OsmoBSC - Bug #3976

osmo-bsc: heap-use-after-free upon MGW CRCX failure response

05/06/2019 11:03 AM - pespin

Status:	New	**Start date:**	05/06/2019
Priority:	Normal	**Due date:**	
Assignee:	neels	**% Done:**	0%
Category:	RTP/Media		
Target version:			
Spec Reference:			

Description

While testing osmux related stuff (WIP), osmo-mgw sometimes sends a 400 FAIL message (because it's WIP, I know why but it's no related to this issue).
When that happens, osmo-bsc ends up in a heap-use-after-free catched by ASan.
That happens after last patches merged in osmo-mgw/osmo-bsc related to osmo-msc handover afaik.

```
20190506125305537 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/abis_rsl.c:1130 lchan(0-0-0-CCCH_SDCCH4-0)[0x612000004720]{ESTABLISHED}: (type=SDCCH) Rx MEAS_RES
20190506125305537 DRSL <0003> /git/osmo-bsc/src/osmo-bsc/abis_rsl.c:1060 (bts=0,trx=0,ts=0,ss=0): meas_rep_count++=2 meas_rep_last_seen_nr=1
20190506125305537 DMEAS <0006> /git/osmo-bsc/src/osmo-bsc/abis_rsl.c:931 [(bts=0,trx=0,ts=0,ss=0)] MEASUREMENT RESULT NR=1 RXL-FULL-ul=-54dBm RXL-SUB-ul=-54dBm RXQ-FULL-ul=0 RXQ-SUB-ul=0 BS_POWER=0 MS_TO=0 L1_MS_PWR= 16dBm L1_FPC=0 L1_TA=0 BA1 RXL-FULL-dl=-48dBm RXL-SUB-dl=-48dBm RXQ-FULL-dl=0 RXQ-SUB-dl=0 NUM_NEIGH=0
20190506125305712 DPAG <0005> /git/osmo-bsc/src/osmo-bsc/paging.c:90 (bts=0) Going to send paging commands: imsi: 901700000015254 tmsi: 0x225bbbe1 for ch. type 0 (attempt 0)
20190506125305712 DLMI <0017> /git/libosmo-abis/src/input/ipaccess.c:356 TX 2: 0c 15 01 90 0e 04 0c 05 f4 22 5b bb e1 28 00
20190506125305964 DLMI <0017> /git/libosmo-abis/src/input/ipaccess.c:251 RX 2: 02 06 01 09 02 00
20190506125305964 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/abis_rsl.c:1603 lchan(0-0-1-TCH_F-0)[0x612000004d20]{WAIT_RLL_RTP_ESTABLISH}: (type=TCH_F) SAPI=0 ESTABLISH INDICATION
20190506125305964 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/abis_rsl.c:1636 lchan(0-0-1-TCH_F-0)[0x612000004d20]{WAIT_RLL_RTP_ESTABLISH}: Received Event LCHAN_EV_RLL_ESTABLISH_IND
20190506125305964 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/lchan_fsm.c:803 lchan(0-0-1-TCH_F-0)[0x612000004d20]{WAIT_RLL_RTP_ESTABLISH}: state_chg to ESTABLISHED
20190506125305964 DAS <0012> /git/osmo-bsc/src/osmo-bsc/lchan_fsm.c:178 assignment(conn2_0-0-1-TCH_F-0)[0x612000005da0]{WAIT_RR_ASS_COMPLETE}: Received Event ASSIGNMENT_EV_LCHAN_ESTABLISHED
20190506125305964 DAS <0012> /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:559 assignment(conn2_0-0-1-TCH_F-0)[0x612000005da0]{WAIT_RR_ASS_COMPLETE}: (bts=0,trx=0,ts=1,ss=0) lchan established, still waiting for RR Assignment Complete
20190506125306141 DLMI <0017> /git/libosmo-abis/src/input/ipaccess.c:251 RX 2: 02 06 01 09 02 00
20190506125306141 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/abis_rsl.c:1603 lchan(0-0-1-TCH_F-0)[0x612000004d20]{ESTABLISHED}: (type=TCH_F) SAPI=0 ESTABLISH INDICATION
20190506125306141 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/abis_rsl.c:1636 lchan(0-0-1-TCH_F-0)[0x612000004d20]{ESTABLISHED}: Received Event LCHAN_EV_RLL_ESTABLISH_IND
20190506125306202 DLMI <0017> /git/libosmo-abis/src/input/ipaccess.c:251 RX 2: 03 02 01 09 02 00 0b 00 03 06 29 00
20190506125306202 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/abis_rsl.c:1594 lchan(0-0-1-TCH_F-0)[0x612000004d20]{ESTABLISHED}: (type=TCH_F) SAPI=0 DATA INDICATION
20190506125306202 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/gsm_04_08_rr.c:908 lchan(0-0-1-TCH_F-0)[0x612000004d20]{ESTABLISHED}: (type=TCH_F) Rx ASSIGNMENT COMPLETE
20190506125306202 DAS <0012> /git/osmo-bsc/src/osmo-bsc/gsm_04_08_rr.c:946 assignment(conn2_0-0-1-TCH_F-0)[0x612000005da0]{WAIT_RR_ASS_COMPLETE}: Received Event ASSIGNMENT_EV_RR_ASSIGNMENT_COMPLETE
