OsmoMSC - Bug #3930

TC_smpp_mt_sms crashes osmo-msc

04/15/2019 09:37 AM - dexter

Status:	Resolved	**Start date:**	04/15/2019
Priority:	Normal	**Due date:**	
Assignee:	neels	**% Done:**	100%
Category:			
Target version:			
Resolution:		**Spec Reference:**	

Description

It seems that there were problems introduced with https://gerrit.osmocom.org/#/c/osmo-msc/+/13136/, which now cause osmo-msc to crash.

```
Mon Apr 15 11:32:52 2019 DVLR <000e> fsm.c:535 lu_compl_vlr_fsm(IMSI-262420000000045:MSISDN-491230
000045:GERAN-A-0:LU)[0x561d3f9224f0]{LU_COMPL_VLR_S_DONE}: Deallocated
Mon Apr 15 11:32:52 2019 DVLR <000e> vlr_lu_fsm.c:749 vlr_lu_fsm(IMSI-262420000000045:MSISDN-49123
0000045:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f9255d0]{VLR_ULA_S_WAIT_LU_COMPL}: state_chg to VLR_U
LA_S_DONE
Mon Apr 15 11:32:52 2019 DMM <0002> vlr_lu_fsm.c:741 RAN_conn(IMSI-262420000000045:MSISDN-49123000
0045:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f926090]{RAN_CONN_S_AUTH_CIPH}: Received Event RAN_CONN_
E_ACCEPTED
Mon Apr 15 11:32:52 2019 DSMPP <000c> smpp_smsc.c:656 [msc_tester] Tx ALERT_NOTIFICATION (49123000
0045/3/1): Available
Mon Apr 15 11:32:52 2019 DMM <0002> ran_conn.c:146 RAN_conn(IMSI-262420000000045:MSISDN-4912300000
45:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f926090]{RAN_CONN_S_AUTH_CIPH}: state_chg to RAN_CONN_S_AC
CEPTED
Mon Apr 15 11:32:52 2019 DMM <0002> ran_conn.c:276 RAN_conn(IMSI-262420000000045:MSISDN-4912300000
45:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f926090]{RAN_CONN_S_ACCEPTED}: Received Event RAN_CONN_E_U
NUSED
Mon Apr 15 11:32:52 2019 DMM <0002> ran_conn.c:297 RAN_conn(IMSI-262420000000045:MSISDN-4912300000
45:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f926090]{RAN_CONN_S_ACCEPTED}: state_chg to RAN_CONN_S_REL
EASING
Mon Apr 15 11:32:52 2019 DMM <0002> ran_conn.c:906 RAN_conn(IMSI-262420000000045:MSISDN-4912300000
45:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f926090]{RAN_CONN_S_RELEASING}: Received Event RAN_CONN_E_
UNUSED
Mon Apr 15 11:32:52 2019 DMM <0002> ran_conn.c:408 RAN_conn(IMSI-262420000000045:MSISDN-4912300000
45:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f926090]{RAN_CONN_S_RELEASING}: state_chg to RAN_CONN_S_RE
LEASED
Mon Apr 15 11:32:52 2019 DMM <0002> ran_conn.c:415 RAN_conn(IMSI-262420000000045:MSISDN-4912300000
45:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f926090]{RAN_CONN_S_RELEASED}: Terminating (cause = OSMO_F
SM_TERM_REGULAR)
Mon Apr 15 11:32:52 2019 DVLR <000e> ran_conn.c:415 vlr_lu_fsm(IMSI-262420000000045:MSISDN-4912300
00045:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f9255d0]{VLR_ULA_S_DONE}: Terminating in cascade, depth
 2 (cause = OSMO_FSM_TERM_PARENT, caused by: RAN_conn(IMSI-262420000000045:MSISDN-491230000045:TMS
I-0x14A42776:GERAN-A-0:LU)[0x561d3f926090])
Mon Apr 15 11:32:52 2019 DVLR <000e> ran_conn.c:415 vlr_lu_fsm(IMSI-262420000000045:MSISDN-4912300
00045:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f9255d0]{VLR_ULA_S_DONE}: Removing from parent RAN_conn
(IMSI-262420000000045:MSISDN-491230000045:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f926090]
Mon Apr 15 11:32:52 2019 DVLR <000e> vlr_lu_fsm.c:1415 vlr_lu_fsm(IMSI-262420000000045:MSISDN-4912
30000045:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f9255d0]{VLR_ULA_S_DONE}: fsm_lu_cleanup called with
 cause OSMO_FSM_TERM_PARENT
Mon Apr 15 11:32:52 2019 DVLR <000e> fsm.c:514 vlr_lu_fsm(IMSI-262420000000045:MSISDN-491230000045
:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f9255d0]{VLR_ULA_S_DONE}: Deferring: will deallocate with RA
N_conn(IMSI-262420000000045:MSISDN-491230000045:TMSI-0x14A42776:GERAN-A-0:LU)[0x561d3f926090]
Mon Apr 15 11:32:52 2019 DMM <0002> fsm.c:530 RAN_conn(IMSI-262420000000045:MSISDN-491230000045:TM
SI-0x14A42776:GERAN-A-0:LU)[0x561d3f926090]{RAN_CONN_S_RELEASED}: Deallocated, including all defer
red deallocations
Mon Apr 15 11:32:52 2019 DSMPP <000c> smpp_smsc.c:753 [msc_tester] smpp_pdu_rx(00 00 00 36 00 00 0
0 04 00 00 00 00 00 00 00 02 43 4d 54 00 00 00 31 32 33 34 35 00 01 01 34 39 31 32 33 30 30 30 30
30 34 35 00 01 00 00 00 00 00 00 01 00 01 00 )
Mon Apr 15 11:32:52 2019 DSMPP <000c> smpp_smsc.c:735 [msc_tester] Rx SUBMIT-SM (491230000045/1/1)
```

```
Assert failed _osmo_use_count_get_put(&(sms->receiver)->use_count, "SMS-receiver", -1, "gsm_04_11.
c", 74) == 0 gsm_04_11.c:74
backtrace() returned 11 addresses
/usr/local/lib/libosmocore.so.12(osmo_panic+0xbb) [0x7f2a78ab58db]
osmo-msc(+0x231f5) [0x561d3f3391f5]
osmo-msc(+0x3a192) [0x561d3f350192]
osmo-msc(+0x37d52) [0x561d3f34dd52]
osmo-msc(+0x382a4) [0x561d3f34e2a4]
/usr/local/lib/libosmocore.so.12(osmo_wqueue_bfd_cb+0x73) [0x7f2a78aaff53]
/usr/local/lib/libosmocore.so.12(osmo_select_main+0x1f1) [0x7f2a78aaabc1]
osmo-msc(+0xd44f) [0x561d3f32344f]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf1) [0x7f2a776402b1]
osmo-msc(+0xd5ea) [0x561d3f3235ea]
signal 6 received
backtrace() returned 15 addresses
osmo-msc(+0xd81d) [0x561d3f32381d]
/lib/x86_64-linux-gnu/libc.so.6(+0x33030) [0x7f2a77653030]
/lib/x86_64-linux-gnu/libc.so.6(gsignal+0xcf) [0x7f2a77652fcf]
/lib/x86_64-linux-gnu/libc.so.6(abort+0x16a) [0x7f2a776543fa]
/usr/local/lib/libosmocore.so.12(osmo_set_panic_handler+0) [0x7f2a78ab58e0]
osmo-msc(+0x231f5) [0x561d3f3391f5]
osmo-msc(+0x3a192) [0x561d3f350192]
osmo-msc(+0x37d52) [0x561d3f34dd52]
osmo-msc(+0x382a4) [0x561d3f34e2a4]
/usr/local/lib/libosmocore.so.12(osmo_wqueue_bfd_cb+0x73) [0x7f2a78aaff53]
/usr/local/lib/libosmocore.so.12(osmo_select_main+0x1f1) [0x7f2a78aaabc1]
osmo-msc(+0xd44f) [0x561d3f32344f]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf1) [0x7f2a776402b1]
osmo-msc(+0xd5ea) [0x561d3f3235ea]
talloc report on 'vty' (total 174968 bytes in 9344 blocks)
    struct vty                     contains    863 bytes in   4 blocks (ref 0) 0x561d3f921d80
    struct vty                     contains   1004 bytes in  16 blocks (ref 0) 0x561d3f91dad0
    Configure SCCP timer values, see ITU-T Q.714
Waiting for connection confirm message, 1 to 2 minutes (default: 60)
Send keep-alive: on an idle connection, delay before sending an Idle Timer message, 5 to 10 minute
s (default: 420)
Receive keep-alive: on an idle connection, delay until considering a connection as stale, 11 to 21
 minutes (default: 900)
Waiting for release complete message, 10 to 20 seconds (default: 10)
Waiting for release complete message; or to repeat sending released message after the initial expi
ry, 10 to 20 seconds (default: 10)
Waiting for release complete message; or to release connection resources, freeze the LRN and alert
 a maintenance function after the initial expiry, extending to 1 minute (default: 60)
Waiting to resume normal procedure for temporary connection sections during the restart procedure,
 23 to 25 minutes (default: 1380)
Waiting to release temporary connection section or alert maintenance function after reset request
message is sent, 10 to 20 seconds (default: 10)
