

Suricata - Bug #3158

'wrong thread' tracking inaccurate for bridging IPS modes

09/09/2019 07:31 AM - Victor Julien

Status: Closed	
Priority: Normal	
Assignee: Victor Julien	
Category:	
Target version: 5.0rc1	
Affected Versions:	Difficulty:
Effort:	Label:
Description When using IPS with AF_PACKET the worker threads are created per interface. So a connection/flow will be handled one interface for one side of the traffic and another interface for the opposing side. This means that by design different threads process a single flow. The code should consider this when checking the 'wrong thread' logic. AF_PACKET and NETMAP are affected.	
Related issues: Related to Support #2725: stream/packet on wrong thread	
	Feedback

History

#1 - 09/09/2019 07:31 AM - Victor Julien

- Related to Support #2725: stream/packet on wrong thread added

#2 - 09/09/2019 07:32 AM - Victor Julien

- Description updated

#3 - 09/20/2019 09:39 PM - Andreas Herz

- Assignee set to OISF Dev

- Target version set to TBD

#4 - 09/21/2019 03:28 AM - Srini J

Hi Team,

Any estimate as to when this might be fixed? We are using NETMAP IPS mode and are affected by this issue.

Thanks,

Sj

#5 - 09/23/2019 05:42 AM - Victor Julien

- Status changed from New to Closed

- Assignee changed from OISF Dev to Victor Julien

- Target version changed from TBD to 5.0rc1

Should be fixed in the git master:

<https://github.com/OISF/suricata/pull/4188>

<https://github.com/OISF/suricata/pull/4188/commits/7cabb025ea530cc97b033cbca55e87053a32fd00>

#6 - 09/24/2019 11:06 AM - Srini J

Victor Julien wrote:

Should be fixed in the git master:

<https://github.com/OISF/suricata/pull/4188>

<https://github.com/OISF/suricata/pull/4188/commits/7cabb025ea530cc97b033cbca55e87053a32fd00>

Thanks you for the quick response. Will try it out.

Regards,
Sj