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

Status: New
Priority: Normal
Assignee: Emmanuel Thompson
Category:
Target version:
Affected Versions:
Effort: low
Difficulty: low
Label:

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

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