Suricata - Bug #3783

Stack overflow in DetectFlowbitsAnalyze

06/26/2020 10:45 AM - Antti Tönkyrä

Status:	Closed		
Priority:	Normal		
Assignee:	Antti Tönkyrä		
Category:			
Target version:	6.0.0beta1		
Affected Versions:		**Difficulty:**	
Effort:		**Label:**	Needs backport to 5.0

Description

When doing torture tests, I discovered a stack overflow in DetectFlowbitsAnalyze. I have made a PR to github @ https://github.com/OISF/suricata/pull/5103

Overflow happens when number of flowbits is sufficiently large which in turn causes array containing FBAnalyze structs to be greater than stack size.

Changeset should apply cleanly to 5.x too.

Related issues:

Copied to Bug #3790: Stack overflow in DetectFlowbitsAnalyze	**Closed**

History

#1 - 06/26/2020 10:48 AM - Antti Tönkyrä

- Description updated

#2 - 06/26/2020 10:55 AM - Antti Tönkyrä

- Description updated

#3 - 06/26/2020 10:59 AM - Victor Julien

- Status changed from New to In Review

- Assignee set to Antti Tönkyrä

- Target version set to 6.0.0beta1

- Label Needs backport to 5.0 added

#4 - 06/26/2020 11:44 AM - Antti Tönkyrä

- Description updated

#5 - 06/27/2020 12:00 PM - Jeff Lucovsky

- Copied to Bug #3790: Stack overflow in DetectFlowbitsAnalyze added

#6 - 07/07/2020 01:38 PM - Victor Julien

- Status changed from In Review to Closed