# OsmoNITB - Bug #70

## nitb crashes in the rtp_proxy when a phone on a MT-call sends a 'CONNECT' before the CRCX ACK came back

02/19/2016 10:47 PM - zecke2

| | | | |
|---|---|---|---|
| **Status:** | New | **Start date:** | |
| **Priority:** | Low | **Due date:** | |
| **Assignee:** | | **% Done:** | 0% |
| **Category:** | | | |
| **Target version:** | | | |
| **Spec Reference:** | | | |

**Description**

Using the FakeBTS it is possible to crash nitb on a MT-call. It appears to that if the MS sends a CALL CONFIRMED and then a CONNECT the rtp_socket is not fully setup and when one attempts to bridge them we have a crash.

### History

#### #1 - 12/25/2012 07:42 AM - zecke2

0004> abis_rsl.c:1411 (bts=0,trx=0,ts=2,ss=0) Activating ARFCN SS lctype TCH/F r=CALL ra=0x42 ta=23
<0004> abis_rsl.c:1148 (bts=0,trx=0,ts=2,ss=0) CHANNEL ACTIVATE ACK
<0000> abis_rsl.c:1591 (bts=0,trx=0,ts=2,ss=0) SAPI=0 ESTABLISH INDICATION
<0002> gsm_04_08.c:875 <- CM SERVICE REQUEST serv_type=0x00 mi_type=0x04 M(1828428732)
<000d> db.c:647 Found Subscriber: ID 1, IMSI 901010000001111, NAME _, TMSI 1828428732, EXTEN '21951', LAC 1, AUTH 1
<000d> db.c:742 Sync Equipment IMEI=6666666666666666, classmark1=33, classmark2=33 19 a2 , classmark3=a3 65 b7 50 9f 6c 08 10
<0002> gsm_04_08.c:801 -> CM SERVICE ACK
<0001> gsm_04_08.c:116 (bts 0 trx 0 ts 2 pd 05) Sending 0x21 to MS.
<0000> abis_rsl.c:1591 (bts=0,trx=0,ts=2,ss=0) SAPI=0 DATA INDICATION
<0001> gsm_04_08.c:3141 (bts 0 trx 0 ts 2 ti 9 sub 21951) Received 'SETUP' from MS in state 0 (NULL)
<0001> gsm_04_08.c:3146 Unknown transaction ID 9, creating new trans.
<0001> transaction.c:69 subscr=0x4a0c458, subscr->net=0x4368eb0
<0001> gsm_04_08.c:1194 new state NULL -> INITIATED
<0001> gsm_04_08.c:1799 Subscriber 901010000001111 (21951) sends SETUP to 40000
<0001> gsm_04_08.c:1255 (bts 0 trx 0 ts 2 ti 9 sub 21951) Sending 'MNCC_SETUP_IND' to MNCC.
<0006> mncc_builtin.c:339 (call 80000002) Call created.
