**Suricata - Bug #2251**

**Suricata won't start - SC_ERR_AHO_CORASICK**

10/25/2017 02:40 AM - Stian Bergseth

| Status: | Closed |
| Priority: | Normal |
| Assignee: | OISF Dev |
| Category: | |
| Target version: | |
| Affected Versions: | |
| Difficulty: | |
| Effort: | |
| Label: | |

**Description**

When starting Suricata it fails after parsing signatures.

```bash
# /usr/bin/suricata --af-packet -c /etc/suricata/suricata.yaml
25/10/2017 -- 09:30:40 - <Notice> - This is Suricata version 3.2.3 RELEASE
25/10/2017 -- 09:30:40 - <Info> - CPUs/cores online: 48
25/10/2017 -- 09:30:40 - <Info> - HTTP memcap: 8589934592
25/10/2017 -- 09:30:40 - <Info> - Found an MTU of 9170 for 'eno49'
25/10/2017 -- 09:30:40 - <Info> - Found an MTU of 9170 for 'eno49'
25/10/2017 -- 09:31:00 - <Info> - 1 rule files processed. 39866 rules successfully loaded, 0 rules failed
25/10/2017 -- 09:31:01 - <Info> - 39868 signatures processed. 6 are IP-only rules, 15387 are inspecting packet payload, 28503 inspect application layer, 0 are decoder event only
```

Some general info about the system:

```bash
@suricata --build-info
This is Suricata version 3.2.3 RELEASE
Features: PCAP_SET_BUFF LIBPCAP_VERSION_MAJOR=1 AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1 HAVE_HTP_URI_NORMALIZE_HOOK PCRE_JIT HAVE_NSS HAVE_LIBJANSSON TLS MAGIC
SIMD support: none
Atomic intrinsics: 1 2 4 8 byte(s)
64-bits, Little-endian architecture
GCC version 4.8.5 20150623 (Red Hat 4.8.5-11), C version 199901
compiled with _FORTIFY_SOURCE=2
L1 cache line size (CLS)=64
thread local storage method: __thread
compiled with LibHTP v0.5.25, linked against LibHTP v0.5.25
```

Suricata Configuration:

- AF_PACKET support: yes
- PF_RING support: no
- 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
- Libmagic support: yes
  - libnss support: yes
  - libnsspr support: yes
  - libjansson support: yes
  - hiredis support: no
  - Prelude support: no
  - PCRE jit: yes
  - LUA support: no
<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>libluajit:</td>
<td>no</td>
</tr>
<tr>
<td>libgeoip:</td>
<td>yes</td>
</tr>
<tr>
<td>Non-bundled http:</td>
<td>no</td>
</tr>
<tr>
<td>Old barnyard2 support:</td>
<td>no</td>
</tr>
<tr>
<td>CUDA enabled:</td>
<td>no</td>
</tr>
<tr>
<td>Hyperscan support:</td>
<td>no</td>
</tr>
<tr>
<td>Libnet support:</td>
<td>yes</td>
</tr>
<tr>
<td>Suricatasc install:</td>
<td>yes</td>
</tr>
<tr>
<td>Profiling enabled:</td>
<td>no</td>
</tr>
<tr>
<td>Profiling locks enabled:</td>
<td>no</td>
</tr>
<tr>
<td>Development settings:</td>
<td></td>
</tr>
<tr>
<td>Coccinelle / spatch:</td>
<td>no</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>Generic build parameters:</td>
<td></td>
</tr>
<tr>
<td>Installation prefix:</td>
<td>/usr</td>
</tr>
<tr>
<td>Configuration directory:</td>
<td>/etc/suricata/</td>
</tr>
<tr>
<td>Log directory:</td>
<td>/var/log/suricata/</td>
</tr>
<tr>
<td>--prefix</td>
<td>/usr</td>
</tr>
<tr>
<td>--sysconfdir</td>
<td>/etc</td>
</tr>
<tr>
<td>--localstatedir</td>
<td>/var</td>
</tr>
</tbody>
</table>

Host: x86_64-redhat-linux-gnu

- Compiler: gcc -std=gnu99 (exec name) / gcc (real)
- GCC Protect enabled: yes
- GCC march native enabled: no
- GCC Profile enabled: no
- Position Independent Executable enabled: no
- CFLAGS: -O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector-strong --param=ssp-buffer-size=4 -grecord-gcc-switches -m64 -mtune=generic
- pcap_cflags: -fstack-protector -D_FORTIFY_SOURCE=2 -Wformat -Wformat-security
- security

This is on CentOS Linux release 7.4

History

#1 - 10/25/2017 03:02 AM - Stian Bergseth
This is with a mix of ET open/pro signatures, VRT signatures and some custom made signatures.
Tried upgrading to 3.2.4 with no success.

After removing 1000 signatures it works again, all of them was "FILE-IDENTIFY" signatures.

#2 - 10/25/2017 03:31 AM - Stian Bergseth
From suricata.yaml

detect-engine:
- profile: custom
- custom-values:
toclient-src-groups: 200
toclient-dst-groups: 200
toclient-sp-groups: 200
toclient-dp-groups: 300
toserver-src-groups: 200
toserver-dst-groups: 400
toserver-sp-groups: 200
toserver-dp-groups: 200
- sgh-mpm-context: single
- inspection-recursion-limit: 3000
mpm-algo: ac

#3 - 10/26/2017 01:55 AM - Victor Julien
- Target version set to TBD

This will be hard to figure out without a proper testcase.

#4 - 10/30/2017 06:33 PM - Andreas Herz
- Assignee set to OISF Dev

#5 - 06/15/2018 09:16 PM - Andreas Herz
- Status changed from New to Closed

Hi, we're closing this issue since there have been no further responses. If you think this bug is still relevant, try to test it again with the most recent version of suricata and reopen the issue. If you want to improve the bug report please take a look at https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Reporting_Bugs

#6 - 02/18/2019 01:02 PM - Victor Julien
- Target version deleted (TBD)