OsmoMSC - Bug #4340

Malformed MM Identity Response crashes OsmoMSC

12/27/2019 10:19 PM - fixeria

Status:	Resolved	**Start date:**	12/28/2019
Priority:	Urgent	**Due date:**	
Assignee:	fixeria	**% Done:**	100%
Category:			
Target version:			
Resolution:		**Spec Reference:**	

Description

From time to time we receive a MM Identity Response that crashes OsmoMSC:

```
(gdb) bt
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
#1  0x00007f8ec198c5fe in __GI_abort () at abort.c:100
#2  0x00007f8ec2016210 in osmo_panic_default (args=0x7ffe75e09f88, fmt=0x558dc6301189 "Assert fail
ed %s %s:%d\n") at ../../../src/libosmocore/src/panic.c:49
#3  osmo_panic (fmt=fmt@entry=0x558dc6301189 "Assert failed %s %s:%d\n") at ../../../src/libosmoco
re/src/panic.c:84
#4  0x0000558dc62f9181 in vlr_subscr_rx_id_resp (vsub=vsub@entry=0x558dc81738e0, mi=mi@entry=0x558
dc811f196 "\377\377\377\377\377\377\377\377", mi_len=mi_len@entry=8)
    at ../../../../src/osmo-msc/src/libvlr/vlr.c:1189
#5  0x0000558dc62ea90e in mm_rx_id_resp (msg=<optimized out>, msc_a=<optimized out>) at ../../../.
./src/osmo-msc/src/libmsc/gsm_04_08.c:197
#6  gsm0408_rcv_mm (msc_a=<optimized out>, msg=<optimized out>) at ../../../../src/osmo-msc/src/li
bmsc/gsm_04_08.c:1086
#7  0x0000558dc62c31cc in msc_a_ran_dec_from_msc_i (msc_a=msc_a@entry=0x558dc8130060, d=d@entry=0x
7ffe75e0ace0) at ../../../../src/osmo-msc/src/libmsc/msc_a.c:1484
#8  0x0000558dc62c3cde in msc_a_ran_decode_cb (msc_a_fi=<optimized out>, data=0x7ffe75e0ace0, msg=
0x7ffe75e0a750) at ../../../../src/osmo-msc/src/libmsc/msc_a.c:1643
#9  0x0000558dc62d0dde in ran_a_decode_l3 (ran_dec=<optimized out>, l3=<optimized out>) at ../../.
./../src/osmo-msc/src/libmsc/ran_msg_a.c:884
#10 0x0000558dc62c09d6 in msc_role_ran_decode (fi=0x558dc8127cb0, an_apdu=an_apdu@entry=0x7ffe75e0
b370, decode_cb=decode_cb@entry=0x558dc62c3be0 <msc_a_ran_decode_cb>,
    decode_cb_data=decode_cb_data@entry=0x7ffe75e0ace0) at ../../../../src/osmo-msc/src/libmsc/msu
b.c:589
#11 0x0000558dc62c179a in msc_a_ran_dec (msc_a=0x558dc8130060, an_apdu=0x7ffe75e0b370, from_role=<
optimized out>) at ../../../../src/osmo-msc/src/libmsc/msc_a.c:184
#12 0x00007f8ec200eaf9 in _osmo_fsm_inst_dispatch (fi=0x558dc8127cb0, event=9, data=0x7ffe75e0b370
, file=0x558dc630de00 "../../../../src/osmo-msc/src/libmsc/msc_i.c",
    line=85) at ../../../src/libosmocore/src/fsm.c:877
#13 0x0000558dc62d0dde in ran_a_decode_l3 (ran_dec=<optimized out>, l3=<optimized out>) at ../../.
./../src/osmo-msc/src/libmsc/ran_msg_a.c:884
#14 0x0000558dc62c09d6 in msc_role_ran_decode (fi=0x558dc81268a0, an_apdu=0x7ffe75e0b370, decode_c
b=<optimized out>, decode_cb_data=<optimized out>)
    at ../../../../src/osmo-msc/src/libmsc/msub.c:589
--Type <RET> for more, q to quit, c to continue without paging--
#15 0x00007f8ec200eaf9 in _osmo_fsm_inst_dispatch (fi=0x558dc81268a0, event=event@entry=9, data=da
ta@entry=0x7ffe75e0b370,
    file=file@entry=0x558dc63129b8 "../../../../src/osmo-msc/src/libmsc/ran_peer.c", line=line@ent
ry=412) at ../../../src/libosmocore/src/fsm.c:877
#16 0x0000558dc62d5bcd in ran_peer_st_ready (fi=<optimized out>, event=2, data=0x7ffe75e0b430) at
../../../../src/osmo-msc/src/libmsc/ran_peer.c:412
#17 0x00007f8ec200eaf9 in _osmo_fsm_inst_dispatch (fi=0x558dc8118ad0, event=2, data=data@entry=0x7
ffe75e0b430,
    file=file@entry=0x558dc63129b8 "../../../../src/osmo-msc/src/libmsc/ran_peer.c", line=line@ent
ry=596) at ../../../src/libosmocore/src/fsm.c:877
#18 0x0000558dc62d69b5 in ran_peer_up_l2 (sri=0x558dc8114750, calling_addr=0x0, co=<optimized out>
, conn_id=<optimized out>, l2=<optimized out>)
    at ../../../../src/osmo-msc/src/libmsc/ran_peer.c:596
#19 0x0000558dc62ad606 in sccp_ran_sap_up (oph=0x558dc811f088, _scu=<optimized out>) at ../../../.
```

```
./src/osmo-msc/src/libmsc/sccp_ran.c:110
#20 0x00007f8ec200eaf9 in _osmo_fsm_inst_dispatch (fi=0x558dc817e4f0, event=11, data=data@entry=0x
558dc8122a90,
    file=file@entry=0x7f8ec1da6e08 "../../../src/libosmo-sccp/src/sccp_scoc.c", line=line@entry=16
77) at ../../../src/libosmocore/src/fsm.c:877
#21 0x00007f8ec1d950bc in sccp_scoc_rx_from_scrc (inst=inst@entry=0x558dc8118310, xua=xua@entry=0x
558dc8122a90) at ../../../src/libosmo-sccp/src/sccp_scoc.c:1677
#22 0x00007f8ec1d92b1e in scrc_rx_mtp_xfer_ind_xua (inst=inst@entry=0x558dc8118310, xua=0x558dc812
2a90) at ../../../src/libosmo-sccp/src/sccp_scrc.c:457
#23 0x00007f8ec1d95ccd in mtp_user_prim_cb (oph=0x558dc8180a98, ctx=0x558dc8118310) at ../../../sr
c/libosmo-sccp/src/sccp_user.c:176
#24 0x00007f8ec1d8d62d in m3ua_rx_xfer (xua=0x558dc81824b0, asp=0x558dc811eb00) at ../../../src/li
bosmo-sccp/src/m3ua.c:586
#25 m3ua_rx_msg (asp=asp@entry=0x558dc811eb00, msg=msg@entry=0x558dc817fd20) at ../../../src/libos
mo-sccp/src/m3ua.c:739
#26 0x00007f8ec1d9cc83 in xua_cli_read_cb (conn=0x558dc811c130) at ../../../src/libosmo-sccp/src/o
smo_ss7.c:1701
#27 0x00007f8ec1fd5d93 in osmo_stream_cli_read (cli=0x558dc811c130) at ../../../src/libosmo-netif/
src/stream.c:222
#28 osmo_stream_cli_fd_cb (ofd=<optimized out>, what=1) at ../../../src/libosmo-netif/src/stream.c
:311
#29 0x00007f8ec200a25a in osmo_fd_disp_fds (_eset=<optimized out>, _wset=<optimized out>, _rset=<o
ptimized out>) at ../../../src/libosmocore/src/select.c:227
#30 _osmo_select_main (polling=<optimized out>) at ../../../src/libosmocore/src/select.c:265
#31 0x00007f8ec200a826 in osmo_select_main_ctx (polling=<optimized out>) at ../../../src/libosmoco
re/src/select.c:291
#32 0x0000558dc62abfe3 in main (argc=<optimized out>, argv=0x7ffe75e0ba48) at ../../../../src/osmo
-msc/src/osmo-msc/msc_main.c:729
```

