OsmoMSC - Bug #3742

libmsc/gsm_04_08.c: OSMO_ASSERT(!conn->vsub) failed in msc_vlr_subscr_assoc()

12/28/2018 05:23 PM - fixeria

Status:	In Progress	**Start date:**	12/28/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	90%
Category:			
Target version:			
Resolution:			

Description

Please see the core dump and logs attached.

```
Core was generated by `/usr/bin/osmo-msc -c /etc/osmocom/osmo-msc.cfg'.
Program terminated with signal SIGABRT, Aborted.
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
51    ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) bt
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
#1  0x00007fd4ca52c51a in __GI_abort () at abort.c:118
#2  0x00007fd4cb8d70d0 in osmo_panic (fmt=0x2 <error: Cannot access memory at address 0x2>,
    fmt@entry=0x55dbe8e70f43 "Assert failed %s %s:%d\n") at ../../../src/libosmocore/src/panic.c:8
2
#3  0x000055dbe8e4ce75 in msc_vlr_subscr_assoc (msc_conn_ref=0x55dbed3087e0, vsub=<optimized out>)
    at ../../../../src/osmo-msc/src/libmsc/gsm_04_08.c:1812
#4  0x000055dbe8e6bef1 in assoc_par_with_subscr (fi=0x55dbeca601c0, vsub=0x55dbec7dc9e0)
    at ../../../../src/osmo-msc/src/libvlr/vlr_access_req_fsm.c:84
#5  proc_arq_vlr_fn_init (fi=0x55dbeca601c0, event=<optimized out>, data=<optimized out>)
    at ../../../../src/osmo-msc/src/libvlr/vlr_access_req_fsm.c:374
#6  0x00007fd4cb8d1553 in _osmo_fsm_inst_dispatch (fi=fi@entry=0x55dbeca601c0, event=event@entry=0
, data=data@entry=0x0,
    file=file@entry=0x55dbe8e80508 "../../../../src/osmo-msc/src/libvlr/vlr_access_req_fsm.c", lin
e=line@entry=693)
    at ../../../src/libosmocore/src/fsm.c:580
#7  0x000055dbe8e6c2df in vlr_proc_acc_req (parent=<optimized out>, parent_event_success=parent_ev
ent_success@entry=2,
    parent_event_failure=parent_event_failure@entry=6, parent_event_data=parent_event_data@entry=0
x0, vlr=0x55dbeaeea2b0,
    msc_conn_ref=msc_conn_ref@entry=0x55dbed3087e0, type=VLR_PR_ARQ_T_CM_SERV_REQ, mi_lv=0x55dbeee
1252a "\005\364KHTc", lai=0x7ffcaaa54358,
    authentication_required=true, ciphering_required=true, is_r99=true, is_utran=false)
    at ../../../../src/osmo-msc/src/libvlr/vlr_access_req_fsm.c:693
#8  0x000055dbe8e4e517 in gsm48_rx_mm_serv_req (conn=conn@entry=0x55dbed3087e0, msg=msg@entry=0x55
dbeee12390)
    at ../../../../src/osmo-msc/src/libmsc/gsm_04_08.c:826
#9  0x000055dbe8e4fd58 in gsm0408_rcv_mm (msg=0x55dbeee12390, conn=0x55dbed3087e0) at ../../../../
src/osmo-msc/src/libmsc/gsm_04_08.c:1157
#10 gsm0408_dispatch (conn=conn@entry=0x55dbed3087e0, msg=msg@entry=0x55dbeee12390) at ../../../..
/src/osmo-msc/src/libmsc/gsm_04_08.c:1521
#11 0x000055dbe8e62afd in ran_conn_dtap (conn=conn@entry=0x55dbed3087e0, msg=msg@entry=0x55dbeee12
390)
    at ../../../../src/osmo-msc/src/libmsc/osmo_msc.c:111
#12 0x000055dbe8e4795d in rx_dtap (scu=0x55dbeee12390, a_conn_info=0x7ffcaaa54480, a_conn_info=0x7
