Suricata - Bug #3840
Integer overflow in DetectContentPropagateLimits leading to unintended signature behavior
07/23/2020 09:25 AM - Philippe Antoine

Status: Closed
Priority: Normal
Assignee: Philippe Antoine
Category: 
Target version: 6.0.0beta1
Affected Versions: 5.0.3
Effort: 
Difficulty: 
Label: Needs backport, Needs backport to 4.1, Needs backport to 5.0

Description
Found by oss-fuzz:
https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=24105

Reproducer is
alert tcp any any -> any any (msg:"JllWorkAndNoPlay"; content:"threshoBoy"; content:"æ†≤<MrkBoyy"; distance:2147483647"id:0;)
distance:2147483647 is 0x7FFFFFFF aka INT32_MAX
This distance is used to compute a new offset but offset is uint16_t

History
#1 - 07/23/2020 09:31 AM - Philippe Antoine
- Status changed from New to In Review
- Assignee set to Philippe Antoine

Gitlab PR

#2 - 07/29/2020 12:40 PM - Victor Julien
- Status changed from In Review to Closed
- Private changed from Yes to No

https://github.com/OISF/suricata/commit/a99ad4c1e4251c8a4a667d613ccb1fb334a9b268

#3 - 07/30/2020 06:19 AM - Philippe Antoine
- Status changed from Closed to In Review

Merged commit https://github.com/OISF/suricata/pull/5242/commits/a99ad4c1e4251c8a4a667d613ccb1fb334a9b268 only fixes a subset of the problem

#4 - 08/04/2020 05:03 AM - Victor Julien
- Status changed from In Review to Closed

https://github.com/OISF/suricata/commit/61c327dd80f02484481cbea6d48168063ae90a69