OsmoMSC - Bug #2573

segfault in osmo-msc when subscriber silently vanishes

10/12/2017 04:56 PM - dexter

Status:	Closed	**Start date:**	10/12/2017
Priority:	Normal	**Due date:**	
Assignee:	neels	**% Done:**	0%
Category:			
Target version:			
Resolution:		**Spec Reference:**	

Description

Experiment: Use two mobiles, make a call from one to the other. While the call is running, remove the battery of the called mobile. After some time a segfault should occur on the MSC.

```
Thu Oct 12 18:50:29 2017 <000a> a_iface.c:527 N-DATA.ind(9, 00 04 22 04 01 01 )
Thu Oct 12 18:50:29 2017 <000a> a_iface_bssap.c:695 Rx BSC DT: 00 04 22 04 01 01
Thu Oct 12 18:50:29 2017 <000a> a_iface_bssap.c:625 Rx MSC DT1 BSSMAP CLEAR REQUEST
Thu Oct 12 18:50:29 2017 <000a> a_iface_bssap.c:225 BSC requested to clear connection (conn_id=9)
Thu Oct 12 18:50:29 2017 <000a> a_iface_bssap.c:79 Looking for A subscriber: conn_id 9
Thu Oct 12 18:50:29 2017 <001f> a_iface_bssap.c:87 Found A subscriber for conn_id 9
Thu Oct 12 18:50:29 2017 <0002> osmo_msc.c:340 Subscr_Conn(27736205)[0x5555558b39c0]{SUBSCR_CONN_S
_COMMUNICATING}: Received Event SUBSCR_CONN_E_CN_CLOSE
Thu Oct 12 18:50:29 2017 <0002> subscr_conn.c:215 Subscr_Conn(27736205)[0x5555558b39c0]{SUBSCR_CON
N_S_COMMUNICATING}: state_chg to SUBSCR_CONN_S_RELEASED
Thu Oct 12 18:50:29 2017 <0002> subscr_conn.c:242 Subscr_Conn(27736205)[0x5555558b39c0]{SUBSCR_CON
N_S_RELEASED}: Terminating (cause = OSMO_FSM_TERM_REGULAR)
Thu Oct 12 18:50:29 2017 <001e> subscr_conn.c:242 Process_Access_Request_VLR(27736205)[0x5555558b2
3e0]{PR_ARQ_S_DONE}: Terminating (cause = OSMO_FSM_TERM_PARENT)
Thu Oct 12 18:50:29 2017 <001e> subscr_conn.c:242 Process_Access_Request_VLR(27736205)[0x5555558b2
3e0]{PR_ARQ_S_DONE}: Removing from parent Subscr_Conn(27736205)[0x5555558b39c0]
Thu Oct 12 18:50:29 2017 <001e> subscr_conn.c:242 Process_Access_Request_VLR(27736205)[0x5555558b2
3e0]{PR_ARQ_S_DONE}: Freeing instance
Thu Oct 12 18:50:29 2017 <001e> fsm.c:273 Process_Access_Request_VLR(27736205)[0x5555558b23e0]{PR_
ARQ_S_DONE}: Deallocated
Thu Oct 12 18:50:29 2017 <0002> osmo_msc.c:328 msc_subscr_conn_close(vsub=MSISDN:23006, cause=2):
no conn fsm, releasing directly without release event.
Thu Oct 12 18:50:29 2017 <0006> gsm_04_08.c:1270 transmit message MNCC_REL_IND
Thu Oct 12 18:50:29 2017 <0001> gsm_04_08.c:1293 Sending 'MNCC_REL_IND' to MNCC.
Thu Oct 12 18:50:29 2017 <0006> mncc_builtin.c:312 (call 5) Received message MNCC_REL_IND
Thu Oct 12 18:50:29 2017 <0006> mncc_builtin.c:242 (call 5) Releasing remote with cause 47
Thu Oct 12 18:50:29 2017 <0006> mncc_builtin.c:52 (call 5) Call removed.
Thu Oct 12 18:50:29 2017 <0006> gsm_04_08.c:2839 receive message MNCC_REL_REQ
Thu Oct 12 18:50:29 2017 <0001> gsm_04_08.c:3014 (ti 08 sub 23001) Received 'MNCC_REL_REQ' from MN
CC in state 10 (ACTIVE)
Thu Oct 12 18:50:29 2017 <0001> gsm_04_08.c:1525 starting timer T308 with 10 seconds
Thu Oct 12 18:50:29 2017 <0001> gsm_04_08.c:1218 new state ACTIVE -> RELEASE_REQ
Thu Oct 12 18:50:29 2017 <000a> msc_ifaces.c:55 msc_tx 6 bytes to MSISDN:23001 via RAN_GERAN_A
Thu Oct 12 18:50:29 2017 <000a> a_iface.c:143 Passing DTAP message from MSC to BSC (conn_id=8)
Thu Oct 12 18:50:29 2017 <000a> a_iface.c:156 Message will be sent as BSSMAP DTAP message!
Thu Oct 12 18:50:29 2017 <000a> a_iface.c:158 N-DATA.req(8, 01 00 06 83 2d 08 02 81 af )
Thu Oct 12 18:50:29 2017 <0001> gsm_04_08.c:1218 new state ACTIVE -> NULL
Thu Oct 12 18:50:29 2017 <000e> transaction.c:134 VLR subscr MSISDN:23006 usage decreases to: 2
Thu Oct 12 18:50:29 2017 <000e> transaction.c:141 MSISDN:23006: MSC conn use - 1 == 0
Thu Oct 12 18:50:29 2017 <0000> osmo_msc.c:230 subscr MSISDN:23006: Freeing subscriber connection
Thu Oct 12 18:50:29 2017 <000e> osmo_msc.c:232 VLR subscr MSISDN:23006 usage decreases to: 1
Thu Oct 12 18:50:29 2017 <000a> a_iface.c:426 Sending clear command to BSC (conn_id=9)

Program received signal SIGSEGV, Segmentation fault.