<0006> mncc_builtin.c:348 (call 80000002) Received message MNCC_SETUP_IND
<0006> mncc_builtin.c:120 (call 80000002) Creating new remote instance 2.
<0006> mncc_builtin.c:129 (call 80000002) Accepting call.
<0006> gsm_04_08.c:2862 receive message MNCC_CALL_PROC_REQ
<0001> gsm_04_08.c:3048 (bts 0 trx 0 ts 2 ti 09 sub 21951) Received 'MNCC_CALL_PROC_REQ' from MNCC in state 1 (INITIATED)
<0001> gsm_04_08.c:1194 new state INITIATED -> MO_CALL_PROC
<0001> gsm_04_08.c:110 (bts 0 trx 0 ts 2 ti 90) Sending 'CALL_PROC' to MS.
<0006> mncc_builtin.c:136 (call 80000002) Modify channel mode.
<0006> gsm_04_08.c:2862 receive message MNCC_LCHAN_MODIFY
<0001> gsm_04_08.c:3048 (bts 0 trx 0 ts 2 ti 09 sub 21951) Received 'MNCC_LCHAN_MODIFY' from MNCC in state 3 (MO_CALL_PROC)
<000a> bsc_api.c:374 Sending ChanModify for speech 33 1
<0003> gsm_04_08_utils.c:460 -> CHANNEL MODE MODIFY mode=0x21
<0006> mncc_builtin.c:143 (call 80000002) Forwarding SETUP to remote.
<0006> gsm_04_08.c:2862 receive message MNCC_SETUP_REQ
<000d> db.c:647 Found Subscriber: ID 2, IMSI 901010000001112, NAME _, TMSI 494545837, EXTEN '40000', LAC 1, AUTH 1
<0001> transaction.c:69 subscr=0x4a54078, subscr->net=0x4368eb0
<0007> paging.c:285 Start paging of subscriber 2 on bts 0.
<0007> paging.c:285 Start paging of subscriber 2 on bts 1.
<0000> abis_rsl.c:1591 (bts=0,trx=0,ts=2,ss=0) SAPI=0 DATA INDICATION
<0003> gsm_04_08_utils.c:506 CHANNEL MODE MODIFY ACK
<0004> abis_rsl.c:1796 (bts=0,trx=0,ts=2,ss=0) IPAC_BIND speech_mode=0x11 RTP_PAYLOAD=97
<000a> osmo_msc.c:79 Assignment complete should not have been reached.
<0004> abis_rsl.c:1167 (bts=0,trx=0,ts=2,ss=0) CHANNEL MODE MODIFY ACK
<0004> abis_rsl.c:1954 (bts=0,trx=0,ts=2,ss=0) IPAC_CRCX_ACK LOCAL_IP=0.0.0.0 LOCAL_PORT=5930 CON_ID=1 <001a> rtp_proxy.c:533 rtp_socket_create(): success
<001a> rtp_proxy.c:615 rtp_socket_bind(rs=0x4a75d48, IP=0.0.0.0): BOUND_IP=0.0.0.0, BOUND_PORT=30002
<001a> rtp_proxy.c:666 rtp_socket_connect(rs=0x4a75d48, ip=0.0.0.0, port=5930)

