OsmoMSC - Bug #3743

subscriber re-assoc crashes osmo-msc

12/29/2018 01:13 AM - neels

Status:	In Progress	**Start date:**	12/29/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:			
Target version:			
Resolution:			

Description

details follow

Related issues:

Is duplicate of OsmoMSC - Bug #3742: libmsc/gsm_04_08.c: OSMO_ASSERT(!conn->v...	**In Progress**	**12/28/2018**

History

#1 - 12/29/2018 01:14 AM - neels

- File osmo-msc.18-12-28--20-48-59.log added

- Status changed from New to In Progress

```
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from /usr/bin/osmo-msc...done.
[New LWP 4114]
b[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
tCore 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  0x00007fa8541ee51a in __GI_abort () at abort.c:118
#2  0x00007fa855599100 in osmo_panic_default (args=0x7ffe8167ee38, fmt=0x5631fcfacf43 "Assert failed %s %s:%d\
n")
    at ../../../src/libosmocore/src/panic.c:49
#3  osmo_panic (fmt=fmt@entry=0x5631fcfacf43 "Assert failed %s %s:%d\n") at ../../../src/libosmocore/src/panic
.c:84
#4  0x00005631fcf88e75 in msc_vlr_subscr_assoc (msc_conn_ref=0x5631fe8fe240, vsub=<optimized out>)
    at ../../../../src/osmo-msc/src/libmsc/gsm_04_08.c:1812
#5  0x00005631fcfa7ef1 in assoc_par_with_subscr (fi=0x5631fe8b1ea0, vsub=0x5631fea05cd0)
    at ../../../../src/osmo-msc/src/libvlr/vlr_access_req_fsm.c:84
#6  proc_arq_vlr_fn_init (fi=0x5631fe8b1ea0, event=<optimized out>, data=<optimized out>)
    at ../../../../src/osmo-msc/src/libvlr/vlr_access_req_fsm.c:374
#7  0x00007fa855593553 in _osmo_fsm_inst_dispatch (fi=fi@entry=0x5631fe8b1ea0, event=event@entry=0, data=data@
entry=0x0,
    file=file@entry=0x5631fcfbc508 "../../../../src/osmo-msc/src/libvlr/vlr_access_req_fsm.c", line=line@entry
=693)
    at ../../../src/libosmocore/src/fsm.c:580
#8  0x00005631fcfa82df in vlr_proc_acc_req (parent=<optimized out>, parent_event_success=parent_event_success@
entry=2,
    parent_event_failure=parent_event_failure@entry=6, parent_event_data=parent_event_data@entry=0x0, vlr=0x56
31fe7682b0,
```

```
    msc_conn_ref=msc_conn_ref@entry=0x5631fe8fe240, type=VLR_PR_ARQ_T_CM_SERV_REQ,
    mi_lv=0x5631fec45a8a "\005\364\255\217", <incomplete sequence \374\234>, lai=0x7ffe8167f0b8, authentication_required=true,
    ciphering_required=true, is_r99=true, is_utran=false) at ../../../../src/osmo-msc/src/libvlr/vlr_access_req_fsm.c:693
#9  0x00005631fcf8a517 in gsm48_rx_mm_serv_req (conn=conn@entry=0x5631fe8fe240, msg=msg@entry=0x5631fec458f0)
    at ../../../../src/osmo-msc/src/libmsc/gsm_04_08.c:826
#10 0x00005631fcf8bd58 in gsm0408_rcv_mm (msg=0x5631fec458f0, conn=0x5631fe8fe240) at ../../../../src/osmo-msc/src/libmsc/gsm_04_08.c:1157
#11 gsm0408_dispatch (conn=conn@entry=0x5631fe8fe240, msg=msg@entry=0x5631fec458f0) at ../../../../src/osmo-msc/src/libmsc/gsm_04_08.c:1521
#12 0x00005631fcf9eafd in ran_conn_dtap (conn=conn@entry=0x5631fe8fe240, msg=msg@entry=0x5631fec458f0)
    at ../../../../src/osmo-msc/src/libmsc/osmo_msc.c:111
#13 0x00005631fcf8395d in rx_dtap (scu=0x5631fec458f0, a_conn_info=0x7ffe8167f1e0, a_conn_info=0x7ffe8167f1e0, msg=0x5631fec458f0)
    at ../../../../src/osmo-msc/src/libmsc/a_iface_bssap.c:673
#14 a_sccp_rx_dt (scu=scu@entry=0x5631fe850400, a_conn_info=a_conn_info@entry=0x7ffe8167f210, msg=0x5631fec458f0)
    at ../../../../src/osmo-msc/src/libmsc/a_iface_bssap.c:695
#15 0x00005631fcf81b24 in sccp_sap_up (oph=0x5631fec45978, _scu=0x5631fe850400) at ../../../../src/osmo-msc/src/libmsc/a_iface.c:573
#16 0x00007fa855593553 in _osmo_fsm_inst_dispatch (fi=0x5631feb5f940, event=11, data=data@entry=0x5631fe877720,
    file=file@entry=0x7fa854f12668 "../../../src/libosmo-sccp/src/sccp_scoc.c", line=line@entry=1670) at ../../../src/libosmocore/src/fsm.c:580
#17 0x00007fa854f028fc in sccp_scoc_rx_from_scrc (inst=inst@entry=0x5631fe8500c0, xua=xua@entry=0x5631fe877720)
    at ../../../src/libosmo-sccp/src/sccp_scoc.c:1670
#18 0x00007fa854f00452 in scrc_rx_mtp_xfer_ind_xua (inst=inst@entry=0x5631fe8500c0, xua=0x5631fe877720)
    at ../../../src/libosmo-sccp/src/sccp_scrc.c:457
#19 0x00007fa854f034c5 in mtp_user_prim_cb (oph=0x5631fec591f8, ctx=0x5631fe8500c0) at ../../../src/libosmo-sccp/src/sccp_user.c:176
#20 0x00007fa854efb802 in m3ua_rx_xfer (xua=0x5631fe88e2f0, asp=0x5631fe84f1b0) at ../../../src/libosmo-sccp/src/m3ua.c:586
#21 m3ua_rx_msg (asp=asp@entry=0x5631fe84f1b0, msg=msg@entry=0x5631fec35c50) at ../../../src/libosmo-sccp/src/m3ua.c:739
#22 0x00007fa854f0973b in xua_cli_read_cb (conn=0x5631fe84fc50) at ../../../src/libosmo-sccp/src/osmo_ss7.c:1607
#23 0x00007fa8535f13db in osmo_stream_cli_read (cli=0x5631fe84fc50) at ../../../src/libosmo-netif/src/stream.c:192
---Type <return> to continue, or q <r
```

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

- Is duplicate of Bug #3742: libmsc/gsm_04_08.c: OSMO_ASSERT(!conn->vsub) failed in msc_vlr_subscr_assoc() added

Files

osmo-msc.18-12-28--20-48-59.log	760 KB	12/29/2018	neels