Waiting to receive all the segments of the remaining segments, single segmented message after rece
iving the first segment, 10 to 20 seconds (default: 10)
Timer value, in seconds
 contains   1194 bytes in   1 blocks (ref 0) 0x561d3f83c830
    sccp-timer (conn_est|ias|iar|rel|repeat_rel|int|guard|reset|reassembly) <1-999999> contains
  83 bytes in   1 blocks (ref 0) 0x561d3f83c6c0
    save_cwd                       contains     37 bytes in   1 blocks (ref 0) 0x561d3f7fe960
    vty_command                    contains 105253 bytes in 5615 blocks (ref 0) 0x561d3f7ebc20
    vty_vector                     contains  66534 bytes in 3705 blocks (ref 0) 0x561d3f7ebbb0
full talloc report on 'osmo_msc' (total  17200 bytes in  93 blocks)
    telnet_connection              contains    177 bytes in   3 blocks (ref 0) 0x561d3f9150f0
        struct telnet_connection       contains     88 bytes in   1 blocks (ref 0) 0x561d3f921cc0
        struct telnet_connection       contains     88 bytes in   1 blocks (ref 0) 0x561d3f920d20
    struct osmo_ss7_instance       contains   2478 bytes in  29 blocks (ref 0) 0x561d3f915650
        struct osmo_sccp_instance      contains    266 bytes in   3 blocks (ref 0) 0x561d3f91d570
            struct osmo_sccp_user          contains     90 bytes in   2 blocks (ref 0) 0x561d3f91e
110
                OsmoMSC-A                      contains     10 bytes in   1 blocks (ref 0) 0x561d3
f915bd0
        struct osmo_ss7_as             contains    624 bytes in   7 blocks (ref 0) 0x561d3f915e70
```

```
            as-clnt-OsmoMSC-A               contains     18 bytes in   1 blocks (ref 0) 0x561d3f916
360
            struct osmo_fsm_inst            contains    364 bytes in   4 blocks (ref 0) 0x561d3f916
040
                struct xua_as_fsm_priv          contains    104 bytes in   1 blocks (ref 0) 0x561d3
f916290
                XUA_AS(as-clnt-OsmoMSC-A)[0x561d3f916040] contains     42 bytes in   1 blocks (ref
 0) 0x561d3f9161f0
                as-clnt-OsmoMSC-A               contains     18 bytes in   1 blocks (ref 0) 0x561d3
f916170
            as-clnt-OsmoMSC-A               contains     18 bytes in   1 blocks (ref 0) 0x561d3f915
fc0
        struct osmo_ss7_asp             contains   1147 bytes in  14 blocks (ref 0) 0x561d3f915aa0
            (r=127.0.0.1:2905<->l=127.0.0.1:52054) contains     39 bytes in   1 blocks (ref 0) 0x5
61d3f915d70
            struct osmo_fsm_inst            contains    367 bytes in   4 blocks (ref 0) 0x561d3f91c
de0
                struct xua_asp_fsm_priv         contains    104 bytes in   1 blocks (ref 0) 0x561d3
f91d4a0
                XUA_ASP(asp-clnt-OsmoMSC-A)[0x561d3f91cde0] contains     44 bytes in   1 blocks (r
ef 0) 0x561d3f91cf10
                asp-clnt-OsmoMSC-A              contains     19 bytes in   1 blocks (ref 0) 0x561d3
f9151d0
            struct osmo_stream_cli          contains    242 bytes in   2 blocks (ref 0) 0x561d3f91b
a00
                127.0.0.1                       contains     10 bytes in   1 blocks (ref 0) 0x561d3
f91bb50
            struct osmo_fsm_inst            contains    278 bytes in   4 blocks (ref 0) 0x561d3f91d
fe0
                struct lm_fsm_priv              contains      8 bytes in   1 blocks (ref 0) 0x561d3
f91eb00
                xua_default_lm(asp-clnt-OsmoMSC-A)[0x561d3f91dfe0] contains     51 bytes in   1 bl
ocks (ref 0) 0x561d3f91c7b0
                asp-clnt-OsmoMSC-A              contains     19 bytes in   1 blocks (ref 0) 0x561d3
f91c860
