Suricata - Bug #1669

Suricate 3.0RC3 segfault after 10 hours

01/13/2016 09:12 AM - Andre ten Bohmer

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category: 
Target version: 3.0.1RC1
Affected Versions: 
Difficulty: 
Effort: 
Label: 

Description
Daily a service restart at 07h CET (logrotate and rules), and sometimes at 16h Suricata segfaults.

Kernel ring message:
RxPFReth51[38079]: segfault at 7f43a1975000 ip 00000000005930c9 sp 00007f43a2373420 error 4 in suricata[400000+225000]

Redhat 6.7

2.6.32-573.12.1.el6.x86_64 #1 SMP Mon Nov 23 12:55:32 EST 2015 x86_64 x86_64 x86_64 GNU/Linux

Pfring from source:
~]# cat /proc/net/pf_ring/info

PF_RING Version : 6.3.0 (unknown)
Total rings : 4

Standard (non DNA/ZC) Options
Ring slots : 8192
Slot version : 16
Capture TX : No [RX only]
IP Defragment : No
Socket Mode : Standard
Total plugins : 0
Cluster Fragment Queue : 0
Cluster Fragment Discard : 0

Suricata:

~]# ldd /usr/bin/suricata
linux-vdso.so.1 => (0x00007ffc3298f000)
libhttp-0.5.18.so.1 => /usr/lib/libhttp-0.5.18.so.1 (0x0000000362580000)
libGeoIP.so.1 => /usr/lib/libGeoIP.so.1 (0x00000003ee020000)
libluajit-5.1.so.2 => /usr/local/lib/libluajit-5.1.so.2 (0x00000007f5315eb000)
limagc.so.1 => /usr/local/lib/libmagic.so.1 (0x00000007f5313ce000)
libcap-ng.so.0 => /lib64/libcap-ng.so.0 (0x0000000321980000)
libpfring.so => /usr/local/lib/libpfring.so (0x00000007f5316f000)
libpcap.so.1 => /usr/local/lib/libpcap.so.1 (0x00000007f530eda000)
linbnet.so.1 => /lib64/libinbnet.so.1 (0x00000003219c0000)
ljbjansson.so.4 => /usr/lib/libjansson.so.4 (0x0000000321ac0000)
liblyaml-0.so.2 => /usr/lib/libyaml-0.so.2 (0x0000000321a40000)
libpcre.so.1 => /opt/pcre-8.37/lib/libpcre.so.1 (0x00000007f530c6e000)
libr.so.1 => /lib64/librl.so.1 (0x0000000321880000)
libnuma.so.1 => /usr/lib/libnuma.so.1 (0x0000000321940000)
libss13.so => /usr/lib64/libss13.so (0x00000003ce4e0000)
libsmime3.so => /usr/lib64/libsmime3.so (0x00000003ce520000)
lbnss3.so => /usr/lib64/lbnss3.so (0x00000003ce4a0000)
lbnssutil3.so => /usr/lib64/lbnssutil3.so (0x00000003815e0000)
libplds4.so => /lib64/libplds4.so (0x0000000381660000)
libplc4.so => /lib64/libplc4.so (0x0000000381620000)
libnspr4.so => /lib64/libnspr4.so (0x00000003815a0000)
libpthread.so.0 => /lib64/libpthread.so.0 (0x0000003218400000)
libdl.so.2 => /lib64/libdl.so.2 (0x0000003218000000)
libc.so.6 => /lib64/libc.so.6 (0x0000003217c00000)
libz.so.1 => /lib64/libz.so.1 (0x0000003219000000)
libm.so.6 => /lib64/libm.so.6 (0x0000003218c00000)
libgcc_s.so.1 => /lib64/libgcc_s.so.1 (0x0000000321780000)

~/]# suricata --build-info

This is Suricata version 3.0RC3 RELEASE
Features: PCAP_SET_BUFF LIBPCAP_VERSION_MAJOR=1 PF_RING AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1 HAVE_HTP_URI_NORMALIZE_HOOK PCRE_JIT HAVE_NSS HAVE_LUA HAVE_LUAJIT HAVE_LIBJANSSON TLS
SIMD support: SSE_4_2 SSE_4_1 SSE_3
Atomic intrinsics: 1 2 4 8 16 byte(s)
64-bits, Little-endian architecture
GCC version 4.4.7 20120313 (Red Hat 4.4.7-16), C version 199901
compiled with -fstack-protector
compiled with _FORTIFY_SOURCE=2
L1 cache line size (CLS)=64
thread local storage method: __thread
compiled with LibHTP v0.5.18, linked against LibHTP v0.5.18

Suricata Configuration:
AF_PACKET support: yes
PF_RING support: yes
NFQueue support: no
NFLOG support: no
IPFW support: no
Netmap support: no
DAG enabled: no
Napatech enabled: no

