pfSense Packages - Bug #15080

Suricata process dying due to Hyperscan error - also may randomly segfault

12/10/2023 04:31 AM - Bill Meeks

Status:	Resolved	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Suricata	**Estimated time:**	0.00 hour
Target version:			
Plus Target Version:		**Affected Plus Version:**	23.09
Affected Version:	2.7.x	**Affected Architecture:**	amd64

Description

Several users on the Netgate Forum are reporting random issues with Suricata failing due to the following Hyperscan error.

Error: spm-hs: Hyperscan returned fatal error -1.

For some users Suricata will error out on startup. But for others, it will run for some random period of time before emitting the Hyperscan error and halting.

History

#1 - 12/10/2023 04:50 AM - Bill Meeks

Pull request 1333 for the RELENG_2_7_2 branch of FreeBSD-ports has been submitted to address this issue.

https://github.com/pfsense/FreeBSD-ports/pull/1333

#2 - 12/11/2023 06:24 PM - Jim Pingle

- Status changed from New to Resolved

- % Done changed from 0 to 100

PRs merged, thanks!

#3 - 12/20/2023 05:18 PM - Bill Meeks

Additional update for this issue for a complete history:

Two additional heap memory buffer overflow bugs were recently discovered in the custom Legacy Blocking Module code used with Suricata on pfSense. Those memory overflows were found during testing with the llvm ASAN tool enabled. It is highly likely these memory buffer overflows contributed to the Hyperscan bug and to other Signal 11 segfault bugs experienced when using Legacy Blocking Mode with Suricata 7.x. The newly identified bugs were fixed in this pull request: https://github.com/pfsense/FreeBSD-ports/pull/1337.

#4 - 12/20/2023 07:08 PM - Jim Pingle

PR merged, thanks!