the message contains invalid Mobile Identity:

```
(gdb) p mi_len
$8 = 8
(gdb) x/2 mi
0x558dc811f196: 0xffffffff      0xffffffff
```

basically all bytes are 0xff.

History

#1 - 12/28/2019 12:27 AM - fixeria

- Status changed from New to Feedback

- Assignee set to fixeria

- % Done changed from 0 to 80

https://gerrit.osmocom.org/c/osmo-msc/+/16683 libmsc/gsm_04_08.c: fix: do not crash on malformed Mobile Identity

This is a quick and dirty fix. We still need to investigate *why* the MS sends an incorrect Mobile Identity.
I noticed a malformed packet in Wireshark, but unfortunately did not save it :/

#2 - 12/28/2019 12:33 AM - fixeria

Huh,

> (gdb) p mi_len
> $8 = 8
> (gdb) x/2 mi
> 0x558dc811f196: 0xffffffff 0xffffffff

this looks pretty much like an IMSI (8 octets may contain 15 BCD-encoded digits + padding) of a non-/half-provisioned SIM card ('ff'O fillig).

#3 - 12/28/2019 03:27 PM - fixeria

Finally caught one of those packets:

```
BSSAP
    Message Type: Direct Transfer (0x01)
    Data Link Connection Identifier
        00.. .... = Control Channel: not further specified (0x0)
        ..00 0... = Spare: 0x0
        .... .000 = SAPI: RR/MM/CC (0x0)
    Length: 11
GSM A-I/F DTAP - Identity Response
    Protocol Discriminator: Mobility Management messages (5)
        .... 0101 = Protocol discriminator: Mobility Management messages (0x5)
        0000 .... = Skip Indicator: No indication of selected PLMN (0)
    01.. .... = Sequence number: 1
    ..01 1001 = DTAP Mobility Management Message Type: Identity Response (0x19)
    Mobile Identity - Format Unknown
        Length: 8
        .... 1... = Odd/even indication: Odd number of identity digits
        .... .111 = Mobile Identity Type: Unknown (7)  <-- This makes OsmoMSC crash
            [Expert Info (Warning/Protocol): Unknown format 7]
                [Unknown format 7]
                [Severity level: Warning]
                [Group: Protocol]
```

#4 - 12/28/2019 04:58 PM - fixeria

The crash can also be reproduced with Mobile Identity Type '000'B (no identity):

https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/16684 MSC_Tests.ttcn: introduce TC_invalid_id_resp_crash for OS#4340

#5 - 01/05/2020 09:11 PM - fixeria

- Status changed from Feedback to Resolved

- % Done changed from 80 to 100

All changes have been merged, the problem is fixed.