Suricata - Bug #2570

Signature affecting another's ability to detect and alert

08/07/2018 06:59 PM - Bryant Smith

<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>4.1rc2</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td>4.0.5, 4.1rc1</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

While creating some signatures I stumbled across an odd issue where when the first signature below doesn't allow the second one to detect the traffic in a pcap. The second signature alone can detect and generate an alert as long as the first one is commented out.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 5054 (msg:"Affects the second one!"; flow:established, to_server; content:"/something/else/"; sid:1111111; rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 5054 (msg:"Affected by the 1st one!"; flow:established, to_server; content:"/goform/activate"; http_uri; pcre:"/(?:actserver|akey)=[^&]*500/"; sid:2222222; rev:1;)
```

I tried narrowing it down to try and figure out what's going on. These were tested on both Ubuntu 16.04 running 4.0.5 and Ubuntu 18.04 running 4.1rc1.

**Changes to sid:111111;**

1. Changed the content matches to something completely different - no affect
2. Changed it from tcp to http - no affect
3. Changed the port - Allow the second one to alert
4. Add http_uri; - Allows the second one to alert

**Changes to sid:222222;**

1. Added U to the pcre modifier - Allows the second one to alert
2. Remove http_uri; from signature - Allows the second one to alert

**Related issues:**

Related to Bug #2554: suricata does not detect a web-attack

**History**

#1 - 08/07/2018 07:36 PM - Victor Julien
- Related to Bug #2554: suricata does not detect a web-attack added

#2 - 08/07/2018 07:55 PM - Victor Julien
- Related to Bug #2522: The cross-effects of rules on each other, without the use of flowbits. added

#3 - 08/07/2018 07:57 PM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Victor Julien
- Priority changed from Normal to High
- Target version set to 4.1rc2

Thanks for your detailed report. It looks like there have been reported a few similar cases. I'm looking into it.

#4 - 08/08/2018 11:34 AM - Victor Julien
- Related to deleted (Bug #2522: The cross-effects of rules on each other, without the use of flowbits.)
#5 - 08/13/2018 11:46 AM - Victor Julien
- Status changed from Assigned to Closed
- Priority changed from High to Normal

https://github.com/OISF/suricata/pull/3451

Files

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature_Error.pcap</td>
<td>2.21 KB</td>
<td>08/07/2018</td>
<td>Bryant Smith</td>
</tr>
</tbody>
</table>