vlr_subscr_name (vsub=0x90) at gsm_subscriber_base.c:45
45        if (vsub->msisdn[0])
(gdb) bt
#0  vlr_subscr_name (vsub=0x90) at gsm_subscriber_base.c:45
```

```
#1  0x0000555555574c72 in _msc_subscr_conn_put (conn=0x5555558b3ee0, file=0x55555558a6a9 "subscr_conn.c", line=228) at osmo_msc.c:375
#2  0x00007ffff733aef5 in _osmo_fsm_inst_term (fi=0x5555558b39c0, cause=OSMO_FSM_TERM_REGULAR, data=0x0, file=0x55555558a6a9 "subscr_conn.c", line=242) at fsm.c:479
#3  0x00007ffff733a77c in _osmo_fsm_inst_state_chg (fi=0x5555558b39c0, new_state=<optimized out>, timeout_secs=0, T=0, file=<optimized out>, line=<optimized out>) at fsm.c:382
#4  0x00007ffff733aa0d in _osmo_fsm_inst_dispatch (fi=0x5555558b39c0, event=event@entry=6, data=data@entry=0x7fffffffcb5c, file=file@entry=0x55555558a513 "osmo_msc.c", line=line@entry=340) at fsm.c:436
#5  0x0000555555574987 in msc_subscr_conn_close (conn=0x5555558b3ee0, cause=<optimized out>, cause@entry=1) at osmo_msc.c:340
#6  0x0000555555574b19 in msc_clear_request (conn=<optimized out>, cause=cause@entry=1) at osmo_msc.c:262
#7  0x000055555556115c in bssmap_rx_clear_rqst (scu=scu@entry=0x5555558974c0, msg=0x5555558b52b0, a_conn_info=<optimized out>, a_conn_info=<optimized out>) at a_iface_bssap.c:242
#8  0x0000555555556213 in rx_bssmap (msg=<optimized out>, a_conn_info=0x7fffffffdbc8, scu=0x5555558974c0) at a_iface_bssap.c:629
#9  sccp_rx_dt (scu=scu@entry=0x7ffff6c7b880 <sccp_scoc_states>, a_conn_info=a_conn_info@entry=0x7fffffffdbd0, msg=<optimized out>) at a_iface_bssap.c:706
#10 0x000055555555f6b4 in sccp_sap_up (oph=0x7ffff6c7e5a0 <sccp_scoc_fsm>, _scu=0x7ffff6c7b880 <sccp_scoc_states>) at a_iface.c:528
#11 0x00007ffff733aa0d in _osmo_fsm_inst_dispatch (fi=0x5555558b1be0, event=11, data=data@entry=0x5555558b4f20, file=file@entry=0x7ffff6a6c4bd "sccp_scoc.c", line=line@entry=1579) at fsm.c:436
#12 0x00007ffff6a5d5cc in sccp_scoc_rx_from_scrc (inst=inst@entry=0x5555558973f0, xua=xua@entry=0x5555558b4f20) at sccp_scoc.c:1579
#13 0x00007ffff6a5b220 in scrc_rx_mtp_xfer_ind_xua (inst=inst@entry=0x5555558973f0, xua=0x5555558b4f20) at sccp_scrc.c:447
#14 0x00007ffff6a5e0f5 in mtp_user_prim_cb (oph=0x5555558a1c68, ctx=0x5555558973f0) at sccp_user.c:174
#15 0x00007ffff6a561c2 in m3ua_rx_xfer (xua=0x5555558a9580, asp=0x555555873230) at m3ua.c:584
#16 m3ua_rx_msg (asp=asp@entry=0x555555873230, msg=msg@entry=0x5555558a2ec0) at m3ua.c:736
#17 0x00007ffff6a6103b in xua_cli_read_cb (conn=<optimized out>) at osmo_ss7.c:1552
#18 0x00007ffff5c6c39b in osmo_stream_cli_read (cli=0x555555896e30) at stream.c:166
#19 osmo_stream_cli_fd_cb (ofd=<optimized out>, what=1) at stream.c:250
#20 0x00007ffff73376ee in osmo_fd_disp_fds (_eset=0x7fffffffdff0, _wset=0x7fffffffdf70, _rset=0x7fffffffdef0) at select.c:213
#21 osmo_select_main (polling=<optimized out>) at select.c:253
#22 0x000055555555ed6c in main (argc=3, argv=0x7fffffffe1d8) at msc_main.c:587
(gdb)
```

Related issues:

Blocked by OsmoMSC - Bug #2672: use-after-free on ending a call	**Closed**	**11/21/2017**

History

#1 - 11/07/2017 03:57 PM - neels

- Assignee changed from dexter to neels

#2 - 11/23/2017 01:01 AM - neels

possibly, this is fixed by https://gerrit.osmocom.org/4974 ... let's wait for this to be merged and try again

#3 - 11/27/2017 02:56 PM - neels

- Blocked by Bug #2672: use-after-free on ending a call added

#4 - 11/28/2017 01:34 AM - neels

- Assignee changed from neels to dexter

dexter, we've just merged a ref count fix for MT calls which is likely the cause for this fault. Could you please run the exact same test again and see whether teardown is graceful now? Thanks!

#5 - 11/28/2017 05:05 PM - dexter

- Assignee changed from dexter to neels

neels: I re-tested, to me it looks good to me now.

#6 - 11/29/2017 12:56 PM - neels

- Status changed from New to Resolved

fixed by #2672

#7 - 02/06/2018 08:26 AM - laforge

- Status changed from Resolved to Closed