OsmoSGSN - Bug #3957

ABORT from gprs_sndcp_comp_free()

04/24/2019 12:23 PM - keith

Status:	Feedback	**Start date:**	04/24/2019
Priority:	Normal	**Due date:**	
Assignee:	keith	**% Done:**	90%
Category:			
Target version:			
Spec Reference:			

Description

```
(gdb) bt
#0  signal_handler (signal=6) at sgsn_main.c:144
#1  <signal handler called>
#2  0x00007ffff5402067 in __GI_raise (sig=sig@entry=6)   at ../nptl/sysdeps/unix/sysv/linux/raise.
c:56
#3  0x00007ffff5403448 in __GI_abort () at abort.c:89
#4  0x00007ffff59ae69c in ?? () from /usr/lib/x86_64-linux-gnu/libtalloc.so.2
#5  0x00007ffff59ada37 in _talloc_free ()   from /usr/lib/x86_64-linux-gnu/libtalloc.so.2
#6  0x0000555555567f9d in gprs_sndcp_comp_free (comp_entities=<optimized out>)  at gprs_sndcp_comp
.c:176
#7  0x0000555555573658 in llme_free (llme=0x555555a1b800) at gprs_llc.c:577
#8  gprs_llgmm_assign (llme=llme@entry=0x555555a1b800, old_tlli=old_tlli@entry=2708627144, new_tll
i=new_tlli@entry=4294967295) at gprs_llc.c:1064
#9  0x0000555555565485 in sgsn_mm_ctx_cleanup_free (mm=0x0) at gprs_sgsn.c:365
#10 0x00007ffff7308526 in osmo_timers_update () from /usr/lib/x86_64-linux-gnu/libosmocore.so.12
#11 0x00007ffff7308d9a in osmo_select_main () from /usr/lib/x86_64-linux-gnu/libosmocore.so.12
#12 0x000055555555b9e7 in main (argc=1, argv=0x7fffffffe668) at sgsn_main.c:524
```

