# OsmoMSC - Bug #2672

## use-after-free on ending a call

11/21/2017 03:26 PM - neels

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 11/21/2017 |
| **Priority:** | Urgent | **Due date:** | |
| **Assignee:** | neels | **% Done:** | 100% |
| **Category:** | | | |
| **Target version:** | | | |
| **Resolution:** | | **Spec Reference:** | |

**Description**

with an asan enabled build of OsmoMSC, I catch a heap use after free when ending a voice call via 3G.

Reproduce in an msc_vlr_test and fix.

details follow...

**Related issues:**

| | | |
|---|---|---|
| Blocks OsmoMSC - Bug #2573: segfault in osmo-msc when subscriber silently van... | **Closed** | **10/12/2017** |

### History

**#1 - 11/21/2017 03:28 PM - neels**

```
20171121160806523 DMM <0002> ../../../../src/osmo-msc/src/libmsc/subscr_conn.c:164 Subscr_Conn(3022658663)[0x6
12000023320]{SUBSCR_CONN_S_COMMUNICATING}: bump: connection still has active transaction: GSM48_PDISC_CC
20171121160806523 DREF <000e> ../../../../src/osmo-msc/src/libmsc/osmo_msc.c:112 MSISDN:123: MSC conn use - 1
== 1
20171121160806523 DLINP <0023> ../../../src/libosmo-netif/src/stream.c:279 connected write
20171121160806523 DLINP <0023> ../../../src/libosmo-netif/src/stream.c:204 sending data
20171121160806523 DLINP <0023> ../../../src/libosmo-netif/src/stream.c:279 connected write
20171121160806523 DLINP <0023> ../../../src/libosmo-netif/src/stream.c:204 sending data
20171121160806523 DLINP <0023> ../../../src/libosmo-netif/src/stream.c:279 connected write
20171121160806523 DLINP <0023> ../../../src/libosmo-netif/src/stream.c:204 sending data
20171121160806841 DLINP <0023> ../../../src/libosmo-netif/src/stream.c:275 connected read
20171121160806841 DLINP <0023> ../../../src/libosmo-netif/src/stream.c:189 message received
20171121160806841 DLSS7 <002d> ../../../src/libosmo-sccp/src/osmo_ss7.c:1513 asp-asp-clnt-OsmoMSC-A-Iu: xua_cl
i_read_cb(): sctp_recvmsg() returned 56 (flags=0x80)
20171121160806841 DLM3UA <0030> ../../../src/libosmo-sccp/src/m3ua.c:721 asp-asp-clnt-OsmoMSC-A-Iu: Received M
3UA Message (XFER:DATA)
20171121160806841 DLM3UA <0030> ../../../src/libosmo-sccp/src/m3ua.c:541 asp-asp-clnt-OsmoMSC-A-Iu: m3ua_rx_xf
er
20171121160806841 DLM3UA <0030> ../../../src/libosmo-sccp/src/m3ua.c:580 asp-asp-clnt-OsmoMSC-A-Iu: m3ua_rx_xf
er(): M3UA data header: opc=24=0.3.0 dpc=185=0.23.1
20171121160806841 DLSS7 <002d> ../../../src/libosmo-sccp/src/osmo_ss7_hmrt.c:208 m3ua_hmdc_rx_from_l2(): found
 dpc=185=0.23.1 as local
20171121160806841 DLSS7 <002d> ../../../src/libosmo-sccp/src/sccp_scrc.c:442 scrc_rx_mtp_xfer_ind_xua:  HDR=(C
O:CODT,V=0,LEN=0),
    PART(T=Destination Reference,L=4,D=0000000d),
    PART(T=Segmentation,L=4,D=00000000),
    PART(T=Data,L=14,D=0014400a0000010010400302836a)
20171121160806841 DLSCCP <002e> ../../../src/libosmo-sccp/src/sccp_scoc.c:1548 Received CO:CODT for local refe
rence 13
20171121160806841 DLSCCP <002e> ../../../src/libosmo-sccp/src/sccp_scoc.c:1581 SCCP-SCOC(13)[0x6120000234a0]{A
CTIVE}: Received Event RCOC-DT1.ind
20171121160806842 DLSCCP <002e> ../../../src/libosmo-sccp/src/sccp_user.c:156 Delivering N-DATA.indication to
SCCP User 'OsmoMSC-IuCS'
20171121160806842 DRANAP <001a> ../../../src/osmo-iuh/src/iu_client.c:709 sccp_sap_up(N-DATA.indication)
20171121160806842 DRANAP <001a> ../../../src/osmo-iuh/src/iu_client.c:743 N-DATA.ind(13, 00 14 40 0a 00 00 01
00 10 40 03 02 83 6a )
20171121160806842 DRR <0003> ../../../src/osmo-iuh/src/ranap_common_cn.c:43 Rx CO IM (Direct Transfer)
