**Suricata - Feature #3481**

**GRE ERSPAN Type 1 Support**

02/17/2020 04:43 PM - Jeff Lucovsky

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Jeff Lucovsky</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>5.0.3</td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td>medium</td>
</tr>
</tbody>
</table>

**Label:** Needs backport, Protocol

**Description**

[backport issue for 5.0.x] Hello Team

Our client uses Cumulus based switch with ERSPAN configured. It seems that Cumulus transfer the traffic as encapsulated ERSPAN Type 1 while Suricata support 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

```c
#line 60> /* only v1 is tested at this time */
#line 61> if (version != 1)
```

After removing the condition and allowing Suricata to try and decode different types (tested Type 1), no content was identify due to different header size (32bit 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

**Related issues:**

- Copied from Feature #3422: GRE ERSPAN Type 1 Support [Closed]
- Copied to Feature #3482: GRE ERSPAN Type 1 Support [Closed]
- Copied to Task #3515: GRE ERSPAN Type 1 Support configuration [In Review]

**History**

#1 - 02/17/2020 04:43 PM - Jeff Lucovsky
- Copied from Feature #3422: GRE ERSPAN Type 1 Support added

#2 - 02/17/2020 04:44 PM - Jeff Lucovsky
- Copied to Feature #3482: GRE ERSPAN Type 1 Support added

#3 - 02/29/2020 01:32 PM - Jeff Lucovsky
ERSPAN Type I handling should be disabled by default.

#4 - 03/03/2020 01:56 PM - Jeff Lucovsky
- Status changed from New to In Review

https://github.com/OISF/suricata/pull/4627

#5 - 03/05/2020 01:37 PM - Jeff Lucovsky

---

06/13/2020 1/2
Copied to Task #3515: GRE ERSPAN Type 1 Support configuration added

#6 - 03/26/2020 01:43 PM - Jeff Lucovsky
- Status changed from In Review to Closed

Merged in https://github.com/OISF/suricata/pull/4728

<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>