Suricata - Bug #3739
Incorrect handling of ASN1 relative_offset keyword
06/03/2020 11:37 AM - Jeff Lucovsky

Status: Closed
Priority: Normal
Assignee: Jeff Lucovsky
Category:
Target version: 5.0.4
Affected Versions:
Effort:
Difficulty:
Label:

Description
The relative_offset keyword option allows to read past the front of the buffer with a negative offset, no bounds checking is done on this i32 value and is not relative to the last "content" match

Related issues:
Copied from Bug #3720: Incorrect handling of ASN1 relative_offset keyword

History
#1 - 06/03/2020 11:37 AM - Jeff Lucovsky
- Copied from Bug #3720: Incorrect handling of ASN1 relative_offset keyword added

#2 - 10/05/2020 10:15 PM - Jeff Lucovsky
- Assignee set to Jeff Lucovsky

#3 - 10/05/2020 10:53 PM - Jeff Lucovsky
- Status changed from Assigned to In Review

https://github.com/OISF/suricata/pull/5467

#4 - 10/06/2020 08:24 AM - Victor Julien
- Status changed from In Review to Closed

https://github.com/OISF/suricata/commit/08beba8f465f05aedd72b7b536f714947b00d96e5