Suricata - Bug #3628
Incorrect ASN.1 long form length parsing
04/09/2020 03:50 PM - Emmanuel Thompson

Status: Closed
Priority: Normal
Assignee: Emmanuel Thompson
Category: 
Target version: 6.0.0beta1
Affected Versions: 
Difficulty: low
Effort: low
Label: Needs backport to 4.1, Needs backport to 5.0

Description
Currently the definite long form is parsed as an additive length. This

https://github.com/OISF/suricata/blob/suricata-5.0.2/src/util-decode-asn1.c#L157

8.1.3.5 In the long form, the length octets shall consist of an initial octet and one or more subsequent octets.

https://www.itu.int/rec/T-REC-X.690-201508-I/en

A more digestible explanation is given here with an example

For the definite form, if the length is less than 128, you just use a single byte, with the high bit set to zero. Otherwise the high bit is set to one, and the low seven bits set to the length of length. The length is then encoded in that many bytes.

https://www.w3.org/Protocols/HTTP-NG/asn1.html

Related issues:
Copied to Bug #3945: Incorrect ASN.1 long form length parsing  Closed
Copied to Bug #3946: Incorrect ASN.1 long form length parsing  Closed

History
#1 - 05/19/2020 02:13 PM - Emmanuel Thompson
PR:

#2 - 05/19/2020 02:14 PM - Emmanuel Thompson
https://github.com/OISF/suricata/pull/4798

#3 - 06/29/2020 08:51 AM - Victor Julien
- Target version set to 6.0.0beta1

#4 - 07/07/2020 08:31 PM - Victor Julien
- Status changed from New to In Review
https://github.com/OISF/suricata/pull/5065

#5 - 07/07/2020 08:31 PM - Victor Julien
- Label Needs backport to 4.1, Needs backport to 5.0 added

#6 - 07/13/2020 10:09 AM - Victor Julien
Fix in master by https://github.com/OISF/suricata/pull/5145
Backports should work of https://github.com/OISF/suricata/pull/5156
#7 - 07/13/2020 10:09 AM - Victor Julien
- Status changed from In Review to Closed

#8 - 09/18/2020 12:23 PM - Jeff Lucovsky
- Copied to Bug #3945: Incorrect ASN.1 long form length parsing added

#9 - 09/18/2020 12:23 PM - Jeff Lucovsky
- Copied to Bug #3946: Incorrect ASN.1 long form length parsing added