20171121160806842 DRLL <0000> ranap_decoder.c:3197 Decoding message RANAP_DirectTransferIEs (ranap_decoder.c:3
197)
20171121160806842 DRANAP <001a> ../../../src/osmo-iuh/src/iu_client.c:459 handle_co(dir=1, proc=20)
20171121160806842 DIUCS <001f> ../../../../src/osmo-msc/src/osmo-msc/msc_main.c:294 got IuCS message 2 bytes:
83 6a
```

```
20171121160806842 DIUCS <001f> ../../../../src/osmo-msc/src/libmsc/iucs.c:111 Looking for IuCS subscriber: con
n_id d
20171121160806842 DIUCS <001f> ../../../../src/osmo-msc/src/libmsc/iucs.c:75   0: MSISDN:124 Iu conn_id 12
20171121160806842 DIUCS <001f> ../../../../src/osmo-msc/src/libmsc/iucs.c:75   1: MSISDN:123 Iu conn_id 13
20171121160806842 DIUCS <001f> ../../../../src/osmo-msc/src/libmsc/iucs.c:99 subscribers registered: 2
20171121160806842 DIUCS <001f> ../../../../src/osmo-msc/src/libmsc/iucs.c:120 Found IuCS subscriber for conn_i
d d
20171121160806842 DREF <000e> ../../../../src/osmo-msc/src/libmsc/osmo_msc.c:107 MSISDN:123: MSC conn use + 1
== 2
20171121160806842 DRLL <0000> ../../../../src/osmo-msc/src/libmsc/gsm_04_08.c:3232 Dispatching 04.08 message G
SM48_MT_CC_RELEASE_COMPL (0x3:0x2a)
20171121160806842 DCC <0001> ../../../../src/osmo-msc/src/libmsc/gsm_04_08.c:1258 stopping pending timer T308
20171121160806842 DMNCC <0006> ../../../../src/osmo-msc/src/libmsc/gsm_04_08.c:1270 transmit message MNCC_REL_
CNF
20171121160806842 DCC <0001> ../../../../src/osmo-msc/src/libmsc/gsm_04_08.c:1293 Sending 'MNCC_REL_CNF' to MN
CC.
20171121160806842 DMNCC <0006> ../../../../src/osmo-msc/src/libmsc/mncc_builtin.c:312 (call 1) Received messag
e MNCC_REL_CNF
20171121160806842 DMNCC <0006> ../../../../src/osmo-msc/src/libmsc/mncc_builtin.c:52 (call 1) Call removed.
20171121160806842 DLMGCP <0031> ../../../../src/osmo-mgw/src/libosmo-mgcp-client/mgcp_client.c:540 Queued 29 b
ytes for MGCP GW
20171121160806842 DCC <0001> ../../../../src/osmo-msc/src/libmsc/gsm_04_08.c:1218 new state RELEASE_REQ -> NUL
L
20171121160806842 DREF <000e> ../../../../src/osmo-msc/src/libmsc/transaction.c:134 VLR subscr MSISDN:123 usag
e decreases to: 2
20171121160806842 DREF <000e> ../../../../src/osmo-msc/src/libmsc/transaction.c:141 MSISDN:123: MSC conn use -
 1 == 1
20171121160806842 DMM <0002> ../../../../src/osmo-msc/src/libmsc/subscr_conn.c:354 Subscr_Conn(3022658663)[0x6
12000023320]{SUBSCR_CONN_S_COMMUNICATING}: Received Event SUBSCR_CONN_E_COMMUNICATING
20171121160806842 DMM <0002> ../../../../src/osmo-msc/src/libmsc/osmo_msc.c:64 Subscr_Conn(3022658663)[0x61200
0023320]{SUBSCR_CONN_S_COMMUNICATING}: Received Event SUBSCR_CONN_E_BUMP
20171121160806842 DMM <0002> ../../../../src/osmo-msc/src/libmsc/subscr_conn.c:168 Subscr_Conn(3022658663)[0x6
12000023320]{SUBSCR_CONN_S_COMMUNICATING}: bump: releasing conn
20171121160806842 DMM <0002> ../../../../src/osmo-msc/src/libmsc/subscr_conn.c:169 Subscr_Conn(3022658663)[0x6
12000023320]{SUBSCR_CONN_S_COMMUNICATING}: state_chg to SUBSCR_CONN_S_RELEASED
20171121160806842 DMM <0002> ../../../../src/osmo-msc/src/libmsc/subscr_conn.c:243 Subscr_Conn(3022658663)[0x6
12000023320]{SUBSCR_CONN_S_RELEASED}: Terminating (cause = OSMO_FSM_TERM_REGULAR)
20171121160806842 DVLR <001e> ../../../../src/osmo-msc/src/libmsc/subscr_conn.c:243 Process_Access_Request_VLR
(3022658663)[0x6120000231a0]{PR_ARQ_S_DONE}: Terminating (cause = OSMO_FSM_TERM_PARENT)
20171121160806842 DVLR <001e> ../../../../src/osmo-msc/src/libmsc/subscr_conn.c:243 Process_Access_Request_VLR
(3022658663)[0x6120000231a0]{PR_ARQ_S_DONE}: Removing from parent Subscr_Conn(3022658663)[0x612000023320]
