Suricata - Bug #2552

"Drop" action is logged as "allowed" in af_packet and netmap modes

07/24/2018 02:20 PM - Alexander Gozman

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Eric Leblond</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>4.1rc2</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
</tbody>
</table>

Description
Version: current git master.

It seems that commit 4474889667d664a66c1c123f4f7d2756e8a7fbb9 has broken AFPRunModeIsIPS() and NetmapRunModeIsIPS(). These functions are called from ParseInterfacesList() and work with 'real' live devices list. However, when ParseInterfacesList() is called, the list is empty because LiveDeviceFinalize() was not called yet. As a result, EngineModeSetIPS() is not called and this obviously breaks logging and, probably, some other things.

Currently I have no idea how to do things right (in other words, correct and good looking). Probably we need to move some blocks from ParseInterfacesList() to somewhere else, after LiveDeviceFinalize().

History
#1 - 07/24/2018 03:11 PM - Eric Leblond
- Assignee set to Eric Leblond

#2 - 07/24/2018 03:33 PM - Eric Leblond
Thanks Alexander for the very detailed report. I have implemented your suggestion.

Could you try the following branch: https://github.com/regit/suricata/tree/bug-2552 ?

#3 - 07/24/2018 03:42 PM - Alexander Gozman

Eric Leblond wrote:

Thanks Alexander for the very detailed report. I have implemented your suggestion.

Could you try the following branch: https://github.com/regit/suricata/tree/bug-2552 ?

Eric, thank you for the quick feedback. Tried the patch, everything works fine (logged action is "blocked").

#4 - 08/04/2018 08:03 AM - Victor Julien
- Status changed from New to Closed
- Target version set to 4.1rc2

https://github.com/OISF/suricata/pull/3434

#5 - 08/04/2018 08:04 AM - Victor Julien

Does this affect 4.0.x?

#6 - 08/04/2018 10:28 AM - Alexander Gozman

Victor Julien wrote:

Does this affect 4.0.x?

IMHO no, because 4.0.x handles "live devices" in an old way. There's no LiveDeviceFinalize() there.