llme in llme_free()

```
$85 = {list = {next = 0x100100, prev = 0x200200}, state = GPRS_LLMS_UNASSIGNED,
  tlli = 0, old_tlli = 0, algo = GPRS_ALGO_GEA0, kc = '\000' <repeats 15 times>,
  cksn = 7 '\a', iov_ui = 3547929860, bvci = 4, nsei = 4, lle = {{list = {
        next = 0x0, prev = 0x0}, sapi = 0, llme = 0x555555a1b800,
      state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
          rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
        timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
      t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
          next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
        active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
      vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
      oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
      retrans_ctr = 0, params = {iov_i_exp = 0, t200_201 = 0, n200 = 0,
        n201_u = 0, n201_i = 0, mD = 0, mU = 0, kD = 0, kU = 0}}, {list = {
        next = 0x0, prev = 0x0}, sapi = 1, llme = 0x555555a1b800,
      state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
          rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
        timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
      t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
          next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
        active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
      vu_send = 1, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
      oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
      retrans_ctr = 0, params = {iov_i_exp = 0, t200_201 = 5, n200 = 3,
        n201_u = 400, n201_i = 0, mD = 0, mU = 0, kD = 0, kU = 0}}, {list = {
        next = 0x0, prev = 0x0}, sapi = 2, llme = 0x555555a1b800,
      state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
          rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
        timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
      t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
          next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
```

```
    active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
  vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
  oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
  retrans_ctr = 0, params = {iov_i_exp = 0, t200_201 = 5, n200 = 3,
    n201_u = 270, n201_i = 0, mD = 0, mU = 0, kD = 0, kU = 0}}, {list = {
    next = 0x0, prev = 0x0}, sapi = 3, llme = 0x555555a1b800,
  state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
      rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
    timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
  t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
      next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
    active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
  vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
  oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
  retrans_ctr = 0, params = {iov_i_exp = 27, t200_201 = 5, n200 = 3,
    n201_u = 500, n201_i = 1503, mD = 1520, mU = 1520, kD = 16, kU = 16}}, {
  list = {next = 0x0, prev = 0x0}, sapi = 4, llme = 0x555555a1b800,
  state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
      rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
    timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
  t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
      next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
    active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
  vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
  oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
  retrans_ctr = 0, params = {iov_i_exp = 0, t200_201 = 0, n200 = 0,
    n201_u = 0, n201_i = 0, mD = 0, mU = 0, kD = 0, kU = 0}}, {list = {
    next = 0x0, prev = 0x0}, sapi = 5, llme = 0x555555a1b800,
  state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
      rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
    timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
  t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
      next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
    active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
  vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
  oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
  retrans_ctr = 0, params = {iov_i_exp = 27, t200_201 = 10, n200 = 3,
    n201_u = 500, n201_i = 1503, mD = 760, mU = 760, kD = 8, kU = 8}}, {
  list = {next = 0x0, prev = 0x0}, sapi = 6, llme = 0x555555a1b800,
  state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
      rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
    timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
  t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
      next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
    active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
  vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
  oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
  retrans_ctr = 0, params = {iov_i_exp = 0, t200_201 = 0, n200 = 0,
    n201_u = 0, n201_i = 0, mD = 0, mU = 0, kD = 0, kU = 0}}, {list = {
    next = 0x0, prev = 0x0}, sapi = 7, llme = 0x555555a1b800,
  state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
      rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
    timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
  t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
      next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
    active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
  vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
  oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
  retrans_ctr = 0, params = {iov_i_exp = 0, t200_201 = 20, n200 = 3,
    n201_u = 270, n201_i = 0, mD = 0, mU = 0, kD = 0, kU = 0}}, {list = {
    next = 0x0, prev = 0x0}, sapi = 8, llme = 0x555555a1b800,
  state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
      rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
    timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
  t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
      next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
    active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
```

```
    vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
    oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
    retrans_ctr = 0, params = {iov_i_exp = 0, t200_201 = 20, n200 = 3,
      n201_u = 270, n201_i = 0, mD = 0, mU = 0, kD = 0, kU = 0}}, {list = {
      next = 0x0, prev = 0x0}, sapi = 9, llme = 0x555555a1b800,
    state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
        rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
      timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
    t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
        next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
      active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
    vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
    oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
    retrans_ctr = 0, params = {iov_i_exp = 27, t200_201 = 20, n200 = 3,
      n201_u = 500, n201_i = 1503, mD = 380, mU = 380, kD = 4, kU = 4}}, {
    list = {next = 0x0, prev = 0x0}, sapi = 10, llme = 0x555555a1b800,
    state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
        rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
      timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
    t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
        next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
      active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
    vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
    oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
    retrans_ctr = 0, params = {iov_i_exp = 0, t200_201 = 0, n200 = 0,
      n201_u = 0, n201_i = 0, mD = 0, mU = 0, kD = 0, kU = 0}}, {list = {
      next = 0x0, prev = 0x0}, sapi = 11, llme = 0x555555a1b800,
    state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
        rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
      timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
    t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
        next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
      active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
    vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
    oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
    retrans_ctr = 0, params = {iov_i_exp = 27, t200_201 = 40, n200 = 3,
      n201_u = 500, n201_i = 1503, mD = 190, mU = 190, kD = 2, kU = 2}}, {
    list = {next = 0x0, prev = 0x0}, sapi = 12, llme = 0x555555a1b800,
    state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
        rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
      timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
    t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
        next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
      active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
    vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
    oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
    retrans_ctr = 0, params = {iov_i_exp = 0, t200_201 = 0, n200 = 0,
      n201_u = 0, n201_i = 0, mD = 0, mU = 0, kD = 0, kU = 0}}, {list = {
      next = 0x0, prev = 0x0}, sapi = 13, llme = 0x555555a1b800,
    state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
        rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
      timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
    t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
        next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
      active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
    vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
    oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
    retrans_ctr = 0, params = {iov_i_exp = 0, t200_201 = 0, n200 = 0,
      n201_u = 0, n201_i = 0, mD = 0, mU = 0, kD = 0, kU = 0}}, {list = {
      next = 0x0, prev = 0x0}, sapi = 14, llme = 0x555555a1b800,
    state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
        rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
      timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
    t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
        next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
      active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
    vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
```

```
      oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
      retrans_ctr = 0, params = {iov_i_exp = 0, t200_201 = 0, n200 = 0,
        n201_u = 0, n201_i = 0, mD = 0, mU = 0, kD = 0, kU = 0}}, {list = {
        next = 0x0, prev = 0x0}, sapi = 15, llme = 0x555555a1b800,
      state = GPRS_LLES_UNASSIGNED, t200 = {node = {rb_parent_color = 0,
          rb_right = 0x0, rb_left = 0x0}, list = {next = 0x0, prev = 0x0},
        timeout = {tv_sec = 0, tv_usec = 0}, active = 0, cb = 0x0, data = 0x0},
      t201 = {node = {rb_parent_color = 0, rb_right = 0x0, rb_left = 0x0}, list = {
          next = 0x0, prev = 0x0}, timeout = {tv_sec = 0, tv_usec = 0},
        active = 0, cb = 0x0, data = 0x0}, v_sent = 0, v_ack = 0, v_recv = 0,
      vu_send = 0, vu_recv = 0, vu_recv_last = 0, vu_recv_duplicates = 0,
      oc_i_send = 0, oc_i_recv = 0, oc_ui_send = 0, oc_ui_recv = 0,
      retrans_ctr = 0, params = {iov_i_exp = 0, t200_201 = 0, n200 = 0,
        n201_u = 0, n201_i = 0, mD = 0, mU = 0, kD = 0, kU = 0}}},
  xid = 0x555555c6d200, comp = {proto = 0x5555559b2e10, data = 0x5555559f9b90},
  age_timestamp = 0}
```