20190506125306202 DAS <0012> /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:555 assignment(conn2_0-0-1-TCH_F-0)[0x612000005da0]{WAIT_RR_ASS_COMPLETE}: state_chg to WAIT_LCHAN_ESTABLISHED
20190506125306202 DAS <0012> /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:581 assignment(conn2_0-0-1-TCH_F-0)[0x612000005da0]{WAIT_LCHAN_ESTABLISHED}: (bts=0,trx=0,ts=1,ss=0) lchan fully established, no need to wait
20190506125306202 DAS <0012> /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:603 assignment(conn2_0-0-1-TCH_F-0)[0x612000005da0]{WAIT_LCHAN_ESTABLISHED}: state_chg to WAIT_MGW_ENDPOINT_TO_MSC
20190506125306202 DAS <0012> /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:617 assignment(conn2_0-0-
```

```
1-TCH_F-0)[0x6120000005da0]{WAIT_MGW_ENDPOINT_TO_MSC}: (bts=0,trx=0,ts=1,ss=0) Connecting MGW endpo
int to the MSC's RTP port: 192.168.30.1:4010
20190506125306202 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:5
76 mgw-endpoint(conn2)[0x6120000060a0]{IN_USE}: rtpbridge/2@mgw CI[1] to-MSC: CRCX: notify=assignm
ent(conn2_0-0-1-TCH_F-0)[0x6120000005da0]
20190506125306202 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:6
23 mgw-endpoint(conn2)[0x6120000060a0]{IN_USE}: rtpbridge/2@mgw CI[1] to-MSC: CRCX 192.168.30.1:40
10: Scheduling
20190506125306202 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:6
26 mgw-endpoint(conn2)[0x6120000060a0]{IN_USE}: state_chg to WAIT_MGW_RESPONSE
20190506125306202 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:6
46 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: rtpbridge/2@mgw CI[1] to-MSC: CRCX 192.
168.30.1:4010: Sending
20190506125306202 DRLL <0000> /git/libosmocore/src/fsm.c:423 MGCP_CONN(conn2)[0x6120000063a0]{ST_C
RCX}: Allocated
20190506125306202 DRLL <0000> /git/libosmocore/src/fsm.c:453 MGCP_CONN(conn2)[0x6120000063a0]{ST_C
RCX}: is child of mgw-endpoint(conn2)[0x6120000060a0]
20190506125306203 DRLL <0000> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_fsm.c:627 MGCP_CON
N(conn2)[0x6120000063a0]{ST_CRCX}: Received Event EV_CRCX
20190506125306203 DRLL <0000> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_fsm.c:215 MGCP_CON
N(conn2)[0x6120000063a0]{ST_CRCX}: MGW/CRCX: creating connection on MGW endpoint:rtpbridge/2@mgw..
.
20190506125306203 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client.c:960 Queued 172
 bytes for MGCP GW
20190506125306203 DRLL <0000> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_fsm.c:233 MGCP_CON
N(conn2)[0x6120000063a0]{ST_CRCX}: state_chg to ST_CRCX_RESP
20190506125306203 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:7
98 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: rtpbridge/2@mgw Sent messages: 1
20190506125306203 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:7
24 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: rtpbridge/2@mgw CI[0] to-BTS CI=8894D49
1: MDCX 192.168.30.1:16384: done (rtpbridge/2@mgw:192.168.30.1:4014)
20190506125306203 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:7
22 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: rtpbridge/2@mgw CI[1] to-MSC: CRCX 192.
168.30.1:4010: waiting for response
20190506125306203 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:7
42 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: rtpbridge/2@mgw CI in use: 2, waiting f
or response: 1
20190506125306203 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client.c:724 Tx MGCP: r
=192.168.30.1:2427<->l=192.168.30.1:2727: len=172 'CRCX 3 rtpbridge/2@mgw MGCP 1.0\r\nC: 2\r\nM: '
...
20190506125306204 DRLL <0000> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_fsm.c:263 MGCP_CON
N(to-MSC)[0x6120000063a0]{ST_CRCX_RESP}: MGW/CRCX: response yields error: 400 FAIL
                <---------- HERE!!!!!!
