

# OsmoMSC - Bug #3168

## heap-use-after-free in MO SMS / SMPP

04/14/2018 12:49 PM - laforge

|   |          |                        |            |
|---|----------|------------------------|------------|
| <b>Status:</b>  | Resolved | <b>Start date:</b>     | 04/14/2018 |
| <b>Priority:</b>  | High     | <b>Due date:</b>       |            |
| <b>Assignee:</b>  | laforge  | <b>% Done:</b>         | 100%       |
| <b>Category:</b>  | SMS      | <b>Spec Reference:</b> |            |
| <b>Target version:</b>  |          |                        |            |
| <b>Resolution:</b>  |          |                        |            |
| <b>Description</b>  |          |                        |            |
| When trying to send a MO-SMS from a TTCN3 test case to an ESME route I get the following report from asan:  |          |                        |            |
| <pre>Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; gsm0411_smc.c:574 SMC(0) message MMSMS-EST-IND (CP DATA) received in state IDLE Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; gsm0411_smc.c:291 SMC(0) received CP-DATA Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; gsm0411_smc.c:141 SMC(0) new CP state IDLE -&gt; MM_ESTABLISHED Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; gsm_04_11.c:142 sending CP message (trans=8) Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; gsm_04_11.c:125 GSM4.11 TX 89 04 Sat Apr 14 12:01:14 2018 DBSSAP &lt;0010&gt; a_iface.c:154 (subscr MSISDN:491230000042, conn_id 1) Passing DTAP message (DLCI=0x03) from MSC to BSC Sat Apr 14 12:01:14 2018 DBSSAP &lt;0010&gt; a_iface.c:168 (subscr MSISDN:491230000042, conn_id 1) N-DATA.req([]) Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; gsm_04_11.c:883 MNSMS-DATA/EST-IND Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; gsm0411_smr.c:488 SMR(0) message MNSMS-EST-IND received in state IDLE Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; gsm0411_smr.c:263 SMR(0) RX SMS RP-DATA Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; gsm0411_smr.c:145 SMR(0) new RP state IDLE -&gt; WAIT_TO_TX_RP_ACK Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; gsm_04_11.c:800 RX SMS RP-DATA (MO) Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; gsm_04_11.c:641 RX_RP-DATA: src_len=0, dst_len=4 ud_len=10 Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; gsm_04_11.c:609 DST(4,00 89 67 f5 ) Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; gsm_04_11.c:512 RX SMS: Sender: MSISDN:491230000042, MTI: 0x01, VPF: 0x00, MR: 0x23 PID: 0x00, DCS: 0x00, DA: 12345, UserDataLength: 0x00, UserData: "" Sat Apr 14 12:01:14 2018 DLSMS &lt;0017&gt; sms_queue.c:365 Triggering SMS queue Sat Apr 14 12:01:14 2018 DSMPP &lt;000c&gt; smpp_smsc.c:279 Looking up route for (0/0/12345) Sat Apr 14 12:01:14 2018 DSMPP &lt;000c&gt; smpp_smsc.c:307 Using existing default route Sat Apr 14 12:01:14 2018 DSMPP &lt;000c&gt; smpp_smsc.c:314 ACL even has ESME, we can route to it! ===== ==20378==ERROR: AddressSanitizer: heap-use-after-free on address 0x6140000017ea at pc 0x55661f7dd2d6 bp 0x7ffffed4f2460 sp 0x7ffffed4f2458 READ of size 1 at 0x6140000017ea thread T0 #0 0x55661f7dd2d5 in smpp_route /home/laforge/projects/git/osmo-msc/src/libmsc/smpp_smsc.c:316 #1 0x55661f7e3b00 in smpp_try_deliver /home/laforge/projects/git/osmo-msc/src/libmsc/smpp_open_bsc.c:751 #2 0x55661f7a33b2 in sms_route_mt_sms /home/laforge/projects/git/osmo-msc/src/libmsc/gsm_04_11.c:373 #3 0x55661f7a6586 in gsm340_rx_tpdu /home/laforge/projects/git/osmo-msc/src/libmsc/gsm_04_11.c:519 #4 0x55661f7a6586 in gsm411_rx_rp_ud /home/laforge/projects/git/osmo-msc/src/libmsc/gsm_04_11.c:611 #5 0x55661f7a6586 in gsm411_rx_rp_data /home/laforge/projects/git/osmo-msc/src/libmsc/gsm_04_11.c:642 #6 0x55661f7a6586 in gsm411_rx_rl_data /home/laforge/projects/git/osmo-msc/src/libmsc/gsm_04_11.c:801 #7 0x55661f7a6586 in gsm411_rl_recv /home/laforge/projects/git/osmo-msc/src/libmsc/gsm_04_11.c:855 #8 0x7f84c7a07beb in gsm411_mmsms_cp_data /home/laforge/projects/git/libosmocore/src/gsm/gsm04_11_smc.c:303 #9 0x55661f7a808c in gsm0411_rcv_sms /home/laforge/projects/git/osmo-msc/src/libmsc/gsm_04_11.c:983 #10 0x55661f79f082 in gsm0408_dispatch /home/laforge/projects/git/osmo-msc/src/libmsc/gsm_04_0</pre> |          |                        |            |

```

8.c:3497
  #11 0x55661f7d056c in msc_dtap /home/laforge/projects/git/osmo-msc/src/libmsc/osmo_msc.c:143
  #12 0x55661f76a51c in rx_dtap /home/laforge/projects/git/osmo-msc/src/libmsc/a_iface_bssap.c:6
27
  #13 0x55661f76a51c in a_sccp_rx_dt /home/laforge/projects/git/osmo-msc/src/libmsc/a_iface_bssa
p.c:649
  #14 0x55661f764079 in sccp_sap_up /home/laforge/projects/git/osmo-msc/src/libmsc/a_iface.c:565
  #15 0x7f84c77d035e in _osmo_fsm_inst_dispatch /home/laforge/projects/git/libosmocore/src/fsm.c
:517
  #16 0x7f84c713c984 in sccp_scoc_rx_from_src /home/laforge/projects/git/libosmo-sccp/src/sccp_
scoc.c:1581
  #17 0x7f84c713a67a in src_rx_mtp_xfer_ind_xua /home/laforge/projects/git/libosmo-sccp/src/scc
p_src.c:449
  #18 0x7f84c713d554 in mtp_user_prim_cb /home/laforge/projects/git/libosmo-sccp/src/sccp_user.c
:176
  #19 0x7f84c7135392 in m3ua_rx_xfer /home/laforge/projects/git/libosmo-sccp/src/m3ua.c:586
  #20 0x7f84c7135392 in m3ua_rx_msg /home/laforge/projects/git/libosmo-sccp/src/m3ua.c:738
  #21 0x7f84c7140552 in xua_cli_read_cb /home/laforge/projects/git/libosmo-sccp/src/osmo_ss7.c:1
592
  #22 0x7f84c43f71fa in osmo_stream_cli_read /home/laforge/projects/git/libosmo-netif/src/stream
.c:192
  #23 0x7f84c43f71fa in osmo_stream_cli_fd_cb /home/laforge/projects/git/libosmo-netif/src/strea
m.c:276
  #24 0x7f84c77ccdf0 in osmo_fd_disp_fds /home/laforge/projects/git/libosmocore/src/select.c:216
  #25 0x7f84c77ccdf0 in osmo_select_main /home/laforge/projects/git/libosmocore/src/select.c:256
  #26 0x55661f75e59b in main /home/laforge/projects/git/osmo-msc/src/osmo-msc/msc_main.c:694
  #27 0x7f84c58e4a86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21a86)
  #28 0x55661f75f319 in _start (/space/home/laforge/projects/git/osmo-msc/src/osmo-msc/osmo-msc+
0xf8319)