            127.0.0.1                       contains     10 bytes in   1 blocks (ref 0) 0x561d3f915
2c0
            asp-clnt-OsmoMSC-A              contains     19 bytes in   1 blocks (ref 0) 0x561d3f915
540
        struct osmo_ss7_route_table     contains    145 bytes in   4 blocks (ref 0) 0x561d3f9157e0
            struct osmo_ss7_route           contains     82 bytes in   2 blocks (ref 0) 0x561d3f91c
9f0
                as-clnt-OsmoMSC-A               contains     18 bytes in   1 blocks (ref 0) 0x561d3
f91ea80
            system                          contains      7 bytes in   1 blocks (ref 0) 0x561d3f915
4d0
    struct osmo_stream_srv_link     contains     96 bytes in   2 blocks (ref 0) 0x561d3f913870
        0.0.0.0                         contains      8 bytes in   1 blocks (ref 0) 0x561d3f913930
    struct sgs_state                contains    376 bytes in   1 blocks (ref 0) 0x561d3f913690
    struct smsc                     contains    600 bytes in   3 blocks (ref 0) 0x561d3f900f20
        struct osmo_esme                contains    336 bytes in   1 blocks (ref 0) 0x561d3f91dd00
        struct osmo_smpp_acl            contains    112 bytes in   1 blocks (ref 0) 0x561d3f916460
    struct gsm_network              contains   7961 bytes in  31 blocks (ref 0) 0x561d3f83e580
        struct bsc_context              contains    441 bytes in   5 blocks (ref 0) 0x561d3f924bc0
            struct osmo_fsm_inst            contains    241 bytes in   3 blocks (ref 0) 0x561d3f924
d60
                A-RESET(bsc-193)[0x561d3f924d60] contains     33 bytes in   1 blocks (ref 0) 0x561
d3f924e90
                bsc-193                         contains      8 bytes in   1 blocks (ref 0) 0x561d3
f923fd0
            struct reset_ctx                contains     16 bytes in   1 blocks (ref 0) 0x561d3f924
ce0
        struct mgcp_client              contains    688 bytes in   1 blocks (ref 0) 0x561d3f91bff0
        struct gsm_sms_queue            contains    216 bytes in   1 blocks (ref 0) 0x561d3f91b830
        struct ctrl_handle              contains    478 bytes in   5 blocks (ref 0) 0x561d3f913fa0
            struct ctrl_connection          contains    199 bytes in   2 blocks (ref 0) 0x561d3f921
bb0
```

```
                (r=127.0.0.1:32793<->l=127.0.0.1:4255) contains     39 bytes in   1 blocks (ref 0)
 0x561d3f91e650
            struct ctrl_connection          contains    199 bytes in   2 blocks (ref 0) 0x561d3f920
b80
                (r=127.0.0.1:39451<->l=127.0.0.1:4255) contains     39 bytes in   1 blocks (ref 0)
 0x561d3f920c90
        struct mncc_sock_state          contains    104 bytes in   1 blocks (ref 0) 0x561d3f915880
        127.0.0.1                       contains     10 bytes in   1 blocks (ref 0) 0x561d3f83f440
        /home/owner/mncc_sock           contains     22 bytes in   1 blocks (ref 0) 0x561d3f915450
        112                             contains      4 bytes in   1 blocks (ref 0) 0x561d3f915160
        127.0.0.1                       contains     10 bytes in   1 blocks (ref 0) 0x561d3f9153d0
        OsmoMSC                         contains      8 bytes in   1 blocks (ref 0) 0x561d3f83f360
        OsmoMSC                         contains      8 bytes in   1 blocks (ref 0) 0x561d3f83f3d0
        struct vlr_instance             contains   2804 bytes in  10 blocks (ref 0) 0x561d3f83f4c0
            struct vlr_subscr               contains   1994 bytes in   4 blocks (ref 0) 0x561d3f925
890
                struct osmo_fsm_inst            contains    266 bytes in   3 blocks (ref 0) 0x561d3
