**Suricata - Bug #1669**

**Suricata 3.0RC3 segfault after 10 hours**

01/13/2016 09:12 AM - Anonymous

<table>
<thead>
<tr>
<th>Status</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee</td>
<td>Victor Julien</td>
</tr>
<tr>
<td>Category</td>
<td></td>
</tr>
<tr>
<td>Target version</td>
<td>3.0.1RC1</td>
</tr>
<tr>
<td>Affected Versions</td>
<td></td>
</tr>
<tr>
<td>Difficulty</td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

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

**Kernel ring message:**

```
RxPFReth5[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 (0x0000003625800000)
libGeoIP.so.1 => /usr/lib64/libGeoIP.so.1 (0x00000003ee020000)
libluajit-5.1.so.2 => /usr/local/lib/libluajit-5.1.so.2 (0x0000007f53177000)
libmagic.so.1 => /usr/local/lib/libmagic.so.1 (0x0000007f5313ce000)
lbtcap-ng.so.0 => /lib64/libbtcap-ng.so.0 (0x0000003219800000)
lbpfring.so => /usr/local/lib/lbpfring.so (0x0000007f5316f000)
lbpcap.so.1 => /usr/local/lib/lbpcap.so (0x0000007f530eda000)
lbnet.so.1 => /lib64/lbnet.so.1 (0x0000003219c00000)
lbjansson.so.4 => /usr/lib64/lbjansson.so.4 (0x0000000321ac0000)
lbyaml-0.so.2 => /usr/lib64/lbyaml-0.so.2 (0x0000000321a40000)
lbpcre.so.1 => /opt/pcre-8.37/lib/lbpcre.so.1 (0x0000007f530c6e000)
lbrtc.so.1 => /lib64/lbrtc.so.1 (0x000000321880000)
lbnuma.so.1 => /usr/lib64/lbnuma.so.1 (0x0000003219400000)
lbssl3.so => /usr/lib64/lbssl3.so (0x00000003ce4e0000)
```
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
Napatch 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 htp: 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                       -g -O2 -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 - Anonymous
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 70

#6 - 01/25/2016 09:04 AM - Anonymous
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>`?
Hello Victor,

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

```bash
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-ipv6: on
tx-checksum-fcoe-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]
rx-lockless: off [fixed]
netns-local: off [fixed]
tx-gso-robust: off [fixed]
tx-fcoe-segmentation: on [fixed]
tx-gre-segmentation: off [fixed]
tx-udp_tunnel-segmentation: off [fixed]
foe-mtu: off [fixed]
loopback: off [fixed]

1. 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-ipv6: on
tx-checksum-fcoe-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]
rxdm-filter: on [fixed]
vlan-challenged: off [fixed]
rx-lockless: off [fixed]
netns-local: off [fixed]
tx-gso-robust: off [fixed]
tx-fcoe-segmentation: on [fixed]
tx-gre-segmentation: off [fixed]
tx-udp_tunnel-segmentation: off [fixed]
foe-mtu: off [fixed]
loopback: off [fixed]
```
tx-gre-segmentation: off [fixed]
rx-gre-segmentation: off [fixed]
rx-udp_tnl-segmentation: off [fixed]
Loose mtu: off [fixed]
loopback: off [fixed]

#9 - 02/02/2016 06:58 AM - Anonymous
Crash today at 13:09 CET, running since a service restart at 07:00 CET today.

RxPFRefs(5): segfault at 7fe120109000 ip 000000000061980b sp 00007fe120b072f0 error 4 in suricata[400000+2cb000]

ethtool -k eth5
Features for eth5:
rx-checksumming: off
rx-checksumming: off
rx-checksum-unneeded: off [fixed]
rx-checksum-ip-generic: off [fixed]
rx-checksum-ipv6: off
rx-checksum-fcoe-crc: on [fixed]
rx-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]
rx-vlan-challenged: off [fixed]
tx-lockless: off [fixed]
netns-local: off [fixed]
rx-fcoe-segmentation: on [fixed]
tx-gre-segmentation: off [fixed]
tx-udp_tnl-segmentation: off [fixed]
fcoe-mtu: 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
<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>libnss support</td>
<td>yes</td>
</tr>
<tr>
<td>libnsprr support</td>
<td>yes</td>
</tr>
<tr>
<td>libjson support</td>
<td>yes</td>
</tr>
<tr>
<td>Prelude support</td>
<td>no</td>
</tr>
<tr>
<td>PCRE jit</td>
<td>yes</td>
</tr>
<tr>
<td>lua support</td>
<td>yes, through luajit</td>
</tr>
<tr>
<td>liblua support</td>
<td>yes</td>
</tr>
<tr>
<td>libgeoip support</td>
<td>yes</td>
</tr>
<tr>
<td>Non-bundled htp</td>
<td>no</td>
</tr>
<tr>
<td>Old barnyard2 support</td>
<td>yes</td>
</tr>
<tr>
<td>CUDA enabled</td>
<td>no</td>
</tr>
<tr>
<td>Suricata install</td>
<td>yes</td>
</tr>
<tr>
<td>Unit tests enabled</td>
<td>no</td>
</tr>
<tr>
<td>Debug output enabled</td>
<td>no</td>
</tr>
<tr>
<td>Debug validation enabled</td>
<td>no</td>
</tr>
<tr>
<td>Profiling enabled</td>
<td>no</td>
</tr>
<tr>
<td>Profiling locks enabled</td>
<td>no</td>
</tr>
<tr>
<td>Coccinelle / spatch</td>
<td>no</td>
</tr>
</tbody>
</table>

**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 70 to 3.0.1RC1

Fixed by [https://github.com/inliniac/suricata/pull/1914](https://github.com/inliniac/suricata/pull/1914)