Suricata - Bug #4810

pppoe decoder fails when protocol identity field is only 1 byte

11/08/2021 10:58 AM - Steven Ottenhoff

Status: Assigned
Priority: Normal
Assignee: Steven Ottenhoff
Category: Target version: 7.0rc1
Affected Versions: git master
Effort: Difficulty: 
Label: C, Needs backport to 5.0, Needs backport to 6.0, Protocol

Description
We have encountered setups where the ppp protocol field is only one byte, which is valid according to rfc2516. In this case the pppoe decoder will fail as it will always uses 2 bytes to try match the protocol identifier.

We created a fix which will check if the two bytes will conform to the hdlc address extension. If not it will assume a 1 byte protocol field. I'm not sure there won't be corner cases but it will not break with 2 bytes protocol fields.

We encountered the issue with the pppoe decoder but probably this issue might also be relevant for the ppp decoder. The same fix could be applied (shared) there.

If I can have a developer role I can assign this ticket to myself present a merge request.

Related issues:
Copied to Bug #4824: pppoe decoder fails when protocol identity field is only... Assigned
Copied to Bug #4825: pppoe decoder fails when protocol identity field is only... Assigned

History
#1 - 11/08/2021 11:22 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Steven Ottenhoff
- Target version set to 7.0rc1
- Label Needs backport to 5.0, Needs backport to 6.0 added

Thanks Steven. I've also tagged it for backports. This will require no action on your side.

#2 - 11/11/2021 02:22 PM - Jeff Lucovsky
- Copied to Bug #4824: pppoe decoder fails when protocol identity field is only 1 byte added

#3 - 11/11/2021 02:23 PM - Jeff Lucovsky
- Copied to Bug #4825: pppoe decoder fails when protocol identity field is only 1 byte added