Unix socket enabled: yes
Detection enabled: yes

libnss support: yes
libnspr support: yes
libjansson support: yes
hiredis support: no
Prelude support: no
PCRE jit: yes
LUA support: yes, through luajit
libluajit: yes
libgeoip: yes
Non-bundled http: no
Old barnyard2 support: yes
CUDA enabled: no

Suricatasc install: yes

Unit tests enabled: no
Debug output enabled: no
Debug validation enabled: no
Profiling enabled: no
Profiling locks enabled: no
Coccinelle / spatch: no

Generic build parameters:
Installation prefix: /usr
Configuration directory:   /etc/suricata/
Log directory:             /var/log/suricata/

--prefix                  /usr
--sysconfdir               /etc
--localstatedir            /var

Host:                      x86_64-unknown-linux-gnu
Compiler:                  gcc (exec name) / gcc (real)
GCC Protect enabled:       yes
GCC march native enabled:  yes
GCC Profile enabled:       no
Position Independent Executable enabled: no
CFLAGS                    -O0 -ggdb -march=native
PCAP_CFLAGS               -I/usr/local/include
SECCFLAGS                 -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security

History
#1 - 01/13/2016 10:17 AM - Peter Manev
From the build-info output I see that there is no debug enabled - hence most likely not so much useful information to chase the issue.
Since you mention this is reproducible - can you please recompile with -

CFLAGS="-O0 -ggdb" ./configure..........

Then the coredump would be very helpful.

#2 - 01/13/2016 10:23 AM - Andre ten Bohmer
Peter Manev wrote:

From the build-info output I see that there is no debug enabled - hence most likely not so much useful information to chase the issue.
Since you mention this is reproducible - can you please recompile with -

[...]

Then the coredump would be very helpful.

Thanks for the input, just reconfigured and compiled/linked again and restart suricata. See what happens coming days.

Host:                      x86_64-unknown-linux-gnu
Compiler:                  gcc (exec name) / gcc (real)
GCC Protect enabled:       yes
GCC march native enabled:  yes
GCC Profile enabled:       no
Position Independent Executable enabled: no
CFLAGS                    -O0 -ggdb -march=native
PCAP_CFLAGS               -I/usr/local/include
SECCFLAGS                 -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security

#3 - 01/21/2016 02:33 PM - Andreas Moe
Any news for this issue? Haven't seen the same issue but very anxious for the outcome / resolution.

#4 - 01/22/2016 03:57 AM - Victor Julien
Wonder if it's related to https://lists.openinfosecfoundation.org/pipermail/oisf-users/2016-January/005594.html

#5 - 01/22/2016 09:49 AM - Victor Julien
- Target version changed from 3.0 to Soon

#6 - 01/25/2016 09:04 AM - Andre ten Bohmer
Well since recompiling it as requested with CFLAGS="-O0 -ggdb" I've not seen any crash yet. Did not upgrade poring or kernel in-between so a little mystery.

#7 - 01/28/2016 11:34 AM - Victor Julien
Andre, do you happen to have some of the nic offloading features still on? Can you show output of 'ethtool -k <youriface>"?  

06/13/2020 3/6
Hello Victor,

Suricata uses input from 2 nic’s (--pfring-int=eth4  --pfring-int=eth5)

1. ethtool -k eth4
   Features for eth4:
   rx-checksumming: on
   tx-checksumming: on
   tx-checksum-ipv4: on
   tx-checksum-unneeded: off [fixed]
   tx-checksum-ip-generic: off [fixed]
   tx-checksum-ip6: on
   tx-checksum-foe-crc: on [fixed]
   tx-checksum-sctp: on
   scatter-gather: on
   tx-scatter-gather: on
   tx-scatter-gather-fraglist: off [fixed]
   tcp-segmentation-offload: on
   tx-tcp-segmentation: on
   tx-tcp-ecn-segmentation: on [fixed]
   tx-tcp6-segmentation: on
   udp-fragmentation-offload: off [fixed]
   generic-segmentation-offload: on
   generic-receive-offload: on
   large-receive-offload: on
   rx-vlan-offload: on
   tx-vlan-offload: on
   ntuple-filters: off
   receive-hashing: on
   highdma: on [fixed]
   rx-vlan-filter: on [fixed]
   vlan-challenged: off [fixed]
   tx-lockless: off [fixed]
   netns-local: off [fixed]
   tx-gso-robust: off [fixed]
   tx-foe-segmentation: on [fixed]
   tx-gre-segmentation: off [fixed]
   tx-udp_tnl-segmentation: off [fixed]
   fcoe-mtu: off [fixed]
   loopback: off [fixed]