<0007> paging.c:81 Going to send paging commands: imsi: '901010000001112' tmsi: '0x1d7a2bad'
<0007> paging.c:81 Going to send paging commands: imsi: '901010000001112' tmsi: '0x1d7a2bad'
<0004> abis_rsl.c:1411 (bts=1,trx=0,ts=2,ss=0) Activating ARFCN SS lctype TCH/F r=CALL ra=0x45 ta=23
<0004> abis_rsl.c:1148 (bts=1,trx=0,ts=2,ss=0) CHANNEL ACTIVATE ACK

<0000> abis_rsl.c:1591 (bts=1,trx=0,ts=2,ss=0) SAPI=0 ESTABLISH INDICATION
<0003> gsm_04_08.c:1092 PAGING RESPONSE: mi_type=0x04 MI
<0003> gsm_04_08.c:1110 <- Channel was requested by 901010000001112
<000d> db.c:742 Sync Equipment IMEI=6666666666666666, classmark1=33, classmark2=33 19 a2 , classmark3=a3 65 b7 50 9f 6c 08 10
<0007> paging.c:353 Stop paging on bts 1, calling cbfn.
<0001> gsm_04_08.c:1338 Paging subscr 40000 succeeded!
<0001> gsm_04_08.c:1720 starting timer T303 with 30 seconds
<0001> gsm_04_08.c:1194 new state NULL -> CALL_PRESENT
<0001> gsm_04_08.c:110 (bts 1 trx 0 ts 2 ti 00) Sending 'SETUP' to MS.
<0007> paging.c:357 Stop paging on bts 0 silently.
<0000> abis_rsl.c:1591 (bts=1,trx=0,ts=2,ss=0) SAPI=0 DATA INDICATION
<0001> gsm_04_08.c:3141 (bts 1 trx 0 ts 2 ti 0 sub 40000) Received 'CALL_CONF' from MS in state 6 (CALL_PRESENT)
<0001> gsm_04_08.c:1235 stopping pending timer T303
<0001> gsm_04_08.c:1720 starting timer T310 with 180 seconds
<0001> gsm_04_08.c:1194 new state CALL_PRESENT -> MO_TERM_CALL_CONF
<0001> gsm_04_08.c:1255 (bts 1 trx 0 ts 2 ti 0 sub 40000) Sending 'MNCC_CALL_CONF_IND' to MNCC.
<0006> mncc_builtin.c:348 (call 2) Received message MNCC_CALL_CONF_IND
<0006> gsm_04_08.c:2862 receive message MNCC_LCHAN_MODIFY
<0001> gsm_04_08.c:3048 (bts 1 trx 0 ts 2 ti 00 sub 40000) Received 'MNCC_LCHAN_MODIFY' from MNCC in state 9 (MO_TERM_CALL_CONF)
<000a> bsc_api.c:374 Sending ChanModify for speech 33 1
<0003> gsm_04_08_utils.c:460 -> CHANNEL MODE MODIFY mode=0x21
<0000> abis_rsl.c:1591 (bts=1,trx=0,ts=2,ss=0) SAPI=0 DATA INDICATION
<0003> gsm_04_08_utils.c:506 CHANNEL MODE MODIFY ACK
<0004> abis_rsl.c:1796 (bts=1,trx=0,ts=2,ss=0) IPAC_BIND speech_mode=0x11 RTP_PAYLOAD=97
<000a> osmo_msc.c:79 Assignment complete should not have been reached.
<0000> abis_rsl.c:1591 (bts=1,trx=0,ts=2,ss=0) SAPI=0 DATA INDICATION
<0001> gsm_04_08.c:3141 (bts 1 trx 0 ts 2 ti 0 sub 40000) Received 'CONNECT' from MS in state 9 (MO_TERM_CALL_CONF)
<0001> gsm_04_08.c:1235 stopping pending timer T310
<0001> gsm_04_08.c:1194 new state MO_TERM_CALL_CONF -> CONNECT_REQUEST
<0001> gsm_04_08.c:1255 (bts 1 trx 0 ts 2 ti 0 sub 40000) Sending 'MNCC_SETUP_CNF' to MNCC.
