Suricata - Bug #3885
6.0.0-beta1 stream-tcp-reassemble.c:1066: AdjustToAcked: Assertion `!(adjusted > check)’ failed
08/18/2020 01:46 PM - Andre ten Bohmer

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category: Target version: 6.0.0rc1
Affected Versions:
Effort:
Description

History
#1 - 08/18/2020 01:51 PM - Andre ten Bohmer
Hello,
Able to configure, compile and link 6.0.0-beta1, config file check was successful, starts via systemctl start suricata, but core dumps after a few seconds (config and rules are all loaded so it start to process in my opinion) Core dump file is available (160Mb).

Kind regards,
Andre

Distributor ID: RedHatEnterpriseServer
Description: Red Hat Enterprise Linux Server release 7.8 (Maipo)
Release: 7.8
Codename: Maipo
Linux scomp1185.wurnet.nl 3.10.0-1127.18.2.el7.x86_64 #1 SMP Mon Jul 20 22:32:16 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

PF_RING Version : 7.5.0 (unknown)
Total rings : 28

Standard (non ZC) Options
Ring slots : 32767
Slot version : 17
Capture TX : No [RX only]
IP Defragment : No
Socket Mode : Standard
Cluster Fragment Queue : 68
Cluster Fragment Discard : 0

Aug 18 15:27:58 scomp1185.wurnet.nl systemd[1]: Starting Suricata Intrusion Detection Service...
Aug 18 15:28:16 scomp1185.wurnet.nl suricata[57058]: 18/8/2020 -- 15:28:16 - <Notice> - FM FM#01/0 starting, min_timeout 10s. Full hash pass in 80s

09/07/2020
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.
Aug 18 15:28:16 scomp1185.wurnet.nl suricata: [ERRCODE: SC_ERR_PF_RING_VLAN(304)] - no VLAN header in the raw packet. See #2355.

#2 - 08/19/2020 05:58 AM - Peter Manev

Seems other users are experiencing this as well. Some report that changing use-for-tracking: true -> use-for-tracking: false improves things.

https://github.com/StamusNetworks/SELKS/issues/248#issuecomment-675321482

#3 - 08/19/2020 07:56 AM - Andre ten Bohmer

Peter Manev wrote in #note-2:

Seems other users are experiencing this as well. Some report that changing use-for-tracking: true -> use-for-tracking: false improves things.

https://github.com/StamusNetworks/SELKS/issues/248#issuecomment-675321482

To no avail, runs a few seconds after processing config and core dumps:

Aug 19 09:52:33 systemd: suricata: main process exited, code=killed, status=6/ABRT
ok - it seems the vlan switching is not helping at all, thanks for checking.

Attached gdb provided from one user on the SELKS forum (link above)

I mange to consistently reproduce this on live traffic -

Additional info and coredump trace attached.

Ring params: block_size=1048576 block_nr=1270 frame_size=1664 frame_nr=800100 (mem: 1331691520)

Ring params: block_size=1048576 block_nr=1270 frame_size=1664 frame_nr=800100 (mem: 1331691520)

Ring params: block_size=1048576 block_nr=1270 frame_size=1664 frame_nr=800100 (mem: 1331691520)

Aborted (core dumped)

#6 - 08/24/2020 03:08 PM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Victor Julien
- Target version set to 6.0.0rc1

#7 - 08/26/2020 05:44 AM - Victor Julien
https://github.com/OISF/suricata/pull/5325

#8 - 08/26/2020 05:44 AM - Victor Julien
- Status changed from Assigned to Closed

Files

gdb.txt 16.5 KB  08/19/2020  Peter Manev
sigabrt-info 145 KB  08/23/2020  Peter Manev