Related issues:

Related to OsmoSGSN - Bug #3964: SIGSEGV in sndcp_sm_deactivate_ind()	**New**	**04/29/2019**
Related to OsmoSGSN - Bug #4245: osmo-sgsn hitting assert during osmo-gsm-tes...	**Resolved**	**10/31/2019**

History

#1 - 04/24/2019 12:24 PM - keith

Maybe helps:

```
(gdb) p *(struct gprs_sndcp_comp *)llme->comp->data
$113 = {
  list = {
    next = 0x5555559f9b90,
    prev = 0x5555559f9b90
  },
  entity = 128,
  nsapi_len = 0 '\000',
  nsapi = "\000\000\000\060\001\000\000\000\000\000",
  comp_len = 0 '\000',
  comp = '\000' <repeats 15 times>, "\060",
  algo = {
    pcomp = (RFC_2507 | unknown: 21844),
    dcomp = (V44 | unknown: 21844)
  },
  compclass = SNDCP_XID_VERSION_NUMBER,
  state = 0x0
}
(gdb) p *(struct gprs_sndcp_comp *)llme->comp->proto
$114 = {
  list = {
    next = 0x5555559b2e10,
    prev = 0x5555559b2e10
  },
  entity = 0,
  nsapi_len = 240 '\360',
  nsapi = "\001\000\000\220\233\237UUU\000",
  comp_len = 144 '\220',
  comp = "\000\000\000\000\000\000\000\200\000\000\000\000\000\000\000\000",
  algo = {
    pcomp = RFC_1144,
    dcomp = V42BIS
  },
  compclass = 1436523920,
  state = 0x0
}
(gdb)
```

