Description

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->lib->radio_pri);

(gdb) bt
#0  gsm48_tx_gsm_act_pdp_acc (pdp=0x560fba776920) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:2535
#1  0x0000560fbb82ed08 in do_act_pdp_req (mmctx=mmctx@entry=0x560fba74a820, delete=delete@entry=0x7fff093b068f) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:2826
#2  0x0000560fbb82ec677 in gsm48_rx_gsm_act_pdp_req (_msg=0x560fba9489f0, mmctx=0x560fba74a820) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:2939
#3  gsm0408_rcv_gsm (mmctx=mmctx@entry=0x560fba74a820, msg=msg@entry=0x560fba9489f0, llme=llme@entry=0x560fba7abe70) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:3050
#4  0x0000560fbb826fc66 in gsm0408_gprs_rcvmsg_gb (msg=msg@entry=0x560fba9489f0, llme=0x560fba7abe70, drop_cipherable=drop_cipherable@entry=false) at ../../../../src/osmo-sgsn/src/gprs/gprs_gmm.c:3188
#5  0x0000560fbb82ef98d in gprs_llc_rcvmsg (msg=0x560fba9489f0, tv=optimized out) at ../../../../src/osmo-sgsn/src/gprs/gprs_llc.c:1003
#6  0x0000000000019acd in ?? ()
#7  0x00007f71d8baf8b3 in bssgp_rx_ul_ud (ctx=optimized out), ctx=optimized out, tp=optimized out) at ../../../src/libosmocore/src/gb/bssgp_ssgp.c:418
#8  bssgp_rx_ptp (ctx=optimized out), tp=optimized out), msg=optimized out) at ../../../src/libosmocore/src/gb/bssgp_ssgp.c:877
#9  bssgp_rcvmsg (msg=0x560fba9489f0) at ../../../src/libosmocore/src/gb/bssgp_ssgp.c:1100
#10 0x00007f71d8ba9ac in gprs_ns_rx_unitdata (msg=0x560fba9489f0, nsvec=0x560fba5faed0) at ../../../src/libosmocore/src/gb/gprs_ns.c:1143
#11 gprs_ns_process_msg (nsi=nsi@entry=0x560fba5c19d0, msg=msg@entry=0x560fba9489f0, nsvec=nsvec@entry=0x7fff093b28c8) at ../../../src/libosmocore/src/gb/gprs_ns.c:1778
#12 0x00007f71d8bab72d in gprs_ns_rccmsg (nsi=nsi@entry=0x560fba5c19d0, msg=msg@entry=0x560fba9489f0, saddr=saddr@entry=0x7fff093b2910, ll=ll@entry=GPRS_NS_LL_UDP) at ../../../src/libosmocore/src/gb/gprs_ns.c:1527
#13 0x00007f71d8bab85f in handle_nisp_read (bfd=0x560fba5c1a00) at ../../../src/libosmocore/src/gb/gprs_ns.c:1993
#14 nisp_fd_cb (bfd=0x560fba5c1a00, what=1) at ../../../src/libosmocore/src/gb/gprs_ns.c:2026
#15 0x00007f71d875ce1 in osmo_fdDisp fds (_eset=0x7fff093b2a80, _wset=0x7fff093b2a00, _rset=0x7fff093b2980) at ../../../src/libosmocore/src/select.c:223
#16 osmo_select_main (polling=optimized out) at ../../../src/libosmocore/src/select.c:263
#17 0x0000560fbb26bce6 in main (argc=3, argv=0x7fff093b2cc0) at ../../../src/osmo-sgsn/src/gprs/gprs_main.c:257
(gdb) frame 2
Undefined command: "fraem". Try "help".
(gdb) frame 2
#2  0x0000560fbb26c677 in gsm48_rx_gsm_act_pdp_req (_msg=0x560fba9489f0, mmctx=0x560fba74a820)
2939 rc = do_act_pdp_req(mmctx, msg, &delete);
(gdb) print
The history is empty.
(gdb) print mmctx
$1 = (struct sgsn_mm_ctx *) 0x560fba7acfb0
(gdb) frame 0
$0 gsm48_tk_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) p mmctx->pmm_state
$6 = MM_READY

Associated revisions
Revision 424628d5 - 09/06/2019 07:34 PM - pespin
sgsn: Reject PdpActReq if no GTP pdp ctx exists
It could happen that SGSN drops GTP side of a pdp ctx (pdp->lib=NULL) while still maintaining the other side (to notify about the entire pdp ctx being torn down). If a PdpActReq arrives during that time, we need to account for that situation, otherwise osmo-sgsn crashes accessing pdp->lib.
If no pdp->lib is found at that time, let's reject the request and expect at some point later in time the entire pdp context will be destroyed and reestablished.
Related: OS#4173
Change-Id: I6dd87557ebb26fdbd280504abde10d976acecf64

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