"Failed to attach filter: Cannot allocate memory" being thrown on some systems but not others that are seemingly identical.

Running 6.0.2 and am running into this issue on a few systems. They are seemingly identical, but for some reason the BPF errors on one, but not another.

And on a working system...

And on a working system...

03/14/2022 08:03 PM - Zane B-H
For the ruleset...

    not ( host 141.206.161.42 and port 514 ) and
    not ( host 141.206.161.42 and port 1514 ) and
    not ( host 141.206.161.42 and port 2514 ) and
    not ( host 141.206.161.42 and port 3514 ) and
    not ( host 141.206.161.42 and port 4514 ) and
    not ( host 141.206.161.42 and port 5514 ) and
    not ( host 141.206.161.42 and port 6514 ) and
    not ( host 141.206.161.42 and port 7514 ) and
    not ( host 141.206.161.42 and port 8514 ) and
    not ( host 141.206.161.42 and port 9514 ) and
    not ( host 2.2.2.1 and port 514 ) and
    not ( host 2.2.2.1 and port 1514 ) and
    not ( host 2.2.2.1 and port 2514 ) and
    not ( host 2.2.2.1 and port 3514 ) and
    not ( host 2.2.2.1 and port 4514 ) and
    not ( host 2.2.2.1 and port 5514 ) and
    not ( host 2.2.2.1 and port 6514 ) and
    not ( host 2.2.2.1 and port 7514 ) and
    not ( host 2.2.2.1 and port 8514 ) and
    not ( host 2.2.2.1 and port 9514 ) and
    not ( host 10.128.134.100 and port 514 ) and
    not ( host 10.128.134.100 and port 1514 ) and
    not ( host 10.128.134.100 and port 2514 ) and
    not ( host 10.128.134.100 and port 3514 ) and
    not ( host 10.128.134.100 and port 4514 ) and
    not ( host 10.128.134.100 and port 5514 ) and
    not ( host 10.128.134.100 and port 6514 ) and
    not ( host 10.128.134.100 and port 7514 ) and
    not ( host 10.128.134.100 and port 8514 ) and
    not ( host 10.128.134.100 and port 9514 ) and
    not port 3260

---

**History**

#1 - 02/01/2022 09:18 PM - Peter Manev

Are both systems the same? (kernel/OS etc?)

#2 - 02/01/2022 09:57 PM - Zane B-H

Peter Manev wrote in #note-1:

> Are both systems the same? (kernel/OS etc?)

So been poking at this a bit more, it appears that our systems running 4.19.67-2+deb10u2 appear to specifically be bumping into this in some cases, just that those appear to be running slightly smaller rule sets in general than our ones running 4.9.30-2+deb9u5. Though we had some larger ones running on both, but it is looking like not.

Going to poke at that angle some more than I get a chance tomorrow.

#3 - 02/01/2022 10:15 PM - Zane B-H

Peter Manev wrote in #note-1:

> Are both systems the same? (kernel/OS etc?)

More testing and nearly certain it is a bug in 4.19.67-2+deb10u2. Throwing large BFPs at it for other things besides suricata results in the same.

#4 - 02/13/2022 08:41 PM - Victor Julien

- Priority changed from High to Normal

So it seems to not be a Suricata issue?
- Tracker changed from Bug to Support
- Status changed from New to Closed