#2 - 04/24/2019 01:14 PM - laforge

#3 - 04/26/2019 08:06 PM - keith

with commit aed46ec97d22c1eccae3578c0010840c3acede0e

```
==13652== Invalid read of size 4
==13652==    at 0x127428: _bssgp_tx_dl_ud (gprs_llc.c:375)
==13652==    by 0x127428: gprs_llc_tx_ui (gprs_llc.c:809)
==13652==    by 0x113047: mmctx_timer_cb (gprs_gmm.c:2160)
==13652==    by 0x56F1525: osmo_timers_update (in /usr/lib/x86_64-linux-gnu/libosmocore.so.12.0.1)
==13652==    by 0x56F1D99: osmo_select_main (in /usr/lib/x86_64-linux-gnu/libosmocore.so.12.0.1)
==13652==    by 0x10F9E6: main (sgsn_main.c:524)
==13652==  Address 0x9aa8454 is 116 bytes inside a block of size 4,408 free'd
==13652==    at 0x4C29E90: free (vg_replace_malloc.c:473)
==13652==    by 0x7055522: _talloc_free (in /usr/lib/x86_64-linux-gnu/libtalloc.so.2.1.2)
==13652==    by 0x12769F: llme_free (gprs_llc.c:580)
==13652==    by 0x12769F: gprs_llgmm_assign (gprs_llc.c:1084)
==13652==    by 0x115FF0: gsm48_rx_gmm_ra_upd_req (gprs_gmm.c:1811)
==13652==    by 0x1170A5: gsm0408_rcv_gmm (gprs_gmm.c:2007)
==13652==    by 0x118021: gsm0408_gprs_rcvmsg_gb (gprs_gmm.c:2932)
==13652==    by 0x12710C: gprs_llc_rcvmsg (gprs_llc.c:997)
==13652==    by 0x52B2F5A: bssgp_rcvmsg (in /usr/lib/x86_64-linux-gnu/libosmogb.so.6.2.0)
==13652==    by 0x52ACE39: gprs_ns_process_msg (in /usr/lib/x86_64-linux-gnu/libosmogb.so.6.2.0)
==13652==    by 0x52AE7F9: gprs_ns_rcvmsg (in /usr/lib/x86_64-linux-gnu/libosmogb.so.6.2.0)
==13652==    by 0x52AE973: nsip_fd_cb (in /usr/lib/x86_64-linux-gnu/libosmogb.so.6.2.0)
==13652==    by 0x56F1DD3: osmo_select_main (in /usr/lib/x86_64-linux-gnu/libosmocore.so.12.0.1)
```

#4 - 04/27/2019 09:21 AM - pespin

So the problem is basically way down the stack (gsm0408_gprs_rcvmsg_gb) llme is assigned to mmctx->gb.llme, and then llme pointer is passed through all the stack as a parameter. Way up the stack, in gsm48_rx_gmm_ra_upd_req()=>gprs_llgmm_unassign()=>gprs_llgmm_assign(), function llme_free() is called on parameter pointer llme, but mmctx->gb.llme is not set to NULL. As a result, when mmctx->gb.llme is later used after a timer triggers, it will use alreadyfreed memory.

Several problems I see:

- gprs_llgmm_assign(llme) frees llme only on one code path inside it, and it's impossible to distinguish it because it doesn't return a specific code in that code path. So there's no way currently for the caller to know whether llme is freed or not after calling the function. IMHO llme should probably not be freed there and just return a specific return code and freed in the caller.
- In the stack trace where gprs_llgmm_assign(llme) is called (gsm48_rx_gmm_ra_upd_req()=>gprs_llgmm_unassign()=>gprs_llgmm_assign()), mmctx is NULL (it was assigned NULL a bit upwards in gsm48_rx_gmm_ra_upd_req), so we cannot set mmctx->gb.llme=NULL. Thus, this assignment must be done before we do mmctx=NULL.

Following patch is proposed which seems to fix the invalid read/crash for now, but probably bigger refactoring of the code is needed to avoid other kind of issues or incorrect logic:

```
diff --git a/src/gprs/gprs_gmm.c b/src/gprs/gprs_gmm.c
index 358bff90..f8bc80cf 100644
--- a/src/gprs/gprs_gmm.c
+++ b/src/gprs/gprs_gmm.c
@@ -1727,6 +1727,9 @@ 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);
+               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..6cd26cd1 100644
--- a/src/gprs/gprs_llc.c
+++ b/src/gprs/gprs_llc.c
@@ -372,7 +372,7 @@ static int _bssgp_tx_dl_ud(struct msgb *msg, struct sgsn_mm_ctx *mmctx)
                dup.ms_ra_cap.v = mmctx->ms_radio_access_capa.buf;

                /* make sure we only send it to the right llme */
-               if (!(msgb_tlli(msg) == mmctx->gb.llme->tlli
+               if (!mmctx->gb.llme || !(msgb_tlli(msg) == mmctx->gb.llme->tlli
                      || msgb_tlli(msg) == mmctx->gb.llme->old_tlli)) {
                        LOGP(DLLC, LOGL_ERROR,
                             "_bssgp_tx_dl_ud(): Attempt to send Downlink Unitdata to wrong LLME:"
@@ -1082,6 +1082,7 @@ int gprs_llgmm_assign(struct gprs_llc_llme *llme,
                        l->state = GPRS_LLES_UNASSIGNED;
                }
```

```
                llme_free(llme);
+               return 1;
        } else
                return -EINVAL;
```

