### Suricata - Bug #3720

#### Incorrect handling of ASN1 relative_offset keyword

05/20/2020 06:24 PM - Emmanuel Thompson

<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>Emmanuel Thompson</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version</td>
<td>6.0.0rc1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td>Needs backport</td>
</tr>
</tbody>
</table>

**Description**

The `relative_offset` keyword option allows to read past the front of the buffer with a negative offset, no bounds checking is done on this i32 value and is not relative to the last "content" match.

**Related issues:**

- Copied to Bug #3738: Incorrect handling of ASN1 relative_offset keyword
- Copied to Bug #3739: Incorrect handling of ASN1 relative_offset keyword

**History**

- #1 - 05/20/2020 06:37 PM - Emmanuel Thompson
  - [https://github.com/OISF/suricata/pull/4966](https://github.com/OISF/suricata/pull/4966)

- #2 - 05/22/2020 08:19 AM - Victor Julien
  - Status changed from New to In Review
  - Target version set to 6.0.0rc1
  - Label Needs backport added

- #3 - 06/03/2020 11:37 AM - Jeff Lucovsky
  - Copied to Bug #3738: Incorrect handling of ASN1 relative_offset keyword added

- #4 - 06/03/2020 11:37 AM - Jeff Lucovsky
  - Copied to Bug #3739: Incorrect handling of ASN1 relative_offset keyword added

- #5 - 06/09/2020 11:56 AM - Victor Julien
  - Status changed from In Review to Closed
  - [https://github.com/OISF/suricata/commit/be3379f00e30fd4776c622c27ca60a92e1](https://github.com/OISF/suricata/commit/be3379f00e30fd4776c622c27ca60a92e1)