Suricata - Bug #5183
TLS Handshake Fragments not Reassembled
03/08/2022 12:56 AM - Gianni Tedesco

<table>
<thead>
<tr>
<th>Status:</th>
<th>In Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>High</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Victor Julien</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>7.0rc1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td>6.0.5, 7.0rc1</td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td>Needs Suricata-Verify test, Needs backport to 6.0</td>
</tr>
</tbody>
</table>

**Description**

TLS handshakes can be sent in multiple TLS frames. This is because the handshakes can be larger than the max size of a single frame (24 bits length field, vs 16 bits length field).

Suricata appears not to combine such fragments which means that TLS app-layer rules can be evaded and TLS events can be hidden if suricata is configured to log TLS events.

Attached are two semantically equivalent pcaps which show the same client hello message in wireshark but which produce INVALID_SSL_RECORD and INVALID_HANDSHAKE_MESSAGE anomaly events in Suricata.

**Related issues:**

Related to Optimization #5481: tls: support incomplete API to replace internal buffering

**History**

#1 - 08/05/2022 09:01 AM - Victor Julien
- Priority changed from Normal to High
- Target version changed from TBD to 7.0rc1
- Label Needs backport to 6.0 added

#2 - 08/05/2022 09:39 AM - Victor Julien
- Status changed from New to In Progress
- Assignee changed from OISF Dev to Victor Julien

#3 - 08/05/2022 09:48 AM - Victor Julien
- Label Needs Suricata-Verify test added

#4 - 08/05/2022 10:26 AM - Victor Julien
- Related to Optimization #5481: tls: support incomplete API to replace internal buffering added

#5 - 08/06/2022 08:22 AM - Victor Julien
@Gianni Tedesco are you able to update the frag pcap to not have the server response be out of window?

#6 - 08/08/2022 08:38 AM - Gianni Tedesco
Yes, there must be a bug in the tool, will look into that.

#7 - 08/19/2022 05:52 PM - Victor Julien
- Status changed from In Progress to In Review

https://github.com/OISF/suricata/pull/7738

**Files**

- tls.pcap: 2 KB, 03/08/2022, Gianni Tedesco
- tlsfrag.pcap: 2.08 KB, 03/08/2022, Gianni Tedesco