f923bd0
                    SGs-UE(imsi:262420000000045)[0x561d3f923bd0] contains     45 bytes in   1 bloc
ks (ref 0) 0x561d3f925700
                    imsi:262420000000045            contains     21 bytes in   1 blocks (ref 0) 0x5
61d3f925230
            struct osmo_gsup_client         contains    490 bytes in   4 blocks (ref 0) 0x561d3f91b
340
                struct osmo_fd                  contains     48 bytes in   1 blocks (ref 0) 0x561d3
f91b5d0
                struct ipa_client_conn          contains    186 bytes in   2 blocks (ref 0) 0x561d3
f91b4b0
                    127.0.0.1                       contains     10 bytes in   1 blocks (ref 0) 0x5
61d3f91b670
            struct ipaccess_unit            contains     64 bytes in   1 blocks (ref 0) 0x561d3f91b
290
        rate_ctr.c:234                  contains   2352 bytes in   1 blocks (ref 0) 0x561d3f83e920
    logging                         contains   4393 bytes in   9 blocks (ref 0) 0x561d3f7eb360
        Configure logging
Set the log level for a specified category
A-bis Radio Link Layer (RLL)
Layer3 Call Control (CC)
Layer3 Mobility Management (MM)
Layer3 Radio Resource (RR)
MNCC API for Call Control application
Paging Subsystem
Mobile Switching Center
Media Gateway Control Protocol
Hand-Over
Database Layer
Reference Counting
Control interface
SMPP interface for external SMS apps
Radio Access Network Application Part Protocol
Visitor Location Register
Iu-CS Protocol
BSSAP Protocol (A Interface)
SGs Interface (SGsAP)
Library-internal global log family
LAPD in libosmogsm
A-bis Intput Subsystem
A-bis B-Subchannel TRAU Frame Multiplex
A-bis Input Driver for Signalling
A-bis Input Driver for B-Channels (voice)
Layer3 Short Message Service (SMS)
Control Interface
GPRS GTP library
Statistics messages and logging
Generic Subscriber Update Protocol
Osmocom Authentication Protocol
libosmo-sigtran Signalling System 7
```

```
libosmo-sigtran SCCP Implementation
libosmo-sigtran SCCP User Adaptation
libosmo-sigtran MTP3 User Adaptation
libosmo-mgcp Media Gateway Control Protocol
libosmo-netif Jitter Buffer
Remote SIM protocol
Deprecated alias for 'no logging level force-all'
 contains   1173 bytes in   1 blocks (ref 0) 0x561d3f853f70
        logging level (rll|cc|mm|rr|mncc|pag|msc|mgcp|ho|db|ref|ctrl|smpp|ranap|vlr|iucs|bssap|sgs
|lglobal|llapd|linp|lmux|lmi|lmib|lsms|lctrl|lgtp|lstats|lgsup|loap|lss7|lsccp|lsua|lm3ua|lmgcp|lj
ibuf|lrspro) everything contains    212 bytes in   1 blocks (ref 0) 0x561d3f853d80
        Configure logging
Set the log level for a specified category
A-bis Radio Link Layer (RLL)
Layer3 Call Control (CC)
Layer3 Mobility Management (MM)
Layer3 Radio Resource (RR)
MNCC API for Call Control application
Paging Subsystem
Mobile Switching Center
Media Gateway Control Protocol
Hand-Over
Database Layer
Reference Counting
Control interface
SMPP interface for external SMS apps
Radio Access Network Application Part Protocol
Visitor Location Register
Iu-CS Protocol
BSSAP Protocol (A Interface)
SGs Interface (SGsAP)
Library-internal global log family
LAPD in libosmogsm
A-bis Intput Subsystem
A-bis B-Subchannel TRAU Frame Multiplex
A-bis Input Driver for Signalling
A-bis Input Driver for B-Channels (voice)
Layer3 Short Message Service (SMS)
Control Interface
GPRS GTP library
Statistics messages and logging
Generic Subscriber Update Protocol
Osmocom Authentication Protocol
libosmo-sigtran Signalling System 7
libosmo-sigtran SCCP Implementation