<0006> mncc_builtin.c:348 (call 2) Received message MNCC_SETUP_CNF
<0006> mncc_builtin.c:189 (call 2) Acknowledge SETUP.
<0006> gsm_04_08.c:2862 receive message MNCC_SETUP_COMPL_REQ
<0001> gsm_04_08.c:3048 (bts 1 trx 0 ts 2 ti 00 sub 40000) Received 'MNCC_SETUP_COMPL_REQ' from MNCC in state 8
(CONNECT_REQUEST)
<0001> gsm_04_08.c:1194 new state CONNECT_REQUEST -> ACTIVE
<0001> gsm_04_08.c:110 (bts 1 trx 0 ts 2 ti 00) Sending 'CONNECT_ACK' to MS.
<0006> mncc_builtin.c:196 (call 2) Sending CONNECT to remote.
<0006> gsm_04_08.c:2862 receive message MNCC_SETUP_RSP
<0001> gsm_04_08.c:3048 (bts 0 trx 0 ts 2 ti 09 sub 21951) Received 'MNCC_SETUP_RSP' from MNCC in state 3 (MO_CALL_PROC)
<0001> gsm_04_08.c:1720 starting timer T313 with 30 seconds
<0001> gsm_04_08.c:1194 new state MO_CALL_PROC -> CONNECT_IND
<0001> gsm_04_08.c:110 (bts 0 trx 0 ts 2 ti 90) Sending 'CONNECT' to MS.
<0006> mncc_builtin.c:202 (call 2) Bridging with remote.
<0006> gsm_04_08.c:2862 receive message MNCC_BRIDGE
<0001> gsm_04_08.c:1502 Setting up TCH map between (bts=1,trx=0,ts=2) and (bts=0,trx=0,ts=2)
6856 Invalid read of size 2
6856 at 0x806536F: rsl_ipacc_mdcx_to_rtpsock (abis_rsl.c:1853)
6856 by 0x8080837: mncc_tx_to_cc (gsm_04_08.c:1515)
6856 by 0x807725A: int_mncc_recv (mncc_builtin.c:212)
6856 by 0x807BCBA: mncc_recvmsg (gsm_04_08.c:83)
6856 by 0x807CA07: gsm48_cc_rx_connect (gsm_04_08.c:2103)
6856 by 0x808139F: gsm0408_dispatch (gsm_04_08.c:3171)
6856 by 0x804F287: gsm0408_rcvmsg (bsc_api.c:623)
6856 by 0x80665AD: abis_rsl_rcvmsg (abis_rsl.c:1612)
6856 by 0x40CC89F: ipaccess_fd_cb (ipaccess.c:452)
6856 by 0x40AE4F1: osmo_select_main (select.c:158)
6856 by 0x804D3B8: main (bsc_hack.c:331)
6856 Address 0xa is not stack'd, malloc'd or (recently) free'd
6856
6856
6856 Process terminating with default action of signal 11 (SIGSEGV): dumping core
6856 Access not within mapped region at address 0xA
6856 at 0x806536F: rsl_ipacc_mdcx_to_rtpsock (abis_rsl.c:1853)
6856 by 0x8080837: mncc_tx_to_cc (gsm_04_08.c:1515)
6856 by 0x807725A: int_mncc_recv (mncc_builtin.c:212)
6856 by 0x807BCBA: mncc_recvmsg (gsm_04_08.c:83)
6856 by 0x807CA07: gsm48_cc_rx_connect (gsm_04_08.c:2103)
6856 by 0x808139F: gsm0408_dispatch (gsm_04_08.c:3171)
6856 by 0x804F287: gsm0408_rcvmsg (bsc_api.c:623)
6856 by 0x80665AD: abis_rsl_rcvmsg (abis_rsl.c:1612)
6856 by 0x40CC89F: ipaccess_fd_cb (ipaccess.c:452)
6856 by 0x40AE4F1: osmo_select_main (select.c:158)
6856 by 0x804D3B8: main (bsc_hack.c:331)

