Our client uses Cumulus based switch with ERSPAN configured. It seems that Cumulus transfers the traffic as encapsulated ERSPAN Type 1 while Suricata supports only ERSPAN Type 2.

We found the following:
Suricata decodes only ERSPAN Type 2
https://github.com/OISF/suricata/blob/master/src/decode-erspan.c

After removing the condition and allowing Suricata to try and decode different types (tested Type 1), no content was identified due to different header size (32 bit for type 1 instead of 64 bit for type 2).
We were able to compile and test a version that supports type 1 instead of type 2.
Since many vendors that are not Cisco may use ERSPAN Type 1, we believe that it is important to have support for both ERSPAN Types in the stable version.

Can you please assist with the issue?

Thank you

Golan
#6 - 04/10/2020 07:12 AM - Shivani Bhardwaj

- Status changed from In Review to Closed

https://github.com/OISF/suricata/pull/4797

<table>
<thead>
<tr>
<th>Files</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>record3.pcap</td>
<td>6.42 KB</td>
<td>12/18/2019</td>
<td>Golan Sharon</td>
</tr>
</tbody>
</table>