null deref in gsm48_rx_gmm_ra_upd_req() / bssgp_parse_cell_id() / gsm48_parse_ra()

12/26/2019 01:11 AM - neels

<table>
<thead>
<tr>
<th>Status:</th>
<th>Resolved</th>
<th>Start date:</th>
<th>12/26/2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td>neels</td>
<td>% Done:</td>
<td>100%</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spec Reference:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Description
---

```c
0  gsm48_parse_ra (raid=0x5651660dd19c, buf=buf@entry=0x0) at ../../../../src/libosmocore/src/gsm/gsm48.c:788
  ra...mcc = (buf[0] & 0xf) * 100;
```

(gdb) bt
---

```
0  gsm48_parse_ra (raid=0x5651660dd19c, buf=buf@entry=0x0) at ../../../../src/libosmocore/src/gsm/gsm48.c:788
1  0x0000007f5176b6e49 in bssgp_parse_cell_id (raid=<optimized out>, buf=0x0) at ../../../../src/libosmocore/src/gb/gprs_bssgp.c:252
2  0x0000007f516543b08d in gsm48_rx_gmm_ra_upd_req (mmctx=0x5651660dd140, msg=0x5651660e1cc0, llme=0x0) at ../../../../src/osmo-sgsn/src/sgsn/gprs_gmm.c:1646
3  0x0000007f5176b8e81 in talloc_named_const () from /usr/lib/x86_64-linux-gnu/libtalloc.so.2
```

hotfix would be
---

```
--- a/src/sgsn/gprs_gmm.c
+++ b/src/sgsn/gprs_gmm.c
@@ -1642,7 +1642,7 @@ static int gsm48_rx_gmm_ra_upd_req(struct sgsn_mm_ctx *mmctx, struct msgb *msg,
     rate_ctr_inc(&mmctx->ctrg->ctr[GMM_CTR_PKTS_SIG_IN]);
     /* Update the MM context with the new RA-ID */
     if (mmctx->ran_type == MM_CTX_T_GERAN_GB) {
-        bssgp_parse_cell_id(&mmctx->ra, msgb_bcid(msg));
+        if (mmctx->ran_type == MM_CTX_T_GERAN_GB && msgb_bcid(msg)) {
+            bssgp_parse_cell_id(&mmctx->ra, msgb_bcid(msg));
+            /* Update the MM context with the new (i.e. foreign) TLLI */
+            mmctx->gb.tlli = msgb_tlli(msg);
        }
```

but not sure what the root cause is (lynxis?)

History
---

#1 - 01/12/2020 10:54 AM - laforge
- Status changed from New to In Progress
- Assignee set to neels
- % Done changed from 0 to 60

proposed patch by Neels in https://gerrit.osmocom.org/c/osmo-sgsn/+//16744/1

SGSN_Tests_Iu_TG.teran_attach_iu_rau tests exactly for this scenario: A Subscriber / MM context that is so far attached via GERAN, but now receives a RAU via UTRAN/Iu.

#2 - 05/10/2020 09:57 PM - neels

lynxis has indicated various times that he has a proper fix for this, my patch is written with very shallow knowledge of what is really going wrong there.

#3 - 05/10/2020 10:42 PM - neels
- Status changed from In Progress to Resolved
- % Done changed from 60 to 100

above mentioned test passes even though the patch was never merged. Apparently we have merged another fix for that crash? Anyway, the linked patch cannot be harmful and still builds, so merging it anyway.