#### #2 - 12/25/2012 07:42 AM - zecke2

```
0004> abis_rsl.c:1411 (bts=0,trx=0,ts=2,ss=0) Activating ARFCN(872) SS(0) lctype TCH/F r=CALL ra=0x42 ta=23
<0004> abis_rsl.c:1148 (bts=0,trx=0,ts=2,ss=0) CHANNEL ACTIVATE ACK
<0000> abis_rsl.c:1591 (bts=0,trx=0,ts=2,ss=0) SAPI=0 ESTABLISH INDICATION
<0002> gsm_04_08.c:875 <- CM SERVICE REQUEST serv_type=0x00 mi_type=0x04 M(1828428732)
<000d> db.c:647 Found Subscriber: ID 1, IMSI 901010000001111, NAME _, TMSI 1828428732, EXTEN '21951', LAC 1, A
UTH 1
<000d> db.c:742 Sync Equipment IMEI=6666666666666666, classmark1=33, classmark2=33 19 a2 , classmark3=a3 65 b7
 50 9f 6c 08 10
<0002> gsm_04_08.c:801 -> CM SERVICE ACK
<0001> gsm_04_08.c:116 (bts 0 trx 0 ts 2 pd 05) Sending 0x21 to MS.
<0000> abis_rsl.c:1591 (bts=0,trx=0,ts=2,ss=0) SAPI=0 DATA INDICATION
<0001> gsm_04_08.c:3141 (bts 0 trx 0 ts 2 ti 9 sub 21951) Received 'SETUP' from MS in state 0 (NULL)
<0001> gsm_04_08.c:3146 Unknown transaction ID 9, creating new trans.
<0001> transaction.c:69 subscr=0x4a0c458, subscr->net=0x4368eb0
<0001> gsm_04_08.c:1194 new state NULL -> INITIATED
<0001> gsm_04_08.c:1799 Subscriber 901010000001111 (21951) sends SETUP to 40000
<0001> gsm_04_08.c:1255 (bts 0 trx 0 ts 2 ti 9 sub 21951) Sending 'MNCC_SETUP_IND' to MNCC.
<0006> mncc_builtin.c:339 (call 80000002) Call created.
<0006> mncc_builtin.c:348 (call 80000002) Received message MNCC_SETUP_IND
<0006> mncc_builtin.c:120 (call 80000002) Creating new remote instance 2.
<0006> mncc_builtin.c:129 (call 80000002) Accepting call.
<0006> gsm_04_08.c:2862 receive message MNCC_CALL_PROC_REQ
<0001> gsm_04_08.c:3048 (bts 0 trx 0 ts 2 ti 09 sub 21951) Received 'MNCC_CALL_PROC_REQ' from MNCC in state 1
(INITIATED)
<0001> gsm_04_08.c:1194 new state INITIATED -> MO_CALL_PROC
<0001> gsm_04_08.c:110 (bts 0 trx 0 ts 2 ti 90) Sending 'CALL_PROC' to MS.
<0006> mncc_builtin.c:136 (call 80000002) Modify channel mode.
<0006> gsm_04_08.c:2862 receive message MNCC_LCHAN_MODIFY
<0001> gsm_04_08.c:3048 (bts 0 trx 0 ts 2 ti 09 sub 21951) Received 'MNCC_LCHAN_MODIFY' from MNCC in state 3 (
MO_CALL_PROC)
<000a> bsc_api.c:374 Sending [[ChanModify]] for speech 33 1
<0003> gsm_04_08_utils.c:460 -> CHANNEL MODE MODIFY mode=0x21
<0006> mncc_builtin.c:143 (call 80000002) Forwarding SETUP to remote.
<0006> gsm_04_08.c:2862 receive message MNCC_SETUP_REQ
<000d> db.c:647 Found Subscriber: ID 2, IMSI 901010000001112, NAME _, TMSI 494545837, EXTEN '40000', LAC 1, AU
TH 1
<0001> transaction.c:69 subscr=0x4a54078, subscr->net=0x4368eb0
<0007> paging.c:285 Start paging of subscriber 2 on bts 0.
<0007> paging.c:285 Start paging of subscriber 2 on bts 1.
<0000> abis_rsl.c:1591 (bts=0,trx=0,ts=2,ss=0) SAPI=0 DATA INDICATION
<0003> gsm_04_08_utils.c:506 CHANNEL MODE MODIFY ACK
<0004> abis_rsl.c:1796 (bts=0,trx=0,ts=2,ss=0) IPAC_BIND speech_mode=0x11 RTP_PAYLOAD=97
<000a> osmo_msc.c:79 Assignment complete should not have been reached.
