

# OsmoSGSN - Bug #4173

## pdp crash when lib pointer null

08/25/2019 12:22 AM - lynxis

<b>Status:</b>	Closed	<b>Start date:</b>	08/25/2019
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	lynxis	<b>% Done:</b>	100%
<b>Category:</b>			
<b>Target version:</b>			
<b>Spec Reference:</b>			
<b>Description</b>			
<pre>Type "apropos word" to search for commands related to "word"... Reading symbols from /usr/bin/osmo-sgsn...done. [New LWP 22489] [Thread debugging using libthread_db enabled] Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1". Core was generated by `/usr/bin/osmo-sgsn -c /etc/osmocom/osmo-sgsn.cfg'. Program terminated with signal SIGSEGV, Segmentation fault. #0  gsm48_tx_gsm_act_pdp_acc (pdp=0x560fba776920) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c :2535 2535      msgb_v_put(msg, pdp-&gt;lib-&gt;radio_pri); (gdb) bt #0  gsm48_tx_gsm_act_pdp_acc (pdp=0x560fba776920) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c :2535 #1  0x0000560fb82ebd08 in do_act_pdp_req (mmctx=mmctx@entry=0x560fba7acfb0, msg=msg@entry=0x560fba 94a820, delete=delete@entry=0x7fff093b068f) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:2826 #2  0x0000560fb82ec677 in gsm48_rx_gsm_act_pdp_req (_msg=0x560fba9489f0, mmctx=0x560fba7acfb0) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:2939 #3  gsm0408_rcv_gsm (mmctx=mmctx@entry=0x560fba7acfb0, msg=msg@entry=0x560fba9489f0, llme=llme@ent ry=0x560fba7abe70) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:3050 #4  0x0000560fb82efc66 in gsm0408_gprs_rcvmsg_gb (msg=msg@entry=0x560fba9489f0, llme=0x560fba7abe7 0, drop_cipherable=drop_cipherable@entry=false) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:3 188 #5  0x0000560fb82fe98d in gprs_llc_rcvmsg (msg=0x560fba9489f0, tv=&lt;optimized out&gt;) at ../../../../sr c/osmo-sgsn/src/gprs/gprs_llc.c:1003 #6  0x00000000000019acd in ?? () #7  0x00007f71d8ba9b83 in bssgp_rx_ul_ud (ctx=&lt;optimized out&gt;, ctx=&lt;optimized out&gt;, tp=&lt;optimized out&gt;, msg=&lt;optimized out&gt;) at ../../../../src/libosmocore/src/gb/gprs_bssgp.c:418 #8  bssgp_rx_ptp (bctx=&lt;optimized out&gt;, tp=&lt;optimized out&gt;, msg=&lt;optimized out&gt;) at ../../../../sr c/libosmocore/src/gb/gprs_bssgp.c:877 #9  bssgp_rcvmsg (msg=0x560fba9489f0) at ../../../../src/libosmocore/src/gb/gprs_bssgp.c:1100 #10 0x00007f71d8ba9cac in gprs_ns_rx_unitdata (msg=0x560fba9489f0, nsvc=0x560fba5faed0) at ../../. ../../src/libosmocore/src/gb/gprs_ns.c:1143 #11 gprs_ns_process_msg (nsi=nsi@entry=0x560fba5c19d0, msg=msg@entry=0x560fba9489f0, nsvc=nsvc@ent ry=0x7fff093b28c8) at ../../../../src/libosmocore/src/gb/gprs_ns.c:1778 #12 0x00007f71d8bab72d in gprs_ns_rcvmsg (nsi=nsi@entry=0x560fba5c19d0, msg=msg@entry=0x560fba9489 f0, saddr=saddr@entry=0x7fff093b2910, ll=ll@entry=GPRS_NS_LL_UDP) at ../../../../src/libosmocore/s rc/gb/gprs_ns.c:1527 #13 0x00007f71d8bab85f in handle_nsip_read (bfd=0x560fba5c1a00) at ../../../../src/libosmocore/src /gb/gprs_ns.c:1993 #14 nsip_fd_cb (bfd=0x560fba5c1a00, what=1) at ../../../../src/libosmocore/src/gb/gprs_ns.c:2026 #15 0x00007f71d875cc1 in osmo_fd_disp_fds (_eset=0x7fff093b2a80, _wset=0x7fff093b2a00, _rset=0x7f ff093b2980) at ../../../../src/libosmocore/src/select.c:223 #16 osmo_select_main (polling=&lt;optimized out&gt;) at ../../../../src/libosmocore/src/select.c:263 #17 0x0000560fb82e6bcf in main (argc=3, argv=0x7fff093b2cc8) at ../../../../src/osmo-sgsn/src/gprs /sgsn_main.c:527 (gdb) fraem 2 Undefined command: "fraem".  Try "help". (gdb) frame 2 #2  0x0000560fb82ec677 in gsm48_rx_gsm_act_pdp_req (_msg=0x560fba9489f0, mmctx=0x560fba7acfb0) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:2939 2939      rc = do_act_pdp_req(mmctx, msg, &amp;delete);</pre>			

```
(gdb) print
The history is empty.
(gdb) print mmctx
$1 = (struct sgsn_mm_ctx *) 0x560fba7acfb0
(gdb) frame 0
#0  gsm48_tx_gsm_act_pdp_acc (pdp=0x560fba776920) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c
:2535
2535     msgb_v_put(msg, pdp->lib->radio_pri);
(gdb) p pdp
$2 = (struct sgsn_pdp_ctx *) 0x560fba776920
(gdb) p pdp->lib
$3 = (struct pdp_t *) 0x0
(gdb) p pdp->lib
$4 = (struct pdp_t *) 0x0
(gdb)
(gdb) p mmctx->pmm_state
$6 = MM_READY
```

## History

---

### #1 - 08/29/2019 12:45 PM - pespin

- Status changed from New to Feedback
- Assignee set to lynxis

I submitted this patch, assigning to [lynxis](#) for him to review it.

<https://gerrit.osmocom.org/c/osmo-sgsn/+15330> sgsn: Reject PdpActReq if no GTP pdp ctx exists

### #2 - 09/09/2019 09:13 AM - pespin

Patch has been merged. [lynxis](#) please have a look and close the ticket if fine for you.

### #3 - 09/10/2019 12:56 PM - lynxis

- Status changed from Feedback to Closed

LGTM.

### #4 - 09/15/2019 11:28 PM - lynxis

- % Done changed from 0 to 100