20190506125306204 DRLL <0000> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_fsm.c:264 MGCP_CON
N(to-MSC)[0x6120000063a0]{ST_CRCX_RESP}: Terminating (cause = OSMO_FSM_TERM_ERROR)
20190506125306204 DRLL <0000> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_fsm.c:264 MGCP_CON
N(to-MSC)[0x6120000063a0]{ST_CRCX_RESP}: Removing from parent mgw-endpoint(conn2)[0x6120000060a0]
20190506125306204 DRLL <0000> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_fsm.c:264 MGCP_CON
N(to-MSC)[0x6120000063a0]{ST_CRCX_RESP}: Freeing instance
20190506125306204 DRLL <0000> /git/libosmocore/src/fsm.c:535 MGCP_CONN(to-MSC)[0x6120000063a0]{ST_
CRCX_RESP}: Deallocated
20190506125306204 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_fsm.c:264 mgw-en
dpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: Received Event MGW Response for CI #1
20190506125306204 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:7
24 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: rtpbridge/2@mgw CI[0] to-BTS CI=8894D49
1: MDCX 192.168.30.1:16384: done (rtpbridge/2@mgw:192.168.30.1:4014)
20190506125306204 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:7
42 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: rtpbridge/2@mgw CI in use: 1, waiting f
or response: 0
20190506125306204 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:7
53 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: state_chg to IN_USE
20190506125306204 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:7
24 mgw-endpoint(conn2)[0x6120000060a0]{IN_USE}: rtpbridge/2@mgw CI[0] to-BTS CI=8894D491: MDCX 192
.168.30.1:16384: done (rtpbridge/2@mgw:192.168.30.1:4014)
20190506125306204 DAS <0012> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:374
assignment(conn2_0-0-1-TCH_F-0)[0x6120000005da0]{WAIT_MGW_ENDPOINT_TO_MSC}: Received Event ASSIGNME
NT_EV_MSC_MGW_FAIL
```

```
20190506125306204 DAS <0012> /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:658 assignment(conn2_0-0-1-TCH_F-0)[0x612000005da0]{WAIT_MGW_ENDPOINT_TO_MSC}: (bts=0,trx=0,ts=1,ss=0) Assignment failed in state WAIT_MGW_ENDPOINT_TO_MSC, cause EQUIPMENT FAILURE: Unable to connect MGW endpoint to the MSC side
20190506125306204 DAS <0012> /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:658 assignment(conn2_0-0-1-TCH_F-0)[0x612000005da0]{WAIT_MGW_ENDPOINT_TO_MSC}: (bts=0,trx=0,ts=1,ss=0) incrementing rate counter: assignment:error Assigment failed for other reason.
20190506125306204 DMSC <0007> /git/osmo-bsc/src/osmo-bsc/osmo_bsc_sigtran.c:386 Tx MSC: BSSMAP: ASSIGNMENT FAIL
20190506125306204 DMSC <0007> /git/osmo-bsc/src/osmo-bsc/osmo_bsc_sigtran.c:409 Sending connection (id=2) oriented data to MSC: RI=SSN_PC,PC=0.23.1,SSN=BSSAP (00 04 03 04 01 20 )
20190506125306204 DLSCCP <0020> /git/libosmo-sccp/src/sccp_scoc.c:1711 Received SCCP User Primitive (N-DATA.request)
20190506125306204 DLSCCP <0020> /git/libosmo-sccp/src/sccp_scoc.c:1751 SCCP-SCOC(2)[0x612000005c20]{ACTIVE}: Received Event N-DATA.req
20190506125306205 DLSS7 <001f> /git/libosmo-sccp/src/sccp_scrc.c:398 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=00000004),
        PART(T=Data,L=6,D=000403040120)
20190506125306205 DLSS7 <001f> /git/libosmo-sccp/src/osmo_ss7_hmrt.c:278 m3ua_hmdc_rx_from_l2(): dpc=185=0.23.1 not local, message is for routing
20190506125306205 DLSS7 <001f> /git/libosmo-sccp/src/osmo_ss7_hmrt.c:227 Found route for dpc=185=0.23.1: pc=0=0.0.0 mask=0x0=0.0.0 via AS as-clnt-msc-0 proto=m3ua
20190506125306205 DLSS7 <001f> /git/libosmo-sccp/src/osmo_ss7_hmrt.c:233 rt->dest.as proto is M3UA for dpc=185=0.23.1
20190506125306205 DLSS7 <001f> /git/libosmo-sccp/src/m3ua.c:507 XUA_AS(as-clnt-msc-0)[0x612000003e20]{AS_ACTIVE}: Received Event AS-TRANSFER.req
20190506125306205 DAS <0012> /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:126 assignment(conn2_0-0-1-TCH_F-0)[0x612000005da0]{WAIT_MGW_ENDPOINT_TO_MSC}: (bts=0,trx=0,ts=1,ss=0) Assignment failed
20190506125306205 DAS <0012> /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:127 assignment(conn2_0-0-1-TCH_F-0)[0x612000005da0]{WAIT_MGW_ENDPOINT_TO_MSC}: Terminating (cause = OSMO_FSM_TERM_ERROR)
20190506125306205 DAS <0012> /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:127 assignment(conn2_0-0-1-TCH_F-0)[0x612000005da0]{WAIT_MGW_ENDPOINT_TO_MSC}: Removing from parent SUBSCR_CONN(conn2)[0x612000005920]
20190506125306205 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/lchan_fsm.c:1350 lchan_rtp(0-0-1-TCH_F-0)[0x612000005f20]{READY}: Received Event LCHAN_RTP_EV_ROLLBACK
20190506125306205 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/lchan_rtp_fsm.c:506 lchan_rtp(0-0-1-TCH_F-0)[0x612000005f20]{READY}: state_chg to ROLLBACK
20190506125306205 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/lchan_rtp_fsm.c:520 lchan_rtp(0-0-1-TCH_F-0)[0x612000005f20]{ROLLBACK}: Terminating (cause = OSMO_FSM_TERM_REQUEST)
20190506125306205 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/lchan_rtp_fsm.c:520 lchan_rtp(0-0-1-TCH_F-0)[0x612000005f20]{ROLLBACK}: Removing from parent lchan(0-0-1-TCH_F-0)[0x612000004d20]
20190506125306205 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:576 mgw-endpoint(conn2)[0x6120000060a0]{IN_USE}: rtpbridge/2@mgw CI[0] to-BTS CI=8894D491: DLCX: notify=NULL
