Suricata - Bug #4672
PR 6336 QA alert deviation
09/10/2021 04:33 PM - Corey Thomas

Status: Closed
Priority: Normal
Assignee:
Category:
Target version:
Affected Versions: git master
Effort: medium
Difficulty: medium
Label: C

Description
Git master had a low alert deviation that happened between QA rebases.

Running against our SURI_TLPR1 test and reverting commits traces back to PR 6336 and commit
https://github.com/OISF/suricata/pull/6336/commits/9b9f909d7db9ba4485bf50577868fa7072998487

Unfortunately the smallest reproducible test so far is TLPR1, which is our largest test and takes over 20minutes to run.

Smaller pcaps with single alerts do not seem to show any loss at small scale.

Running with "toserver" has alert deviation.
https://github.com/ct0br0/suricata/commit/546b7b15d70a9bd0ed8f7356250f5eee5fd0c17e

Commenting out "toclient" lines of the commit do not seem to have any alert drops.

History
#1 - 09/11/2021 06:27 AM - Peter Manev
Seems related mostly to http_useragent/to_server.
I have not found a single stream reproducible case so far.
There are no memcap hits during the run

#2 - 09/13/2021 12:46 PM - Corey Thomas
Neither have I. Alerts that show up in only baseline and only test run have the same type of rules (to_server and some user agents)

#3 - 11/26/2021 06:59 AM - Victor Julien
- Status changed from New to Closed
Fix tracked in #4685

#4 - 12/15/2021 08:01 AM - Victor Julien
- Private changed from Yes to No