<0004> abis_rsl.c:1167 (bts=0,trx=0,ts=2,ss=0) CHANNEL MODE MODIFY ACK
<0004> abis_rsl.c:1954 (bts=0,trx=0,ts=2,ss=0) IPAC_CRCX_ACK LOCAL_IP=0.0.0.0 LOCAL_PORT=5930 CON_ID=1 <001a>
rtp_proxy.c:533 rtp_socket_create(): success
<001a> rtp_proxy.c:615 rtp_socket_bind(rs=0x4a75d48, IP=0.0.0.0): BOUND_IP=0.0.0.0, BOUND_PORT=30002
<001a> rtp_proxy.c:666 rtp_socket_connect(rs=0x4a75d48, ip=0.0.0.0, port=5930)

<0007> paging.c:81 Going to send paging commands: imsi: '901010000001112' tmsi: '0x1d7a2bad'
<0007> paging.c:81 Going to send paging commands: imsi: '901010000001112' tmsi: '0x1d7a2bad'
<0004> abis_rsl.c:1411 (bts=1,trx=0,ts=2,ss=0) Activating ARFCN(809) SS(0) lctype TCH/F r=CALL ra=0x45 ta=23
<0004> abis_rsl.c:1148 (bts=1,trx=0,ts=2,ss=0) CHANNEL ACTIVATE ACK
<0000> abis_rsl.c:1591 (bts=1,trx=0,ts=2,ss=0) SAPI=0 ESTABLISH INDICATION
<0003> gsm_04_08.c:1092 PAGING RESPONSE: mi_type=0x04 MI(494545837)
<0003> gsm_04_08.c:1110 <- Channel was requested by 901010000001112
<000d> db.c:742 Sync Equipment IMEI=6666666666666666, classmark1=33, classmark2=33 19 a2 , classmark3=a3 65 b7
 50 9f 6c 08 10
<0007> paging.c:353 Stop paging on bts 1, calling cbfn.
<0001> gsm_04_08.c:1338 Paging subscr 40000 succeeded!
<0001> gsm_04_08.c:1720 starting timer T303 with 30 seconds
<0001> gsm_04_08.c:1194 new state NULL -> CALL_PRESENT
<0001> gsm_04_08.c:110 (bts 1 trx 0 ts 2 ti 00) Sending 'SETUP' to MS.
<0007> paging.c:357 Stop paging on bts 0 silently.
<0000> abis_rsl.c:1591 (bts=1,trx=0,ts=2,ss=0) SAPI=0 DATA INDICATION
<0001> gsm_04_08.c:3141 (bts 1 trx 0 ts 2 ti 0 sub 40000) Received 'CALL_CONF' from MS in state 6 (CALL_PRESEN
T)
<0001> gsm_04_08.c:1235 stopping pending timer T303
<0001> gsm_04_08.c:1720 starting timer T310 with 180 seconds
<0001> gsm_04_08.c:1194 new state CALL_PRESENT -> MO_TERM_CALL_CONF
<0001> gsm_04_08.c:1255 (bts 1 trx 0 ts 2 ti 0 sub 40000) Sending 'MNCC_CALL_CONF_IND' to MNCC.
<0006> mncc_builtin.c:348 (call 2) Received message MNCC_CALL_CONF_IND
<0006> gsm_04_08.c:2862 receive message MNCC_LCHAN_MODIFY
```

```
<0001> gsm_04_08.c:3048 (bts 1 trx 0 ts 2 ti 00 sub 40000) Received 'MNCC_LCHAN_MODIFY' from MNCC in state 9 (
MO_TERM_CALL_CONF)
<000a> bsc_api.c:374 Sending [[ChanModify]] for speech 33 1
<0003> gsm_04_08_utils.c:460 -> CHANNEL MODE MODIFY mode=0x21
<0000> abis_rsl.c:1591 (bts=1,trx=0,ts=2,ss=0) SAPI=0 DATA INDICATION
<0003> gsm_04_08_utils.c:506 CHANNEL MODE MODIFY ACK
<0004> abis_rsl.c:1796 (bts=1,trx=0,ts=2,ss=0) IPAC_BIND speech_mode=0x11 RTP_PAYLOAD=97
<000a> osmo_msc.c:79 Assignment complete should not have been reached.
<0000> abis_rsl.c:1591 (bts=1,trx=0,ts=2,ss=0) SAPI=0 DATA INDICATION
<0001> gsm_04_08.c:3141 (bts 1 trx 0 ts 2 ti 0 sub 40000) Received 'CONNECT' from MS in state 9 (MO_TERM_CALL_
CONF)
<0001> gsm_04_08.c:1235 stopping pending timer T310
<0001> gsm_04_08.c:1194 new state MO_TERM_CALL_CONF -> CONNECT_REQUEST
<0001> gsm_04_08.c:1255 (bts 1 trx 0 ts 2 ti 0 sub 40000) Sending 'MNCC_SETUP_CNF' to MNCC.