20190506125306205 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:623 mgw-endpoint(conn2)[0x6120000060a0]{IN_USE}: rtpbridge/2@mgw CI[0] to-BTS CI=8894D491: DLCX: Scheduling
20190506125306205 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:626 mgw-endpoint(conn2)[0x6120000060a0]{IN_USE}: state_chg to WAIT_MGW_RESPONSE
20190506125306205 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:673 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: rtpbridge/2@mgw CI[0] to-BTS CI=8894D491: Sending MGCP: DLCX 8894D491
20190506125306205 DRLL <0000> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_fsm.c:711 MGCP_CONN(to-BTS)[0x612000006220]{ST_READY}: Received Event EV_DLCX
20190506125306206 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client.c:960 Queued 52 bytes for MGCP GW
20190506125306207 DRLL <0000> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_fsm.c:372 MGCP_CONN(to-BTS)[0x612000006220]{ST_READY}: state_chg to ST_DLCX_RESP
20190506125306207 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:798 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: rtpbridge/2@mgw Sent messages: 1
20190506125306207 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:742 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: rtpbridge/2@mgw CI in use: 0, waiting for response: 0
20190506125306207 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:747 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: Terminating (cause = OSMO_FSM_TERM_REGU
```

```
LAR)
20190506125306207 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:7
47 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: Removing from parent SUBSCR_CONN(conn2)
[0x612000005920]
20190506125306207 DLMGCP <0023> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:7
47 mgw-endpoint(conn2)[0x6120000060a0]{WAIT_MGW_RESPONSE}: Freeing instance
20190506125306207 DLMGCP <0023> /git/libosmocore/src/fsm.c:535 mgw-endpoint(conn2)[0x6120000060a0]
{WAIT_MGW_RESPONSE}: Deallocated
20190506125306207 DMSC <0007> /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:747
 SUBSCR_CONN(conn2)[0x612000005920]{ASSIGNMENT}: Received Event FORGET_MGW_ENDPOINT
20190506125306207 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/lchan_rtp_fsm.c:520 lchan_rtp(0-0-1-TCH_
F-0)[0x612000005f20]{ROLLBACK}: Freeing instance
20190506125306207 DCHAN <0010> /git/libosmocore/src/fsm.c:535 lchan_rtp(0-0-1-TCH_F-0)[0x612000005
f20]{ROLLBACK}: Deallocated
20190506125306207 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/lchan_rtp_fsm.c:520 lchan(0-0-1-TCH_F-0)
[0x612000004d20]{ESTABLISHED}: Received Event LCHAN_EV_RTP_RELEASED
20190506125306207 DRSL <0003> /git/osmo-bsc/src/osmo-bsc/abis_rsl.c:633 (bts=0,trx=0,ts=1,ss=0) DE
ACTivate SACCH CMD
20190506125306207 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/lchan_fsm.c:1361 lchan(0-0-1-TCH_F-0)[0x
612000004d20]{ESTABLISHED}: state_chg to WAIT_RF_RELEASE_ACK
20190506125306207 DCHAN <0010> /git/osmo-bsc/src/osmo-bsc/lchan_fsm.c:1406 lchan(0-0-1-TCH_F-0)[0x
612000004d20]{WAIT_RF_RELEASE_ACK}: lchan detaches from conn SUBSCR_CONN(conn2)[0x612000005920]
20190506125306207 DMSC <0007> /git/osmo-bsc/src/osmo-bsc/lchan_fsm.c:1409 SUBSCR_CONN(conn2)[0x612
000005920]{ASSIGNMENT}: lchan lchan(0-0-1-TCH_F-0)[0x612000004d20] detaches from conn
=================================================================
==24184==ERROR: AddressSanitizer: heap-use-after-free on address 0x62b000000a80 at pc 0x7ffff661b8
50 bp 0x7fffffffce40 sp 0x7fffffffce30
READ of size 8 at 0x62b000000a80 thread T0
    #0 0x7ffff661b84f in osmo_mgcpc_ep_check_ci /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_
endpoint_fsm.c:139
    #1 0x7ffff662264a in osmo_mgcpc_ep_ci_request /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_clien
t_endpoint_fsm.c:536
    #2 0x555555b33bdb in osmo_mgcpc_ep_ci_dlcx /build/new/out/include/osmocom/mgcp_client/mgcp_cli
ent_endpoint_fsm.h:37
    #3 0x555555b34484 in assignment_reset /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:107
    #4 0x555555b6dc42 in assignment_fsm_cleanup /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:761
    #5 0x7ffff62619cd in _osmo_fsm_inst_term /git/libosmocore/src/fsm.c:890
    #6 0x555555b35b44 in on_assignment_failure /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:127
    #7 0x555555b66838 in assignment_fsm_wait_mgw_endpoint_to_msc /git/osmo-bsc/src/osmo-bsc/assign
ment_fsm.c:657
    #8 0x7ffff625f2d2 in _osmo_fsm_inst_dispatch /git/libosmocore/src/fsm.c:818
    #9 0x7ffff661e85d in on_failure /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm
.c:374
    #10 0x7ffff663e5a1 in osmo_mgcpc_ep_fsm_handle_ci_events /git/osmo-mgw/src/libosmo-mgcp-client
/mgcp_client_endpoint_fsm.c:813
    #11 0x7ffff625f2d2 in _osmo_fsm_inst_dispatch /git/libosmocore/src/fsm.c:818
    #12 0x7ffff626221c in _osmo_fsm_inst_term /git/libosmocore/src/fsm.c:905
    #13 0x7ffff6614545 in mgw_crcx_resp_cb /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_fsm.c
:264
    #14 0x7ffff66058e5 in mgcp_client_handle_response /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_c
lient.c:206
    #15 0x7ffff6608d74 in mgcp_client_rx /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client.c:680
    #16 0x7ffff66092e8 in mgcp_do_read /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client.c:714
    #17 0x7ffff6262b10 in osmo_wqueue_bfd_cb /git/libosmocore/src/write_queue.c:51