#5 - 04/27/2019 10:50 AM - keith

New backtrace:

```
Program received signal SIGABRT, Aborted.
0x00007ffff5403067 in __GI_raise (sig=sig@entry=6) at ../nptl/sysdeps/unix/sysv/linux/raise.c:56
56      ../nptl/sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) bt
#0  0x00007ffff5403067 in __GI_raise (sig=sig@entry=6) at ../nptl/sysdeps/unix/sysv/linux/raise.c:56
#1  0x00007ffff5404448 in __GI_abort () at abort.c:89
#2  0x00007ffff7314310 in osmo_panic_default (args=0x7fffffffe060, fmt=<optimized out>) at panic.c:49
#3  osmo_panic (fmt=<optimized out>) at panic.c:84
#4  0x0000555555556c32f in gprs_sndcp_dcomp_term (comp_entity=0x555555b839d0) at gprs_sndcp_dcomp.c:130
#5  0x0000555555556b9ee in gprs_sndcp_comp_free (comp_entities=0x555555d16ba0) at gprs_sndcp_comp.c:172
#6  0x0000555555557ab82 in llme_free (llme=0x555555d7f6c0) at gprs_llc.c:583
#7  0x0000555555557bda2 in gprs_llgmm_assign (llme=0x555555d7f6c0, old_tlli=3166033600, new_tlli=4294967295) at
 gprs_llc.c:1090
#8  0x0000555555566c82 in sgsn_mm_ctx_cleanup_free (mm=0x0) at gprs_sgsn.c:365
#9  0x0000555555555d658 in mm_ctx_cleanup_free (ctx=0x555555999c80, log_text=0x555555589396 "T3350") at gprs_gm
m.c:326
#10 0x0000555555562d45 in mmctx_timer_cb (_mm=0x555555999c80) at gprs_gmm.c:2156
#11 0x00007ffff7308526 in osmo_timers_update () at timer.c:257
#12 0x00007ffff7308d9a in osmo_select_main (polling=0) at select.c:260
#13 0x0000555555572c9f in main (argc=1, argv=0x7fffffffe618) at sgsn_main.c:524
```

#6 - 04/27/2019 10:53 AM - keith

```
(gdb) print *comp_entity
$1 = {list = {next = 0x415454415f4d4d47, prev = 0x465f5145525f4843}, entity = 1730694483, nsapi_len = 98 'b',
nsapi = "_gmm_req)[0", comp_len = 120 'x',
  comp = "555555e02750]\000\000\240", algo = {pcomp = RFC_1144, dcomp = V42BIS}, compclass = 128, state = 0x55
5555bbabb0}
```

#7 - 04/27/2019 10:59 AM - keith

- File core_bin.tgz added

#8 - 04/27/2019 12:40 PM - laforge

On Sat, Apr 27, 2019 at 09:21:21AM +0000, pespin [REDMINE] wrote:

> Following patch is proposed which seems to fix the invalid read/crash for now, but probably bigger refactoring of the code is needed to avoid other kind of issues or incorrect logic:

as you seem to udnerstand the issue in detail, I'm still wondering about what exactly needs
to be done to reproduce the isuse. I've tried for quite some time now various combinations
of mising an IMSI attach on one PCU/RA-ID with a RA Update on another PCU/RA-ID, and couldn't
reproduce any issue that valgrind would show.

Before merging any patches we should at least have a test to reproduce the issue.

