Suricata - Bug #3450
signature with sticky buffer with subsequent pcre check in a different buffer loads but will never match
01/27/2020 06:44 PM - Jason Taylor

Status: Closed
Priority: Normal
Assignee: Jeff Lucovsky
Category:
Target version: 5.0.3
Affected Versions: 5.0.1
Effort: 
Difficulty: 
Label: 

Description
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"suri 5 pcre fun"; flow:established,to_server; http.method; content:"POST"; http.uri; content:".php"; http.header; content:"\[0d 0a|User-Agent|0d 0a|"; content:"!Referer|3a 20|"; pcre:"/^(?:[A-F0-9]{2}){200,}$/P";)

This rule loads in suri 5 but does not fire on pcap. It seems that the sticky buffer is set and loads the pcre within the existing sticky buffer even though we specify the buffer for the pcre.

If the pcre is moved to the front of the rule, the rule fires as expected, example:
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"suri 5 pcre fun"; flow:established,to_server; pcre:"/^(?:[A-F0-9]{2}){200,}$/P"; http.method; content:"POST"; http.uri; content:".php"; http.header; content:"\[0d 0a|User-Agent|0d 0a|"; content:"!Referer|3a 20|";)

History
#1 - 01/27/2020 07:13 PM - Victor Julien
What if you reset the sticky buffer before the pcre? By adding a pkt_data; before it.

#2 - 01/28/2020 01:22 PM - Jason Taylor
Victor Julien wrote:

What if you reset the sticky buffer before the pcre? By adding a pkt_data; before it.

Resetting with pkt_data prior to the pcre will result in the rule firing as expected. It will also work if we switch it up to use something like "http.request_body; pcre:"/^(?:[A-F0-9]{2}){200,}$/";"

#3 - 02/06/2020 07:53 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Jeff Lucovsky
- Target version set to 5.0.2

We should probably reject the rule based on the pcre specifying a buffer while a sticky buffer is already active.

#4 - 02/12/2020 01:09 PM - Victor Julien
- Target version changed from 5.0.2 to 5.0.3

#5 - 02/19/2020 02:31 PM - Jeff Lucovsky
- Status changed from Assigned to In Review

https://github.com/OISF/suricata/pull/4570

#6 - 02/25/2020 12:39 PM - Jeff Lucovsky
- Status changed from In Review to Closed

07/16/2022 1/2