    #18 0x7ffff623b883 in osmo_fd_disp_fds /git/libosmocore/src/select.c:223
    #19 0x7ffff623bba9 in osmo_select_main /git/libosmocore/src/select.c:263
    #20 0x555555d4e622 in main /git/osmo-bsc/src/osmo-bsc/osmo_bsc_main.c:932
    #21 0x7ffff546ace2 in __libc_start_main (/usr/lib/libc.so.6+0x23ce2)
    #22 0x555555ab590d in _start (/build/new/out/bin/osmo-bsc+0x56190d)

0x62b000000a80 is located 2176 bytes inside of 25216-byte region [0x62b000000200,0x62b000006480)
freed by thread T0 here:
    #0 0x7ffff72ebf89 in __interceptor_free /build/gcc/src/gcc/libsanitizer/asan/asan_malloc_linux
.cc:66
    #1 0x7ffff6142323  (/usr/lib/libtalloc.so.2+0xb323)

previously allocated by thread T0 here:
```

```
    #0 0x7ffff72ec389 in __interceptor_malloc /build/gcc/src/gcc/libsanitizer/asan/asan_malloc_lin
ux.cc:86
    #1 0x7ffff613fe11 in _talloc_zero (/usr/lib/libtalloc.so.2+0x8e11)

SUMMARY: AddressSanitizer: heap-use-after-free /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_e
ndpoint_fsm.c:139 in osmo_mgcpc_ep_check_ci
Shadow bytes around the buggy address:
  0x0c567fff8100: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff8110: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff8120: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff8130: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff8140: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c567fff8150:[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff8160: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff8170: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff8180: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff8190: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c567fff81a0: 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
  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
==24184==ABORTING

Program received signal SIGABRT, Aborted.
0x00007ffff547e82f in raise () from /usr/lib/libc.so.6
(gdb) bt full
#0  0x00007ffff547e82f in raise () from /usr/lib/libc.so.6
No symbol table info available.
#1  0x00007ffff5469672 in abort () from /usr/lib/libc.so.6
No symbol table info available.
#2  0x00007ffff730cd64 in __sanitizer::Abort () at /build/gcc/src/gcc/libsanitizer/sanitizer_commo
n/sanitizer_posix_libcdep.cc:145
No locals.
#3  0x00007ffff73159dd in __sanitizer::Die () at /build/gcc/src/gcc/libsanitizer/sanitizer_common/
sanitizer_termination.cc:57
No locals.
#4  0x00007ffff72f78fe in __asan::ScopedInErrorReport::~ScopedInErrorReport (this=<optimized out>,
 __in_chrg=<optimized out>) at /build/gcc/src/gcc/libsanitizer/asan/asan_report.cc:181
        buffer_copy = <optimized out>
#5  __asan::ReportGenericError (pc=<optimized out>, bp=bp@entry=140737488342592, sp=sp@entry=14073
7488342576, addr=108508053768832, is_write=is_write@entry=false, access_size=access_size@entry=8,
exp=0,
    fatal=true) at /build/gcc/src/gcc/libsanitizer/asan/asan_report.cc:397
        in_report = {error_report_lock_ = {<No data fields>}, static current_error_ = {kind = __as
an::kErrorKindGeneric, {Base = {scariness = {score = 51,
                descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177\0
00\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\00
0\000\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\377
\377\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q\0
05\000\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\00
0\000\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000\0
```

```
00\006\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, DeadlySignal = {<_
_asan::ErrorBase> = {scariness = {score = 51,
                descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177
\000\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\
000\000\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\3
77\377\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q
\005\000\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\
000\000\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000
\000\006\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, signal = {siginf
o = 0x2, context = 0x62b000000a80, addr = 0, pc = 0, sp = 3098476548018143233, bp = 10850805376883
2, is_memory_access = 128,
              write_flag = __sanitizer::SignalContext::UNKNOWN}}, DoubleFree = {<__asan::Error
Base> = {scariness = {score = 51,
                descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177
\000\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\
000\000\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\3
77\377\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q
\005\000\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\
000\000\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000
\000\006\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, second_free_stac
k = 0x2, addr_description = {addr = 108508053768832, alloc_tid = 0, free_tid = 0, alloc_stack_id =
 92274689, free_stack_id = 721420289,
              chunk_access = {bad_addr = 108508053768832, offset = 2176, chunk_begin = 1085080
53766656, chunk_size = 25216, access_type = 2, alloc_type = 1}}},
            NewDeleteSizeMismatch = {<__asan::ErrorBase> = {scariness = {score = 51,
                descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177
\000\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\
000\000\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\3
