Suricata - Support #3183

Dropping privileges on debian. Permission denied to bind to socket

09/22/2019 04:25 AM - Daniel Vein

Status: Closed
Priority: Normal
Assignee:
Category:
Affected Versions: 4.1.2

Description
user@debian:~$ sudo suricata -f /etc/suricata/suricata.yaml -q 0 --user suri --group suri
21/9/2019 -- 23:02:23 - <Notice> - This is Suricata version 4.1.2 RELEASE
21/9/2019 -- 23:02:40 - <Warning> - [ERRCODE: SC_ERR_INITIALIZATION(45)] - Unix socket: UNIX socket bind(/var/run/suricata-command.socket) error: Permission denied
21/9/2019 -- 23:02:40 - <Warning> - [ERRCODE: SC_ERR_INITIALIZATION(45)] - Unable to create unix command socket
21/9/2019 -- 23:02:40 - <Notice> - all 10 packet processing threads, 4 management threads initialized, engine started.

History
#1 - 09/22/2019 08:58 PM - Daniel Vein
You can close this support ticket. I was able to figure it out looking at Bug #1973. I needed to change the default debian suricata.yaml and change /var/run/suricata-command.socket to /var/run/suricata/suricata-command.socket, then create the dir /var/run/suricata and give it the proper permissions.

On another note the debian suricata package doesn't ship with suricata-update and instead is packaged with oinkmaster, but when I update the rules and run it, I get a bunch of flowbit errors...

#2 - 09/23/2019 08:26 PM - Andreas Herz
- Status changed from New to Closed

The issue with suricata-update will be adressed by the debian team :)

06/13/2020