Suricata - Bug #3900

After a completed rule reload, Suricata sometimes is stuck for 1h with `rs_nfs_state_get_tx` peak

09/01/2020 07:02 AM - Andreas Herz

Status: Assigned
Priority: Normal
Assignee: OISF Dev
Category:

Target version: TBD
Affected Versions: 5.0.3
Effort:

Description

We discovered some strange behavior with Suricata on one machine after the rule reload happened.

1/9/2020 -- 06:27:18 - <Notice> - rule reload starting
1/9/2020 -- 06:27:31 - <Info> - 3 rule files processed. 40732 rules successfully loaded, 0 rules failed
1/9/2020 -- 06:27:32 - <Info> - Threshold config parsed: 0 rule(s) found
1/9/2020 -- 06:27:33 - <Info> - 40761 signatures processed. 0 are IP-only rules, 10671 are inspecting packet payload, 30034 inspect application layer, 0 are decoder event only
1/9/2020 -- 06:30:09 - <Info> - cleaning up signature grouping structure... complete
1/9/2020 -- 06:30:09 - <Notice> - rule reload complete
1/9/2020 -- 06:30:09 - <Info> - Unix socket: lost connection with client

I see in htop that 1 process is at 100% cpu load, I still see stats.log being updated but NO values change. So Suricata itself is still running.

With perf top I saw the attached peak of `rs_nfs_state_get_tx` function.

Samples: 1M of event 'cycles', 4000 Hz, Event count (approx.): 53158890162, DSO: suricata

```
rs_nfs_state_get_tx /usr/bin/suricata [Percent: local period]

<table>
<thead>
<tr>
<th>Percent</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>▶</td>
</tr>
</tbody>
</table>

Disassembly of section .text:

```

00000000000020a0c30 <strlcpy@@Base+0x2a0c0>:

| 0.00 | add $0x1,%rsi |
|      | mov $0xffffffffffffffed0,%rax |
| 0.00 | add 0x50(%rdi),%rax |
```
It’s somehow stuck with the `cmp`.

Since it’s just at this machine we suspect that some sort of traffic could produce that. This is also backed by the fact that this doesn’t happen on every daily rule reload.