```

0x6140000017ea is located 426 bytes inside of 432-byte region [0x614000001640,0x6140000017f0) freed by thread T0 here:

```

#0 0x7f84c83508c8 in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xd98c8)
#1 0x7f84c7e46e82 in _talloc_free (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x3e82)

```

previously allocated by thread T0 here:

```

#0 0x7f84c8350c20 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xd9c20)
#1 0x7f84c7e49150 in _talloc_zero (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x6150)

```

SUMMARY: AddressSanitizer: heap-use-after-free /home/laforge/projects/git/osmo-msc/src/libmsc/smpp\_smsc.c:316 in smpp\_route

Shadow bytes around the buggy address:

```

0x0c287fff82a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c287fff82b0: 00 00 00 00 00 00 00 00 00 00 00 00 fa fa fa fa
0x0c287fff82c0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
0x0c287fff82d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c287fff82e0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c287fff82f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c287fff8300: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
0x0c287fff8310: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c287fff8320: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c287fff8330: fd fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa fa
0x0c287fff8340: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00

```

Shadow byte legend (one shadow byte represents 8 application bytes):

```

Addressable:                00
Partially addressable:     01 02 03 04 05 06 07
Heap left redzone:         fa
Freed heap region:         fd
Stack left redzone:        f1
Stack mid redzone:         f2
Stack right redzone:       f3
Stack after return:        f5
Stack use after scope:     f8
Global redzone:            f9
Global init order:         f6
Poisoned by user:          f7
Container overflow:        fc
Array cookie:              ac

```

```
Intra object redzone:  bb
ASan internal:         fe
Left alloca redzone:   ca
Right alloca redzone:  cb
==20378==ABORTING
```

#### Related issues:

Related to Cellular Network Infrastructure - Bug #3167: Build osmo-\*  
-master d...

New

04/14/2018

#### History

##### #1 - 04/14/2018 12:55 PM - laforge

ok, it seems that the SMPP connection has just died shortly before the SMS was received. So it seems that `acl->esme` is still set, but 'esme' has already been `free()`d. (reading context at `smpp_smsc.c:316` which is top of the backtrace)

##### #2 - 04/14/2018 12:59 PM - laforge

- Status changed from *New* to *In Progress*
- Assignee changed from *sysmocom* to *laforge*
- % Done changed from *0* to *30*

##### #3 - 04/14/2018 01:08 PM - laforge

- % Done changed from *30* to *80*

proposed patch: <https://gerrit.osmocom.org/7795>

##### #4 - 04/14/2018 01:08 PM - laforge

- Related to Bug #3167: Build osmo-\*  
-master docker containers with address sanitizer added

##### #5 - 04/15/2018 07:43 PM - laforge

- Status changed from *In Progress* to *Resolved*
- % Done changed from *80* to *100*