ffcaaa54480, msg=0x55dbeee12390)
    at ../../../../src/osmo-msc/src/libmsc/a_iface_bssap.c:673
#13 a_sccp_rx_dt (scu=scu@entry=0x55dbeafd2060, a_conn_info=a_conn_info@entry=0x7ffcaaa544b0, msg=
0x55dbeee12390)
    at ../../../../src/osmo-msc/src/libmsc/a_iface_bssap.c:695
#14 0x000055dbe8e45b24 in sccp_sap_up (oph=0x55dbeee12418, _scu=0x55dbeafd2060) at ../../../../src
/osmo-msc/src/libmsc/a_iface.c:573
#15 0x00007fd4cb8d1553 in _osmo_fsm_inst_dispatch (fi=0x55dbee5a6f00, event=11, data=data@entry=0x
```

```
55dbebf1cb60,
    file=file@entry=0x7fd4cb250668 "../../../src/libosmo-sccp/src/sccp_scoc.c", line=line@entry=16
70) at ../../../src/libosmocore/src/fsm.c:580
#16 0x00007fd4cb2408fc in sccp_scoc_rx_from_scrc (inst=inst@entry=0x55dbeafd1e00, xua=xua@entry=0x
55dbebf1cb60)
    at ../../../src/libosmo-sccp/src/sccp_scoc.c:1670
#17 0x00007fd4cb23e452 in scrc_rx_mtp_xfer_ind_xua (inst=inst@entry=0x55dbeafd1e00, xua=0x55dbebf1
cb60)
    at ../../../src/libosmo-sccp/src/sccp_scrc.c:457
#18 0x00007fd4cb2414c5 in mtp_user_prim_cb (oph=0x55dbeeeddaf8, ctx=0x55dbeafd1e00) at ../../../sr
c/libosmo-sccp/src/sccp_user.c:176
#19 0x00007fd4cb239802 in m3ua_rx_xfer (xua=0x55dbeca8c970, asp=0x55dbeafbaa60) at ../../../src/li
bosmo-sccp/src/m3ua.c:586
#20 m3ua_rx_msg (asp=asp@entry=0x55dbeafbaa60, msg=msg@entry=0x55dbeeedcd80) at ../../../src/libos
mo-sccp/src/m3ua.c:739
#21 0x00007fd4cb24773b in xua_cli_read_cb (conn=0x55dbeafba4c0) at ../../../src/libosmo-sccp/src/o
smo_ss7.c:1607
#22 0x00007fd4c992f3db in osmo_stream_cli_read (cli=0x55dbeafba4c0) at ../../../src/libosmo-netif/
src/stream.c:192
---Type <return> to continue, or q <return> to quit---
#23 osmo_stream_cli_fd_cb (ofd=<optimized out>, what=3) at ../../../src/libosmo-netif/src/stream.c
:276
#24 0x00007fd4cb8cd8ae in osmo_fd_disp_fds (_eset=0x7ffcaaa548c0, _wset=0x7ffcaaa54840, _rset=0x7f
fcaaa547c0)
    at ../../../src/libosmocore/src/select.c:217
#25 osmo_select_main (polling=<optimized out>) at ../../../src/libosmocore/src/select.c:257
#26 0x000055dbe8e43f75 in main (argc=<optimized out>, argv=<optimized out>) at ../../../../src/osm
o-msc/src/osmo-msc/msc_main.c:708
```

Related issues:

Has duplicate OsmoMSC - Bug #3743: subscriber re-assoc crashes osmo-msc	**In Progress**	**12/29/2018**

History

#1 - 12/28/2018 05:26 PM - fixeria

- Tags set to 35c3

#2 - 01/02/2019 04:08 PM - neels

- Has duplicate Bug #3743: subscriber re-assoc crashes osmo-msc added

#3 - 01/02/2019 04:25 PM - neels

- Status changed from New to In Progress

- % Done changed from 0 to 90

Fixed by Ic0d54644bc735700220b1ef3a4384c217d57d20f (tested on 35c3)
https://gerrit.osmocom.org/#/c/osmo-msc/+/12449

#4 - 03/30/2019 05:50 PM - fixeria

Ping? I think we can close this one now.

Files

osmo_msc_20684.dump.gz	7.19 MB	12/28/2018	fixeria
osmo-msc.18-12-28--17-19-34.log	739 KB	12/28/2018	fixeria