Suricata - Bug #1714

Kernel panic on application exit with netmap Suricata 3.0 stable

02/19/2016 04:57 AM - Vadim Fedorenko

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>High</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Aleksey Katargin</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>3.1rc1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

Description

I've got kernel panic on application exit when I use netmap to capture traffic in IDS mode. The problem is in NetmapClose function, in the rings freeing order. Changing the order to make NR_REG_SW ring to free first solves the problem.

Patch attached.

History

#1 - 02/19/2016 05:04 AM - Victor Julien
If you submit it as git patch you can become part of the git history.

#2 - 02/19/2016 05:06 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Aleksey Katargin
- Target version changed from 3.0.1RC1 to 70

Aleksey, are you able to have a look at this?

#3 - 02/19/2016 05:21 AM - Aleksey Katargin
Vadim, which netmap and OS version do you use? Could you submit any kind of kernel panic info? It seems to me it could be a bug in netmap, cuz order must not be important.

#4 - 02/19/2016 05:44 AM - Vadim Fedorenko
Well, I'm using CentOS 6.7 based Linux with 4.1.16 kernel built from elrepo spec and the latest git netmap. I've opened netmap ticket also.

#5 - 02/19/2016 10:01 AM - Peter Manev
Vadim - can you please share the compile/install steps that you did for netmap (I would like to run a short cross ref on 3.16 and 4.4 kernel). Thanks.

#6 - 02/19/2016 11:19 AM - Vadim Fedorenko
So, compile/install steps for netmap:

git clone https://github.com/luigirizzo/netmap.git

Assuming src/linux-4.1.16 is a linux kernel source tree.
Then rmmod ixgbe & modprobe ixgbe - this loads ixgbe module with netmap module as dependency.

For suricata:

./configure --enable-libnet --enable-af-packet --enable-netmap --enable-pie --enable-gcc-march-native --prefix=/usr/ --sysconfdir=/etc/ --localstatedir=/var/
make install && make install-conf

03/17/2022 1/2
To properly start listening on eth1:

```bash
ethtool -K eth1 tso off tx off sg off && ethtool -G eth1 rx 4096 tx 4096 && ethtool -A eth1 rx off tx off
```

echo 66000 > /sys/module/netmap/parameters/ring_size

```
suricata --netmap=eth1
```

Such behavior reproduces with default config and no rules loaded.

**#7** - 02/19/2016 10:44 PM - Aleksey Katargin

Vadim, can you you test suricata with this netmap version?
https://github.com/luigirizzo/netmap/commit/60d516a6e43858e2a768ea48e5214eea614da4e

**#8** - 02/19/2016 11:53 PM - Vadim Fedorenko

Aleksey,
The version of netmap i've used includes this commit.
As I said before, I've use git clone netmap.git to get the latest version from github.

**#9** - 02/20/2016 12:02 AM - Aleksey Katargin

Vadim,
I know that this commit is included in the master branch of netmap.
If this issue is related with latest changes in netmap, you can try older version and figure this out and then use git bisect to address bogus commit.
In our production systems (not suricata) we tried to use more recent netmap version, but sometimes we got failures with it.

**#10** - 02/20/2016 12:57 AM - Vadim Fedorenko

Aleksey,
Ok, I'll try. I have another instance with Suricata 2.1beta4 with netmap support and netmap version at 31.03.2015. I'll update this instance to Suricata 3.0 without updating netmap. I'll write feedback soon.

**#11** - 02/20/2016 02:44 AM - Vadim Fedorenko

Aleksey,
Well, on linux-3.19.3 with netmap version at 31.03.2015 everything seems to be OK. I'll try to examine netmap's source code changes to understand what's went wrong. The ticket in netmap's github repo is opened, #144

**#12** - 02/20/2016 02:45 AM - Aleksey Katargin

This may be helpful for you https://git-scm.com/book/en/v2/Git-Tools-Debugging-with-Git

**#13** - 02/20/2016 04:26 PM - Vadim Fedorenko

While Netmap ticket is in investigation I think we can use the patch to work with latest netmap. The pull request was send via email.

**#14** - 05/21/2016 02:54 AM - Victor Julien

- Priority changed from Normal to High

**#15** - 05/27/2016 03:54 AM - Victor Julien

https://github.com/luigirizzo/netmap/issues/144

**#16** - 05/27/2016 10:02 AM - Victor Julien

- Status changed from Assigned to Closed
- Target version changed from 70 to 3.1rc1

https://github.com/inliniac/suricata/pull/2106

**Files**

- source-netmap.c.diff 575 Bytes 02/19/2016 Vadim Fedorenko