**Suricata - Bug #5077**

**byte_math rule options need to be in order or will fail otherwise**

02/14/2022 04:50 PM - Andreas Herz

<table>
<thead>
<tr>
<th>Status:</th>
<th>In Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Jeff Lucovsky</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>TBD</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td>6.0.4</td>
</tr>
</tbody>
</table>

Description

If a rule write doesn't follow the order in the table of [https://suricata.readthedocs.io/en/latest/rules/payload-keywords.html#byte-math](https://suricata.readthedocs.io/en/latest/rules/payload-keywords.html#byte-math) it will run into a parsing error

```
alert tcp any any -> any any (msg:"Byte-math test"; ipv4.hdr; byte_math:bytes 4, offset 72, oper +, rvalue 77, endian little, result result_val; tcp.hdr; byte_test: 1, =, 0x88, 1, relative; sid:1; )
```

results in

```
<Error> - [ERRCODE: SC_ERR_PCRE_PARSE(7)] - byte_math parse error; invalid value: ret -1, string "bytes 4, offset 72, oper +, rvalue 77, endian little, result result_val"
```

while the correct order works

```
alert tcp any any -> any any (msg:"Byte-math test"; ipv4.hdr; byte_math:bytes 4, offset 72, oper +, rvalue 77, result result_val, endian little; tcp.hdr; byte_test: 1, =, 0x88, 1, relative; sid:1; )
```

The test rules swap the endian and result option.

The root cause is IMHO the regex used in src/detect-byte_math.c

---

**History**

#1 - 02/26/2022 06:45 PM - Jeff Lucovsky
- Status changed from Assigned to In Review

[https://github.com/OISF/suricata/pull/7509](https://github.com/OISF/suricata/pull/7509)