Suricata - Bug #1475

app-layer-modbus: AddressSanitizer error (heap-buffer-overflow)

05/27/2015 09:58 AM - David DIALLO

Status: Closed
Priority: Normal
Assignee: David DIALLO
Category: 
Target version: 3.0RC1
Affected Versions: 
Difficulty: 
Effort: 
Label: 

Description
In processing modbus_test_data_part2.pcap from https://github.com/digitalbond/quickdraw, the following error occurs:
13679 ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60040001eda0 at pc 0x55a799 bp 0x7f920102d7f0 sp 0x7f920102d7e8
READ of size 1 at 0x60040001eda0 thread T1 (PcapFile)
#0 0x55a798 in ModbusExtractUint8 /home/victor/devel/eidps/src/app-layer-modbus.c:394

History
#1 - 05/27/2015 11:20 AM - David DIALLO
- Status changed from New to Resolved
- % Done changed from 80 to 100

#2 - 07/06/2015 04:41 PM - Victor Julien
- Status changed from Resolved to Closed

https://github.com/inliniac/suricata/pull/1509