 7.6.0 durch.
2. Nach dem Upgrade auf die feste Version überwachen Sie die Speicherblockauslastung, um die Stabilisierung zu bestätigen und sicherzustellen, dass keine Speicherblockauslastung mehr auftritt.
3. Nach dem Upgrade auf die feste Version kann SMB-Datenverkehr bei Bedarf sicher aus dem Vorfilter entfernt werden, da der zugrunde liegende Fehler behoben wurde.

Verwendete Fehlerbehebungsbefehle

Diese Diagnosebefehle wurden verwendet, um die Speicherblockzuordnungsmuster zu analysieren:

```
show blocks | redirect disk0:/show.blocks.txt
show blocks pool 80 dump | redirect disk0:/show.block.pool.80.dump.txt
show blocks queue history detail | redirect disk0:/show.blocks.Q.history.detail.txt
```

```
show blocks queue history core-local | redirect disk0:/show.blocks.Q.hist.core-local.txt
show blocks old core-local | redirect disk0:/show.blocks.old.core-local.txt
show blocks exhaustion snapshot | redirect disk0:/show.blocks.exhaustion.shapshot.txt
show blocks exhaustion history | redirect disk0:/show.blocks.exhaustion.history.txt
show blocks assigned | redirect disk0:/show.blocks.assigned.txt
```

Ursache

Das Problem wird durch einen bekannten Softwarefehler Cisco Bug-ID CSCws19823 in Cisco Secure Firewall Threat Defense verursacht, bei dem ein hohes Volumen an überprüfem SMB (TCP/445)-Datenverkehr zu einer Erschöpfung der Speicherblockgröße 80 führen könnte, was zu Paketverlusten im Datenpfad und sekundären Auswirkungen wie EIGRP-Instabilität und Datenverkehrsverlust führen könnte. Der Fehler tritt auf, wenn der SMB-Datenverkehr einer vollständigen Überprüfung unterzogen wird.

Verwandte Inhalte

- [Blockverarmung der Cisco Bug-ID CSCws19823 - 80, 1550 und 9472 bei ASA/FTD 2100, wenn SMB-Multichannel-Datenverkehr gesendet wird](#)
- [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.