20171121160806842 DVLR <001e> ../../../../src/osmo-msc/src/libmsc/subscr_conn.c:243 Process_Access_Request_VLR
(3022658663)[0x6120000231a0]{PR_ARQ_S_DONE}: Freeing instance
20171121160806842 DVLR <001e> ../../../src/libosmocore/src/fsm.c:287 Process_Access_Request_VLR(3022658663)[0x
6120000231a0]{PR_ARQ_S_DONE}: Deallocated
20171121160806842 DMM <0002> ../../../../src/osmo-msc/src/libmsc/osmo_msc.c:328 msc_subscr_conn_close(vsub=MSI
SDN:123, cause=2): no conn fsm, releasing directly without release event.
20171121160806842 DLSCCP <002e> ../../../src/libosmo-sccp/src/sccp_scoc.c:1615 Received SCCP User Primitive N-
DATA.request)
20171121160806842 DLSCCP <002e> ../../../src/libosmo-sccp/src/sccp_scoc.c:1653 SCCP-SCOC(13)[0x6120000234a0]{A
CTIVE}: Received Event N-DATA.req
20171121160806842 DLSS7 <002d> ../../../src/libosmo-sccp/src/sccp_scrc.c:391 sccp_scrc_rx_scoc_conn_msg:  HDR=
(CO:CODT,V=0,LEN=0),
    PART(T=Routing Context,L=4,D=00000000),
    PART(T=Destination Reference,L=4,D=000003e8),
    PART(T=Data,L=13,D=00010009000001000440020780)
20171121160806842 DLSS7 <002d> ../../../src/libosmo-sccp/src/osmo_ss7_hmrt.c:212 m3ua_hmdc_rx_from_l2(): dpc=2
4=0.3.0 not local, message is for routing
20171121160806842 DLSS7 <002d> ../../../src/libosmo-sccp/src/osmo_ss7_hmrt.c:166 Found route for dpc=24=0.3.0:
 pc=0=0.0.0 mask=0x0 via AS as-clnt-OsmoMSC-A-Iu proto=m3ua
20171121160806842 DLSS7 <002d> ../../../src/libosmo-sccp/src/osmo_ss7_hmrt.c:171 rt->dest.as proto is M3UA for
 dpc=24=0.3.0
20171121160806842 DLSS7 <002d> ../../../src/libosmo-sccp/src/m3ua.c:507 XUA_AS(as-clnt-OsmoMSC-A-Iu)[0x6120000
05da0]{AS_ACTIVE}: Received Event AS-TRANSFER.req
20171121160806842 DREF <000e> ../../../../src/osmo-msc/src/libmsc/subscr_conn.c:228 MSISDN:123: MSC conn use -
 1 == 0
20171121160806842 DRLL <0000> ../../../../src/osmo-msc/src/libmsc/osmo_msc.c:230 subscr MSISDN:123: Freeing su
bscriber connection
20171121160806842 DREF <000e> ../../../../src/osmo-msc/src/libmsc/osmo_msc.c:232 VLR subscr MSISDN:123 usage d
ecreases to: 1
20171121160806842 DMM <0002> ../../../../src/osmo-msc/src/libmsc/subscr_conn.c:243 Subscr_Conn(3022658663)[0x6
12000023320]{SUBSCR_CONN_S_RELEASED}: Freeing instance
20171121160806842 DMM <0002> ../../../src/libosmocore/src/fsm.c:287 Subscr_Conn(3022658663)[0x612000023320]{SU
BSCR_CONN_S_RELEASED}: Deallocated
```

```
20171121160806842 DMM <0002> ../../../src/libosmocore/src/fsm.c:287 Subscr_Conn(3022658663)[0x612000023320]{SU
BSCR_CONN_S_RELEASED}: Deallocated
=================================================================
==31038==ERROR: AddressSanitizer: heap-use-after-free on address 0x6150000037f0 at pc 0x45ba22 bp 0x7fffffffd5
70 sp 0x7fffffffd568
READ of size 4 at 0x6150000037f0 thread T0
    #0 0x45ba21 in _msc_subscr_conn_put ../../../../src/osmo-msc/src/libmsc/osmo_msc.c:367
    #1 0x46013a in gsm0408_rcvmsg_iucs ../../../../src/osmo-msc/src/libmsc/iucs.c:167
    #2 0x7ffff45994c4 in ranap_handle_co_dt ../../../src/osmo-iuh/src/iu_client.c:335
    #3 0x7ffff45994c4 in cn_ranap_handle_co ../../../src/osmo-iuh/src/iu_client.c:469
    #4 0x7ffff4590f6c in ranap_cn_rx_co ../../../src/osmo-iuh/src/ranap_common_cn.c:307
    #5 0x7ffff45954b5 in sccp_sap_up ../../../src/osmo-iuh/src/iu_client.c:746
    #6 0x7ffff5ffb941 in _osmo_fsm_inst_dispatch ../../../src/libosmocore/src/fsm.c:450
    #7 0x7ffff5071d23 in sccp_scoc_rx_from_scrc ../../../src/libosmo-sccp/src/sccp_scoc.c:1581