<0006> mncc_builtin.c:348 (call 2) Received message MNCC_SETUP_CNF
<0006> mncc_builtin.c:189 (call 2) Acknowledge SETUP.
<0006> gsm_04_08.c:2862 receive message MNCC_SETUP_COMPL_REQ
<0001> gsm_04_08.c:3048 (bts 1 trx 0 ts 2 ti 00 sub 40000) Received 'MNCC_SETUP_COMPL_REQ' from MNCC in state
8 (CONNECT_REQUEST)
<0001> gsm_04_08.c:1194 new state CONNECT_REQUEST -> ACTIVE
<0001> gsm_04_08.c:110 (bts 1 trx 0 ts 2 ti 00) Sending 'CONNECT_ACK' to MS.
<0006> mncc_builtin.c:196 (call 2) Sending CONNECT to remote.
<0006> gsm_04_08.c:2862 receive message MNCC_SETUP_RSP
<0001> gsm_04_08.c:3048 (bts 0 trx 0 ts 2 ti 09 sub 21951) Received 'MNCC_SETUP_RSP' from MNCC in state 3 (MO_
CALL_PROC)
<0001> gsm_04_08.c:1720 starting timer T313 with 30 seconds
<0001> gsm_04_08.c:1194 new state MO_CALL_PROC -> CONNECT_IND
<0001> gsm_04_08.c:110 (bts 0 trx 0 ts 2 ti 90) Sending 'CONNECT' to MS.
<0006> mncc_builtin.c:202 (call 2) Bridging with remote.
<0006> gsm_04_08.c:2862 receive message MNCC_BRIDGE
<0001> gsm_04_08.c:1502 Setting up TCH map between (bts=1,trx=0,ts=2) and (bts=0,trx=0,ts=2)
==6856== Invalid read of size 2
==6856==    at 0x806536F: rsl_ipacc_mdcx_to_rtpsock (abis_rsl.c:1853)
==6856==    by 0x8080837: mncc_tx_to_cc (gsm_04_08.c:1515)
==6856==    by 0x807725A: int_mncc_recv (mncc_builtin.c:212)
==6856==    by 0x807BCBA: mncc_recvmsg (gsm_04_08.c:83)
==6856==    by 0x807CA07: gsm48_cc_rx_connect (gsm_04_08.c:2103)
==6856==    by 0x808139F: gsm0408_dispatch (gsm_04_08.c:3171)
==6856==    by 0x804F287: gsm0408_rcvmsg (bsc_api.c:623)
==6856==    by 0x80665AD: abis_rsl_rcvmsg (abis_rsl.c:1612)
==6856==    by 0x40CC89F: ipaccess_fd_cb (ipaccess.c:452)
==6856==    by 0x40AE4F1: osmo_select_main (select.c:158)
==6856==    by 0x804D3B8: main (bsc_hack.c:331)
==6856==  Address 0xa is not stack'd, malloc'd or (recently) free'd
==6856==
==6856==
==6856== Process terminating with default action of signal 11 (SIGSEGV): dumping core
==6856==  Access not within mapped region at address 0xA
==6856==    at 0x806536F: rsl_ipacc_mdcx_to_rtpsock (abis_rsl.c:1853)
==6856==    by 0x8080837: mncc_tx_to_cc (gsm_04_08.c:1515)
==6856==    by 0x807725A: int_mncc_recv (mncc_builtin.c:212)
==6856==    by 0x807BCBA: mncc_recvmsg (gsm_04_08.c:83)
==6856==    by 0x807CA07: gsm48_cc_rx_connect (gsm_04_08.c:2103)
==6856==    by 0x808139F: gsm0408_dispatch (gsm_04_08.c:3171)
==6856==    by 0x804F287: gsm0408_rcvmsg (bsc_api.c:623)
==6856==    by 0x80665AD: abis_rsl_rcvmsg (abis_rsl.c:1612)
==6856==    by 0x40CC89F: ipaccess_fd_cb (ipaccess.c:452)
==6856==    by 0x40AE4F1: osmo_select_main (select.c:158)
==6856==    by 0x804D3B8: main (bsc_hack.c:331)
```

#### #3 - 02/21/2016 04:45 PM - laforge

*- Project changed from OpenBSC to OsmoNITB*

*- Category deleted (OpenBSC)*

#### #4 - 03/17/2016 09:55 AM - laforge

*- Assignee deleted (laforge)*

#### #5 - 05/09/2016 07:37 PM - laforge

*- Priority changed from High to Low*