77\377\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q
\005\000\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\
000\000\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000
\000\006\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, free_stack = 0x2
, addr_description = {addr = 108508053768832, alloc_tid = 0, free_tid = 0, alloc_stack_id = 922746
89, free_stack_id = 721420289,
              chunk_access = {bad_addr = 108508053768832, offset = 2176, chunk_begin = 1085080
53766656, chunk_size = 25216, access_type = 2, alloc_type = 1}}, delete_size = 106790066870560},
            FreeNotMalloced = {<__asan::ErrorBase> = {scariness = {score = 51,
                descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177
\000\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\
000\000\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\3
77\377\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q
\005\000\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\
000\000\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000
\000\006\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, free_stack = 0x2
, addr_description = {data = {kind = 2688, {shadow = {addr = 0, kind = __asan::kShadowKindLow, sha
dow_byte = 0 '\000'}, heap = {addr = 0,
                    alloc_tid = 0, free_tid = 3098476548018143233, alloc_stack_id = 2688, free
_stack_id = 25264, chunk_access = {bad_addr = 2176, offset = 108508053766656, chunk_begin = 25216,
                      chunk_size = 73014429286, access_type = 0, alloc_type = 0}}, stack = {ad
dr = 0, tid = 0, offset = 3098476548018143233, frame_pc = 108508053768832, access_size = 2176,
                    frame_descr = 0x62b000000200 "\001"}, global = {addr = 0, static kMaxGloba
ls = 4, globals = {{beg = 0, size = 3098476548018143233, size_with_redzone = 108508053768832,
                        name = 0x880 <error: Cannot access memory at address 0x880>, module_na
me = 0x62b000000200 "\001", has_dynamic_init = 25216, location = 0x10ffffc666,
                        odr_indicator = 106790066870560}, {beg = 93825001346016, size = 107889
578482016, size_with_redzone = 140737488340688,
                        name = 0x10000 <error: Cannot access memory at address 0x10000>, modul
e_name = 0x555555e053e0 "ASSIGNMENT", has_dynamic_init = 1, location = 0x7fffffffc6d0,
                        odr_indicator = 140737323068233}, {beg = 140737327176224, size = 89277
66694574236160, size_with_redzone = 68719477483, name = 0x7ffff630aee0 "\003",
                        module_name = 0x7ffff48f3978 "", has_dynamic_init = 140737327185120, l
ocation = 0x1, odr_indicator = 106446469593184}, {beg = 106446469588608, size = 140737339683169,
--Type <RET> for more, q to quit, c to continue without paging--
                        size_with_redzone = 106446469593184, name = 0x7ffff6683ae0 <osmo_mgcpc
_ep_fsm> "\200\223\024\367\377\177", module_name = 0x7fffffffc750 "te-read-heap-use-after-free",
                        has_dynamic_init = 140737323082285, location = 0x2300000001, odr_indic
ator = 106790066847904}}, reg_sites = {4133788192, 32767, 0, 0}, access_size = 8589935339, size =
```

```
80 'P'},
                    addr = 0}}}}, AllocTypeMismatch = {<__asan::ErrorBase> = {scariness = {score
 = 51,
                  descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177
\000\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\
000\000\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\3
77\377\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q
\005\000\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\
000\000\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000
\000\006\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, dealloc_stack =
0x2, addr_description = {addr = 108508053768832, alloc_tid = 0, free_tid = 0, alloc_stack_id = 922
74689, free_stack_id = 721420289,
                chunk_access = {bad_addr = 108508053768832, offset = 2176, chunk_begin = 1085080
53766656, chunk_size = 25216, access_type = 2, alloc_type = 1}}, alloc_type = 22816, dealloc_type
= 24864},
            MallocUsableSizeNotOwned = {<__asan::ErrorBase> = {scariness = {score = 51,
                  descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177
\000\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\
000\000\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\3
77\377\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q
\005\000\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\
000\000\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000
\000\006\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, stack = 0x2, add
r_description = {data = {kind = 2688, {shadow = {addr = 0, kind = __asan::kShadowKindLow, shadow_b
yte = 0 '\000'}, heap = {addr = 0,
                    alloc_tid = 0, free_tid = 3098476548018143233, alloc_stack_id = 2688, free
_stack_id = 25264, chunk_access = {bad_addr = 2176, offset = 108508053766656, chunk_begin = 25216,
                      chunk_size = 73014429286, access_type = 0, alloc_type = 0}}, stack = {ad
dr = 0, tid = 0, offset = 3098476548018143233, frame_pc = 108508053768832, access_size = 2176,
                    frame_descr = 0x62b000000200 "\001"}, global = {addr = 0, static kMaxGloba
ls = 4, globals = {{beg = 0, size = 3098476548018143233, size_with_redzone = 108508053768832,
