Suricata - Feature #2312
http: parsing for async streams

12/01/2017 03:49 AM - Victor Julien

Status: Closed
Priority: Normal
Assignee: Philippe Antoine
Category:
Target version: 6.0.0rc1
Effort:
Difficulty:

Description
Currently the parser requires traffic from both sides to be useful/effective.

Related issues:
Related to Task #2309: SuriCon 2017 brainstorm

History
#1 - 12/01/2017 03:49 AM - Victor Julien
- Related to Task #2309: SuriCon 2017 brainstorm added

#2 - 11/16/2018 10:12 PM - Raymond Hansen
Jeffrey has created an http parser that we should evaluate for use. Should include http2?

#3 - 11/16/2018 10:12 PM - Pierre Chifflier
- Geoffroy :)

#4 - 06/06/2019 01:51 PM - Philippe Antoine
Currently the parser requires traffic from both sides to be useful/effective.

How so?
From my experience of the code, it is "effective" as it should match signature with http keywords
I did not test it yet but I would like what is expected first.

#5 - 06/06/2019 02:06 PM - Victor Julien
Not sure if this is still true. Some updates were made to libhttp and suricata to allow for this. I think it's a good idea to create some test cases (suricata-verify) for both all request and all response traffic. I'm especially curious how multi-tx sessions work.

#6 - 09/27/2019 08:23 AM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Philippe Antoine

Philippe, can you make some SV tests for this? TS only, TC only. Checking logging, file extraction, signature matching?

#7 - 01/21/2020 09:03 AM - Victor Julien
- Target version changed from TBD to 6.0.0rc1

#8 - 02/18/2020 12:44 PM - Philippe Antoine
- Status changed from Assigned to In Review

https://github.com/OISF/suricata-verify/pull/143

06/12/2020
#9 - 03/21/2020 02:32 PM - Philippe Antoine

- Status changed from In Review to Closed

https://github.com/OISF/suricata-verify/pull/143