2. ethtool -k eth5
   Features for eth5:
   rx-checksumming: on
   tx-checksumming: on
   tx-checksum-ipv4: on
   tx-checksum-unneeded: off [fixed]
   tx-checksum-ip-generic: off [fixed]
   tx-checksum-ip6: on
   tx-checksum-foe-crc: on [fixed]
   tx-checksum-sctp: on
   scatter-gather: on
   tx-scatter-gather: on
   tx-scatter-gather-fraglist: off [fixed]
   tcp-segmentation-offload: on
   tx-tcp-segmentation: on
   tx-tcp-ecn-segmentation: off [fixed]
   tx-tcp6-segmentation: on
   udp-fragmentation-offload: off [fixed]
   generic-segmentation-offload: on
   generic-receive-offload: on
   large-receive-offload: on
   rx-vlan-offload: on
   tx-vlan-offload: on
   ntuple-filters: off
   receive-hashing: on
   highdma: on [fixed]
   rx-vlan-filter: on [fixed]
   vlan-challenged: off [fixed]
   tx-lockless: off [fixed]
   netns-local: off [fixed]
   tx-gso-robust: off [fixed]
   tx-foe-segmentation: on [fixed]
Crash today at 13:09 CET, running since a service restart at 07:00 CET today.

RxPFReth51: segfault at 7fe120109000 ip 000000000061980b sp 00007fe120b072f0 error 4 in suricata[400000+2cb000]

ethtool -k eth5
Features for eth5:
rx-checksumming: off
tx-checksumming: off
tx-checksum-ipv4: off
tx-checksum-unneeded: off [fixed]
tx-checksum-ip-generic: off [fixed]
tx-checksum-ipv6: off
tx-checksum-fcoe-crc: on [fixed]
tx-checksum-sctp: off
scatter-gather: off
tx-scatter-gather: off
tx-scatter-gather-fraglist: off [fixed]
tcp-segmentation-offload: off
tx-tcp-segmentation: off
tx-tcp-ecn-segmentation: off [fixed]
tx-tcp6-segmentation: off
udp-fragmentation-offload: off [fixed]
generic-segmentation-offload: off
generic-receive-offload: off
large-receive-offload: off
rx-vlan-offload: off
tx-vlan-offload: off
ntuple-filters: off
receive-hashing: on
highdma: on [fixed]
rx-vlan-filter: on [fixed]
vlan-challenged: off [fixed]
tx-lockless: off [fixed]
netns-local: off [fixed]
tx-gso-robust: off [fixed]
tx-fcoe-segmentation: on [fixed]
tx-gre-segmentation: off [fixed]
tx-udp_tnl-segmentation: off [fixed]
loopback: off [fixed]

suricata --build-info
This is Suricata version 3.0 RELEASE
Features: PCAP_SET_BUFF LIBPCAP_VERSION_MAJOR=1 PF_RING AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1
HAVE_HTP_URI_NORMALIZE_HOOK PCRE_JIT HAVE_NSS HAVE_LUA HAVE_LUAJIT HAVE_LIBJANSSON TLS
SIMD support: SSE_4_2 SSE_4_1 SSE_3
Atomic intrinsics: 1 2 4 8 16 byte(s)
64-bits, Little-endian architecture
GCC version 4.4.7 20120313 (Red Hat 4.4.7-16), C version 199901
compiled with -fstack-protector
compiled with _FORTIFY_SOURCE=2
L1 cache line size (CLS)=64
thread local storage method: __thread
compiled with LibHTP v0.5.18, linked against LibHTP v0.5.18

Suricata Configuration:
AF_PACKET support: yes
PF_RING support: yes
NFQueue support: no
NFLOG support: no
IPFW support: no
Netmap support: no
DAG enabled: no
Napatech enabled: no
Unix socket enabled: yes
Detection enabled: yes
libnss support: yes
libnspr support: yes
libjansson support: yes
hiredis support: no
Prelude support: no
PCRE jit: yes
LUA support: yes, through luajit
liblua: yes
libgeoip: yes
Non-bundled htp: no
Old barnyard2 support: yes
CUDA enabled: no

Suricata install: yes

Unit tests enabled: no
Debug output enabled: no
Debug validation enabled: no
Profiling enabled: no
Profiling locks enabled: no
Cocinelle / spatch: no

Generic build parameters:
Installation prefix: /usr
Configuration directory: /etc/suricata/
Log directory: /var/log/suricata/

--prefix /usr
--sysconfdir /etc
--localstatedir /var

Host: x86_64-unknown-linux-gnu
Compiler: gcc (exec name) / gcc (real)
GCC Protect enabled: yes
GCC march native enabled: yes
GCC Profile enabled: no
Position Independent Executable enabled: no
CFLAGS -O0 -ggdb -march=native
PCAP_CFLAGS -I/usr/local/include
SECCFLAGS -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security

According to CFLAGS a crashdump should be generated, correct? But where to find it?

#10 - 02/18/2016 08:10 AM - Victor Julien
- Description updated

#11 - 03/03/2016 02:12 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Victor Julien

Still investigating.

#12 - 03/16/2016 06:47 AM - Victor Julien
- Status changed from Assigned to Closed
- Target version changed from Soon to 3.0.1RC1

Fixed by https://github.com/inliniac/suricata/pull/1914