                        name = 0x880 <error: Cannot access memory at address 0x880>, module_na
me = 0x62b000000200 "\001", has_dynamic_init = 25216, location = 0x10ffffc666,
                        odr_indicator = 106790066870560}, {beg = 93825001346016, size = 107889
578482016, size_with_redzone = 140737488340688,
                        name = 0x10000 <error: Cannot access memory at address 0x10000>, modul
e_name = 0x555555e053e0 "ASSIGNMENT", has_dynamic_init = 1, location = 0x7fffffffc6d0,
                        odr_indicator = 140737323068233}, {beg = 140737327176224, size = 89277
66694574236160, size_with_redzone = 68719477483, name = 0x7ffff630aee0 "\003",
                        module_name = 0x7ffff48f3978 "", has_dynamic_init = 140737327185120, l
ocation = 0x1, odr_indicator = 106446469593184}, {beg = 106446469588608, size = 140737339683169,
                        size_with_redzone = 106446469593184, name = 0x7ffff6683ae0 <osmo_mgcpc
_ep_fsm> "\200\223\024\367\377\177", module_name = 0x7fffffffc750 "te-read-heap-use-after-free",
                        has_dynamic_init = 140737323082285, location = 0x2300000001, odr_indic
ator = 106790066847904}}, reg_sites = {4133788192, 32767, 0, 0}, access_size = 8589935339, size =
80 'P'},
                    addr = 0}}}}, SanitizerGetAllocatedSizeNotOwned = {<__asan::ErrorBase> = {sc
ariness = {score = 51,
                  descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177
\000\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\
000\000\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\3
77\377\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q
\005\000\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\
000\000\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000
\000\006\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, stack = 0x2, add
r_description = {data = {kind = 2688, {shadow = {addr = 0, kind = __asan::kShadowKindLow, shadow_b
yte = 0 '\000'}, heap = {addr = 0,
                    alloc_tid = 0, free_tid = 3098476548018143233, alloc_stack_id = 2688, free
_stack_id = 25264, chunk_access = {bad_addr = 2176, offset = 108508053766656, chunk_begin = 25216,
                      chunk_size = 73014429286, access_type = 0, alloc_type = 0}}, stack = {ad
dr = 0, tid = 0, offset = 3098476548018143233, frame_pc = 108508053768832, access_size = 2176,
                    frame_descr = 0x62b000000200 "\001"}, global = {addr = 0, static kMaxGloba
ls = 4, globals = {{beg = 0, size = 3098476548018143233, size_with_redzone = 108508053768832,
                        name = 0x880 <error: Cannot access memory at address 0x880>, module_na
me = 0x62b000000200 "\001", has_dynamic_init = 25216, location = 0x10ffffc666,
                        odr_indicator = 106790066870560}, {beg = 93825001346016, size = 107889
578482016, size_with_redzone = 140737488340688,
```

```
                            name = 0x10000 <error: Cannot access memory at address 0x10000>, modul
e_name = 0x555555e053e0 "ASSIGNMENT", has_dynamic_init = 1, location = 0x7fffffffc6d0,
                            odr_indicator = 140737323068233}, {beg = 140737327176224, size = 89277
66694574236160, size_with_redzone = 68719477483, name = 0x7ffff630aee0 "\003",
                            module_name = 0x7ffff48f3978 "", has_dynamic_init = 140737327185120, l
ocation = 0x1, odr_indicator = 106446469593184}, {beg = 106446469588608, size = 140737339683169,
                            size_with_redzone = 106446469593184, name = 0x7ffff6683ae0 <osmo_mgcpc
_ep_fsm> "\200\223\024\367\377\177", module_name = 0x7fffffffc750 "te-read-heap-use-after-free",
                            has_dynamic_init = 140737323082285, location = 0x2300000001, odr_indic
ator = 106790066847904}}, reg_sites = {4133788192, 32767, 0, 0}, access_size = 8589935339, size =
80 'P'},
                        addr = 0}}}}, StringFunctionMemoryRangesOverlap = {<__asan::ErrorBase> = {sc
ariness = {score = 51,
                      descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177
\000\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\
000\000\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\3
77\377\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q
\005\000\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\
000\000\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000
\000\006\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, stack = 0x2, len
gth1 = 108508053768832, length2 = 0, addr1_description = {data = {kind = __asan::kAddressKindWild,
 {shadow = {addr = 3098476548018143233,
                        kind = (unknown: -128), shadow_byte = 10 '\n'}, heap = {addr = 30984765480
18143233, alloc_tid = 108508053768832, free_tid = 2176, alloc_stack_id = 512, free_stack_id = 2526
4,
                        chunk_access = {bad_addr = 25216, offset = 73014429286, chunk_begin = 1067
90066870560, chunk_size = 93825001346016, access_type = 0, alloc_type = 0}}, stack = {
                        addr = 3098476548018143233, tid = 108508053768832, offset = 2176, frame_pc
 = 108508053766656, access_size = 25216, frame_descr = 0x10ffffc666 ""}, global = {
--Type <RET> for more, q to quit, c to continue without paging--
                        addr = 3098476548018143233, static kMaxGlobals = 4, globals = {{beg = 1085