#9 - 04/29/2019 04:00 PM - keith

With the binary mentioned in https://osmocom.org/issues/3964#note-2

the latest is SIGSEGV at gprs_sndcp_comp_free.c:161

```
(gdb) print *comp_entities
$2 = {next = 0xdfa46, prev = 0x1}
```

backtrace:

```
#0  0x0000555555556b918 in gprs_sndcp_comp_free (comp_entities=0x5555559476f0) at gprs_sndcp_comp.c:161
#1  0x0000555555557ac04 in llme_free (llme=0x555555924d30) at gprs_llc.c:583
#2  0x0000555555557be24 in gprs_llgmm_assign (llme=0x555555924d30, old_tlli=2378990690, new_tlli=4294967295) at
```

```
 gprs_llc.c:1090
#3  0x0000555555566c82 in sgsn_mm_ctx_cleanup_free (mm=0x0) at gprs_sgsn.c:365
#4  0x000055555555d658 in mm_ctx_cleanup_free (ctx=0x5555558fc950, log_text=0x555555589416 "T3350") at gprs_gm
m.c:326
#5  0x0000555555562d45 in mmctx_timer_cb (_mm=0x5555558fc950) at gprs_gmm.c:2156
#6  0x00007ffff7308526 in osmo_timers_update () at timer.c:257
#7  0x00007ffff7308d9a in osmo_select_main (polling=0) at select.c:260
#8  0x0000555555572d21 in main (argc=1, argv=0x7fffffffe618) at sgsn_main.c:524
```

#10 - 04/29/2019 04:09 PM - keith

- Related to Bug #3964: SIGSEGV in sndcp_sm_deactivate_ind() added

#11 - 05/01/2019 01:33 PM - laforge

- Status changed from New to Feedback

- Assignee set to pespin

Assigning to pespin for feedback on how this can be reproduced. I'm happy to write the test case if somebody can explain to me how to actually reproduce the issue. I tried various different things at OsmoDevCon2019 without success :/

#12 - 06/25/2019 10:25 AM - keith

laforge Just a note.. that this one (I think) was provoked by a "typo" in the osmo-nitb config

With a sysmobts 2050,

BTS 0 has gprs routing area 0
BTS 1 has gprs routing area 1

This causes much RA update of course.. Does that help to reproduce, or indeed write a test?

that said, I filed a number of bug reports and I now am not even sure which config or even in some cases the exact binary that was used.

We might just close all these from osmodevcon time and I will start again with a fresh view on it?

#13 - 06/25/2019 10:28 AM - keith

Ah sorry.. reading again above comments about routing area ID, I think what I just wrote was already quite clear.

#14 - 06/25/2019 10:39 AM - keith

There are in fact 4 BTS in this config

BTS 0-3

for each BTS, the relevant config was:

gprs routing area 0
gprs cell bvci [BTS_NUMBER + 2]
gprs nsei [BTS_NUMBER + 2]
gprs nsvc 0 nsvci [BTS_NUMBER + 2]

except bts 3 that had routing area 1

#15 - 08/12/2019 05:16 PM - pespin

I submitted a pair of commits which may help find or exclude some causes of the crash:
remote: https://gerrit.osmocom.org/c/osmo-sgsn/+/15166 gprs_sgsn.c: Warn upon llme free unexpected scenarios
remote: https://gerrit.osmocom.org/c/osmo-sgsn/+/15167 gprs_gmm: Introduce assert to guard against unexpected condition

#16 - 11/08/2019 05:00 PM - pespin

- Related to Bug #4245: osmo-sgsn hitting assert during osmo-gsm-tester ping.py test added

#17 - 11/08/2019 05:08 PM - pespin

It seems we have catched this one (or related one) in osmo-gsm-tester, see ticket #4245 were the assert I added here is triggered:
https://gerrit.osmocom.org/c/osmo-sgsn/+/15167

#18 - 11/08/2019 06:31 PM - pespin

- % Done changed from 0 to 90

Should be fixed by:
https://gerrit.osmocom.org/c/osmo-sgsn/+/16015 gmm: Fix assertion hit during RA UPD REQ before completting gmm attach

And TTCN3 test triggering the issue:
https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/16016 sgsn: Introduce test TC_attach_req_id_req_ra_update

#19 - 11/21/2019 04:53 PM - pespin

- Assignee changed from pespin to keith

Patch was merged, assigning to keith for him to give it a try with the faulty setup.

Files

core_bin.tgz	970 KB	04/27/2019	keith