**Suricata - Feature #2689**

**Normalized HTTP client body buffer**

11/17/2018 12:23 AM - David Wharton

<table>
<thead>
<tr>
<th>Status:</th>
<th>In Review</th>
<th><strong>Priority:</strong></th>
<th>Normal</th>
<th><strong>Assignee:</strong></th>
<th>Philippe Antoine</th>
<th><strong>Category:</strong></th>
<th></th>
<th><strong>Target version:</strong></th>
<th>TBD</th>
<th><strong>Effort:</strong></th>
<th>medium</th>
<th><strong>Difficulty:</strong></th>
<th>low</th>
<th><strong>Label:</strong></th>
</tr>
</thead>
</table>

**Description**

Currently the 'http_uri' buffer is normalized. This is a request to extend the same normalization (URI decode) to the 'http_client_body' buffer.

This would probably require a new keyword (e.g. 'http_client_body_norm'). Or you could do something like 'http_client_body,norm', with the default being 'http_client_body,raw' (meaning, 'http_client_body' would be the same as 'http_client_body,raw'). This would ensure this functionality would not break current rules. However, the proposed keyword nomenclature may not be congruent with current standards or desired direction so this request is not intended to dictate specific implementation, just functionality.

The decoding of the HTTP client body would be done when the content type is recognized as URL encoded. The easy way to do this is to just look for the 'x-www-form-urlencoded' Content-Type header. Heuristic detection is possible but likely not worth the effort or performance impact (although just relying on the client header provides opportunity for bypass).

**Related issues:**

- Related to Task #2685: SuriCon 2018 brainstorm

**History**

**#1 - 11/17/2018 12:44 AM - David Wharton**

This could possibly be implemented as a transform but seems more natural to treat similar to the http_uri normalized buffer. For performance reasons, a hard decode limit could be enforced (e.g. 4000 bytes).

**#2 - 11/21/2018 11:28 AM - Victor Julien**

- Related to Task #2685: SuriCon 2018 brainstorm added

**#3 - 05/23/2019 09:49 PM - Andreas Herz**

- Assignee set to Community Ticket
- Target version set to TBD

**#4 - 11/01/2019 02:51 PM - Andreas Herz**

- Assignee changed from Community Ticket to Philippe Antoine

**#5 - 02/18/2020 12:45 PM - Philippe Antoine**

- Status changed from New to In Review

https://github.com/OISF/suricata/pull/4398