    #8 0x7ffff5066190 in scrc_rx_mtp_xfer_ind_xua ../../../src/libosmo-sccp/src/sccp_scrc.c:449
    #9 0x7ffff507478e in mtp_user_prim_cb ../../../src/libosmo-sccp/src/sccp_user.c:176
    #10 0x7ffff5040830 in m3ua_rx_xfer ../../../src/libosmo-sccp/src/m3ua.c:586
    #11 0x7ffff5040830 in m3ua_rx_msg ../../../src/libosmo-sccp/src/m3ua.c:738
    #12 0x7ffff507f22f in xua_cli_read_cb ../../../src/libosmo-sccp/src/osmo_ss7.c:1554
    #13 0x7ffff1ec0165 in osmo_stream_cli_read ../../../src/libosmo-netif/src/stream.c:192
    #14 0x7ffff1ec0165 in osmo_stream_cli_fd_cb ../../../src/libosmo-netif/src/stream.c:276
    #15 0x7ffff5feb5b4 in osmo_fd_disp_fds ../../../src/libosmocore/src/select.c:216
    #16 0x7ffff5feb5b4 in osmo_select_main ../../../src/libosmocore/src/select.c:256
    #17 0x407e8b in main ../../../../src/osmo-msc/src/osmo-msc/msc_main.c:559
    #18 0x7ffff328db44 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b44)
    #19 0x4088a4 (/usr/local/bin/osmo-msc+0x4088a4)

0x6150000037f0 is located 112 bytes inside of 480-byte region [0x615000003780,0x615000003960)
freed by thread T0 here:
    #0 0x7ffff6f59527 in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.1+0x54527)
    #1 0x7ffff6a0a522 in _talloc_free (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x3522)

previously allocated by thread T0 here:
    #0 0x7ffff6f5973f in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.1+0x5473f)
    #1 0x7ffff6a0e630 in _talloc_zero (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x7630)

SUMMARY: AddressSanitizer: heap-use-after-free ../../../../src/osmo-msc/src/libmsc/osmo_msc.c:367 _msc_subscr_
conn_put
Shadow bytes around the buggy address:
  0x0c2a7fff86a0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a7fff86b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a7fff86c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a7fff86d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa
  0x0c2a7fff86e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c2a7fff86f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd[fd]fd
  0x0c2a7fff8700: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a7fff8710: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a7fff8720: fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c2a7fff8730: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fff8740: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Contiguous container OOB:fc
  ASan internal:           fe
==31038==ABORTING
[Inferior 1 (process 31038) exited with code 01]
```

#### #2 - 11/21/2017 09:51 PM - neels

*- Status changed from New to In Progress*

#### #3 - 11/22/2017 12:14 PM - neels

*- % Done changed from 0 to 70*

got it reproduced in msc_vlr_test_call, in the MT call leg

#### #4 - 11/23/2017 12:55 AM - neels

*- % Done changed from 70 to 90*

https://gerrit.osmocom.org/4974 fixes the issue, amid a number of improvement patches around that failure.

#### #5 - 11/27/2017 02:44 PM - neels

still waiting for review of https://gerrit.osmocom.org/4972 and https://gerrit.osmocom.org/4971 that precede the fix. I could rebase the fix onto master, but with 4972 first the fix is shown clearly in the regression test logs.

#### #6 - 11/27/2017 02:56 PM - neels

*- Blocks Bug #2573: segfault in osmo-msc when subscriber silently vanishes added*

#### #7 - 11/28/2017 01:32 AM - neels

*- Status changed from In Progress to Resolved*

*- % Done changed from 90 to 100*

merged

#### #8 - 02/06/2018 08:26 AM - laforge

*- Status changed from Resolved to Closed*