When running 2 x 8100 vlan tags within my data the packets are parsed neatly into the eve.json log file in the format "vlan": [123,987]. We have just added a third tag to this data and despite being able to validate the tags in pcaps, the traffic is no longer be parsed into the eve.json log at all.

Is this a system limitation or a bug?

Thanks

History

#1 - 02/14/2019 10:44 AM - Victor Julien
Currently Suricata will only deal with a max of 2 vlans per packet.

#2 - 02/14/2019 10:56 AM - Tony Gumbrell
Thanks for the speedy response. Is it on the roadmap to resolve this?

#3 - 02/14/2019 10:58 AM - Victor Julien
- Tracker changed from Bug to Feature
- Subject changed from 3 VLAN tags breaks eve.json to vlan: support more than 2 layers
- Affected Versions deleted (4.1)

Not yet, but you're not the first to bring this up. So I think it should be addressed.

#4 - 05/23/2019 09:40 PM - Andreas Herz
- Assignee set to OISF Dev
- Target version set to TBD

#5 - 09/26/2019 08:58 AM - Victor Julien
- Target version changed from TBD to 6.0.0beta1

#6 - 01/30/2020 01:26 PM - Victor Julien
- Label Protocol added

#7 - 04/13/2020 03:22 PM - Victor Julien
- Status changed from New to Assigned
- Assignee changed from OISF Dev to Victor Julien

#8 - 08/04/2020 05:04 AM - Victor Julien
- Target version changed from 6.0.0beta1 to 7.0rc1