OsmoSTP - Bug #4236

osmo-stp segfaults if IPA client sends unparseable SCCP

10/19/2019 03:27 PM - laforge

<table>
<thead>
<tr>
<th>Status:</th>
<th>Resolved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>High</td>
</tr>
<tr>
<td>Assignee:</td>
<td>laforge</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Spec Reference:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

When an IPA ASP is sending a SCCP message that cannot be parsed, osmo-stp currently crashes in `ipa_rx_msg_sccp()` which doesn't anticipate `@patch_sccp_with_pci` returning NULL.

**Related issues:**
Related to OsmoSTP - Feature #4219: IPA: no point code insertion to SCCP

**Associated revisions**

Revision d747573f - 10/19/2019 03:47 PM - laforge

ipa: Fix crash when parsing of received IPA SCCP message fails

- Related to Feature #4219: IPA: no point code insertion to SCCP added

**Change-Id:** Ib7a8c2a36dd1b82ca8ed472760c1682ede50cb90

Fixes: OS#4236

**History**

#1 - 10/19/2019 03:28 PM - laforge

- % Done changed from 0 to 40

Patch available in [https://gerrit.osmocom.org/c/libosmo-sccp/+/15813](https://gerrit.osmocom.org/c/libosmo-sccp/+/15813)

#2 - 10/19/2019 03:28 PM - laforge

- Related to Feature #4219: IPA: no point code insertion to SCCP added

#3 - 10/20/2019 09:44 AM - laforge

- % Done changed from 40 to 80

patch merged

#4 - 11/05/2019 04:40 PM - laforge

- Status changed from In Progress to Resolved
- % Done changed from 80 to 100