OsmoSGSN - Bug #3964

SIGSEGV in sndcp_sm_deactivate_ind()

04/29/2019 08:41 AM - keith

Status:	New	**Start date:**	04/29/2019
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

```
(gdb) bt
#0  0x000055555556989c in sndcp_sm_deactivate_ind (lle=0x358, nsapi=5 '\005') at gprs_sndcp.c:507
#1  0x000055555556703c in sgsn_pdp_ctx_terminate (pdp=0x5555559a3d00) at gprs_sgsn.c:445
#2  0x0000555555566ac9 in sgsn_mm_ctx_cleanup_free (mm=0x55555591f5e0) at gprs_sgsn.c:337
#3  0x000055555555d658 in mm_ctx_cleanup_free (ctx=0x55555591f5e0, log_text=0x555555589416 "T3350"
) at gprs_gmm.c:326
#4  0x0000555555562d45 in mmctx_timer_cb (_mm=0x55555591f5e0) at gprs_gmm.c:2156
#5  0x00007ffff7308526 in osmo_timers_update () at timer.c:257
#6  0x00007ffff7308d9a in osmo_select_main (polling=0) at select.c:260
#7  0x0000555555572d21 in main (argc=1, argv=0x7fffffffe618) at sgsn_main.c:524
```

Log leading up to this:

```
DMM NOTICE <0002> gprs_gmm.c:2155 MM(334020160307203/f05ed185) T3350 expired >= 5 times
DMM INFO <0002> gprs_gmm.c:319 MM(334020160307203/f05ed185) Cleaning MM context due to T3350
DMM NOTICE <0002> gprs_sgsn.c:336 MM(334020160307203/f05ed185) Dropping PDP context for NSAPI=5
DGPRS INFO <000e> gprs_sgsn.c:441 PDP(334020160307203/0) Forcing release of PDP context
```

in sgsn_pdp_ctx_terminate

```
(gdb) print pdp->mm->gb.llme
$7 = (struct gprs_llc_llme *) 0x0
```

Related issues:

Related to OsmoSGSN - Bug #3957: ABORT from gprs_sndcp_comp_free()	**Feedback**	**04/24/2019**
Related to OsmoSGSN - Bug #4221: create ttcn testcase for T3350 in combinatio...	**New**	**10/08/2019**

History

#1 - 04/29/2019 08:46 AM - keith

- File core.tgz added

#2 - 04/29/2019 03:51 PM - keith

The binary used here was complied from 6de5698c5cba37536679c6228915ddf27eafd8ee

and the following:

```
diff --git a/src/gprs/gprs_gmm.c b/src/gprs/gprs_gmm.c
index 358bff90..cb587eea 100644
--- a/src/gprs/gprs_gmm.c
+++ b/src/gprs/gprs_gmm.c
@@ -1727,6 +1727,12 @@ static int gsm48_rx_gmm_ra_upd_req(struct sgsn_mm_ctx *mmctx, struct msgb *msg,
                        "The MM context cannot be used, RA: %03d-%0*d-%d-%d\n",
                        mmctx->ra.mcc, mmctx->ra.mnc_3_digits, mmctx->ra.mnc,
                        mmctx->ra.lac, mmctx->ra.rac);
+               //mm_ctx_cleanup_free(mmctx, "GPRS RA UPDATE REJ");
+               if (llme)
+                       if (gprs_llgmm_unassign(llme) == 1) {
+                               mmctx->gb.llme = NULL;
+                               llme = NULL;
```

```
+                       }
                mmctx = NULL;
        }

diff --git a/src/gprs/gprs_llc.c b/src/gprs/gprs_llc.c
index acf4b547..12b8d8f0 100644
--- a/src/gprs/gprs_llc.c
+++ b/src/gprs/gprs_llc.c
@@ -371,6 +371,12 @@ static int _bssgp_tx_dl_ud(struct msgb *msg, struct sgsn_mm_ctx *mmctx)
                dup.ms_ra_cap.len = mmctx->ms_radio_access_capa.len;
                dup.ms_ra_cap.v = mmctx->ms_radio_access_capa.buf;

+               if (!mmctx->gb.llme) {
+                       LOGP(DLLC, LOGL_ERROR, "mmctx->gb.llme unset.\n");
+                       msgb_free(msg);
+                       return -EINVAL;
+
+               }
                /* make sure we only send it to the right llme */
                if (!(msgb_tlli(msg) == mmctx->gb.llme->tlli
                      || msgb_tlli(msg) == mmctx->gb.llme->old_tlli)) {
@@ -1082,6 +1088,7 @@ int gprs_llgmm_assign(struct gprs_llc_llme *llme,
                        l->state = GPRS_LLES_UNASSIGNED;
                }
                llme_free(llme);
+               return 1;
        } else
                return -EINVAL;
```

#3 - 04/29/2019 04:09 PM - keith

- Related to Bug #3957: ABORT from gprs_sndcp_comp_free() added

#4 - 10/08/2019 04:21 PM - lynxis

- Related to Bug #4221: create ttcn testcase for T3350 in combination with a PDP context added

#5 - 10/08/2019 04:28 PM - lynxis

One crashed has been fixed by https://gerrit.osmocom.org/c/osmo-sgsn/+/15486

#6 - 10/08/2019 04:29 PM - lynxis

keith I can not find the git commit ref 6de5698c5cba37536679c6228915ddf27eafd8ee

#7 - 10/10/2019 07:04 PM - keith

lynxis sorry about that.

IIRC, this ticket was made during some chaotic hacking at osmodevcon.

I have that commit in my local tree, and the Change ID is I4600e6a137f42f20fdf69637e4a9048b265c1748

https://gerrit.osmocom.org/#/c/osmo-sgsn/+/13799/

but the commit there has a different ref. no idea how that happened.

#8 - 10/10/2019 07:11 PM - keith

```
rhizomatica@deb9rccn:~/src/osmo-sgsn$ git reflog show --all  | grep 6de5698
6de5698c refs/heads/master@{21}: cherry-pick: gprs_sndcp_comp_free: Replace ifelse with switch and better hand
ling of error
```

Does that explain it? cherry-pick creates a new commit, correct?

Anyway, I compared the commits and they are indeed the same.
The one you want is b72141458c2c1ff73e97688233c6341b2eca09a9

Files

core.tgz	1.04 MB	04/29/2019	keith