libosmo-sigtran SCCP User Adaptation
libosmo-sigtran MTP3 User Adaptation
libosmo-mgcp Media Gateway Control Protocol
libosmo-netif Jitter Buffer
Remote SIM protocol
Log debug messages and higher levels
Log informational messages and higher levels
Log noticeable messages and higher levels
Log error messages and higher levels
Log only fatal messages
 contains   1308 bytes in   1 blocks (ref 0) 0x561d3f8537f0
        logging level (rll|cc|mm|rr|mncc|pag|msc|mgcp|ho|db|ref|ctrl|smpp|ranap|vlr|iucs|bssap|sgs
|lglobal|llapd|linp|lmux|lmi|lmib|lsms|lctrl|lgtp|lstats|lgsup|loap|lss7|lsccp|lsua|lm3ua|lmgcp|lj
ibuf|lrspro) (debug|info|notice|error|fatal) contains    233 bytes in   1 blocks (ref 0) 0x561d3f8
53600
        struct log_target              contains    242 bytes in   2 blocks (ref 0) 0x561d3f7eb970
            struct log_category            contains     74 bytes in   1 blocks (ref 0) 0x561d3f7eb
a80
        struct log_info                contains   1224 bytes in   2 blocks (ref 0) 0x561d3f7eb3d0
            struct log_info_cat            contains   1184 bytes in   1 blocks (ref 0) 0x561d3f7eb
460
    transaction                    contains      0 bytes in   1 blocks (ref 0) 0x561d3f7eb2f0
```

```
    gsm_call                        contains      0 bytes in   1 blocks (ref 0) 0x561d3f7eb280
    sms                             contains    648 bytes in   2 blocks (ref 0) 0x561d3f7eb210
        struct gsm_sms                  contains    648 bytes in   1 blocks (ref 0) 0x561d3f924f20
    osmo_signal                     contains    280 bytes in   8 blocks (ref 0) 0x561d3f7eb1a0
        struct signal_handler           contains     40 bytes in   1 blocks (ref 0) 0x561d3f915ce0
        struct signal_handler           contains     40 bytes in   1 blocks (ref 0) 0x561d3f915c50
        struct signal_handler           contains     40 bytes in   1 blocks (ref 0) 0x561d3f921840
        struct signal_handler           contains     40 bytes in   1 blocks (ref 0) 0x561d3f920690
        struct signal_handler           contains     40 bytes in   1 blocks (ref 0) 0x561d3f9155c0
        struct signal_handler           contains     40 bytes in   1 blocks (ref 0) 0x561d3f915340
        struct signal_handler           contains     40 bytes in   1 blocks (ref 0) 0x561d3f8c9e60
    msgb                            contains    190 bytes in   2 blocks (ref 0) 0x561d3f7eb130
        SMPP Rx                         contains    190 bytes in   1 blocks (ref 0) 0x561d3f923d00
./start_msc.sh: line 6: 21718 Aborted                 osmo-msc -c ./osmo-msc.cfg
```

History

#1 - 04/15/2019 09:39 AM - dexter

- Status changed from New to In Progress

I am trying to pinpoint the issue, but it is rather difficult. When I run osmo-msc in gdb the problem does not occur. The only trace I currently have is the following line:

```
Assert failed _osmo_use_count_get_put(&(sms->receiver)->use_count, "SMS-receiver", -1, "gsm_04_11.c", 74) == 0
 gsm_04_11.c:74
```

Unfortunately this does not help much since the location of the assert is not obvious. It seems to come from some callback.

#2 - 04/15/2019 10:46 AM - dexter

It seems to fail because vlr_subscr_use_cb() returns -ERANGE. For some reason e->count drops down to -1, which then triggers the OSMO_ASSERT in vlr.h

#3 - 04/15/2019 10:47 AM - dexter

- Assignee set to neels

#4 - 04/15/2019 11:53 AM - neels

- Status changed from In Progress to Resolved

- % Done changed from 0 to 100

fix: https://gerrit.osmocom.org/#/c/osmo-msc/+/13638