Suricata - Bug #3671
Protocol detection evasion by packet splitting
04/24/2020 11:40 AM - Jeff Lucovsky

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category: 
Target version: 4.1.8
Affected Versions: 4.1.7
Difficulty: 
Label: 

Description
Found by oss-fuzz

Output of fuzz target gives:
Assertion failure : With input length 24, found enip instead of dns on attached input

History
#2 - 04/25/2020 06:20 AM - Shivani Bhardwaj
- Priority changed from Normal to Immediate

#3 - 04/26/2020 06:16 PM - Victor Julien
- Assignee changed from Shivani Bhardwaj to Victor Julien

#4 - 04/26/2020 06:16 PM - Victor Julien
- Priority changed from Immediate to High

#5 - 04/27/2020 08:01 PM - Victor Julien
- Status changed from Assigned to In Review

#6 - 04/28/2020 01:28 PM - Victor Julien
- Status changed from In Review to Closed
- Priority changed from High to Normal
- Affected Versions 4.1.7 added
- Affected Versions deleted (5.0.2)

https://github.com/OISF/suricata/commit/2d21be0a5cfe47345fde3ade451ae57aa10eca70

#7 - 04/28/2020 01:33 PM - Victor Julien
- Private changed from Yes to No

Files
clusterfuzz-testcase-minimized-fuzz_applayerprotodetectgetproto-512345678946880.00162020 04/06/2020

05/30/2020