08053768832, size = 2176, size_with_redzone = 108508053766656,
                            name = 0x6280 <error: Cannot access memory at address 0x6280>, module_
name = 0x10ffffc666 "", has_dynamic_init = 106790066870560, location = 0x555555e053e0,
                            odr_indicator = 107889578482016}, {beg = 140737488340688, size = 65536
, size_with_redzone = 93825001346016, name = 0x1 <error: Cannot access memory at address 0x1>,
                            module_name = 0x7fffffffc6d0 "P\307\377\377\377\177", has_dynamic_init
 = 140737323068233, location = 0x7ffff6649a20, odr_indicator = 8927766694574236160}, {beg = 687194
77483,
                            size = 140737323773664, size_with_redzone = 140737296415096, name = 0x
7ffff664bce0 "WAIT_MGW_RESPONSE", module_name = 0x1 <error: Cannot access memory at address 0x1>,
                            has_dynamic_init = 106446469593184, location = 0x60d00001e680, odr_ind
icator = 140737339683169}, {beg = 106446469593184, size = 140737327413984,
                            size_with_redzone = 140737488340816, name = 0x7ffff626222d <_osmo_fsm_
inst_term+12102> "\213@\b\205\300t8fH\215=\244\214\n", module_name = 0x2300000001 "",
                            has_dynamic_init = 106790066847904, location = 0x7ffff6649a20, odr_ind
icator = 0}}, reg_sites = {747, 2, 4133599312, 32767}, access_size = 140737488342592, size = 48 '0
'},
                      addr = 3098476548018143233}}}, addr2_description = {data = {kind = 8, {shado
w = {addr = 140737340699588, kind = __asan::kShadowKindLow, shadow_byte = 253 '\375'}, heap = {
                        addr = 140737340699588, alloc_tid = 140737488354560, free_tid = 0, alloc_s
tack_id = 0, free_stack_id = 0, chunk_access = {bad_addr = 0, offset = 0, chunk_begin = 0, chunk_s
ize = 0,
                          access_type = 0, alloc_type = 0}}, stack = {addr = 140737340699588, tid
= 140737488354560, offset = 0, frame_pc = 0, access_size = 0, frame_descr = 0x0}, global = {
                        addr = 140737340699588, static kMaxGlobals = 4, globals = {{beg = 14073748
8354560, size = 0, size_with_redzone = 0, name = 0x0, module_name = 0x0, has_dynamic_init = 0,
                            location = 0x0, odr_indicator = 0}, {beg = 0, size = 0, size_with_redz
one = 0, name = 0x0, module_name = 0x0, has_dynamic_init = 0, location = 0x0, odr_indicator = 0},
{
                            beg = 140737340571560, size = 3621364556, size_with_redzone = 14073735
0584160, name = 0x7fffffffce90 "\340d\002", module_name = 0x0, has_dynamic_init = 0, location = 0x
0,
                            odr_indicator = 0}, {beg = 1384, size = 1256, size_with_redzone = 1256
, name = 0x568 <error: Cannot access memory at address 0x568>,
                            module_name = 0x1a <error: Cannot access memory at address 0x1a>, has_
dynamic_init = 1256, location = 0x4e8, odr_indicator = 140737340922304}}, reg_sites = {4146210054,
```

```
 32767,
                          156800, 24992}, access_size = 107339822818416, size = 128 '\200'}, addr
= 140737340699588}}}, function = 0x7 <error: Cannot access memory at address 0x7>},
              StringFunctionSizeOverflow = {<__asan::ErrorBase> = {scariness = {score = 51,
                    descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177
\000\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\
000\000\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\3
77\377\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q
\005\000\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\
000\000\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000
\000\006\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, stack = 0x2, add
r_description = {data = {kind = 2688, {shadow = {addr = 0, kind = __asan::kShadowKindLow, shadow_b
yte = 0 '\000'}, heap = {addr = 0,
                      alloc_tid = 0, free_tid = 3098476548018143233, alloc_stack_id = 2688, free
_stack_id = 25264, chunk_access = {bad_addr = 2176, offset = 108508053766656, chunk_begin = 25216,
                        chunk_size = 73014429286, access_type = 0, alloc_type = 0}}, stack = {ad
dr = 0, tid = 0, offset = 3098476548018143233, frame_pc = 108508053768832, access_size = 2176,
                      frame_descr = 0x62b000000200 "\001"}, global = {addr = 0, static kMaxGloba
ls = 4, globals = {{beg = 0, size = 3098476548018143233, size_with_redzone = 108508053768832,
                        name = 0x880 <error: Cannot access memory at address 0x880>, module_na
me = 0x62b000000200 "\001", has_dynamic_init = 25216, location = 0x10ffffc666,
                        odr_indicator = 106790066870560}, {beg = 93825001346016, size = 107889
578482016, size_with_redzone = 140737488340688,
                        name = 0x10000 <error: Cannot access memory at address 0x10000>, modul
e_name = 0x555555e053e0 "ASSIGNMENT", has_dynamic_init = 1, location = 0x7fffffffc6d0,
                        odr_indicator = 140737323068233}, {beg = 140737327176224, size = 89277
66694574236160, size_with_redzone = 68719477483, name = 0x7ffff630aee0 "\003",
                        module_name = 0x7ffff48f3978 "", has_dynamic_init = 140737327185120, l
ocation = 0x1, odr_indicator = 106446469593184}, {beg = 106446469588608, size = 140737339683169,
                        size_with_redzone = 106446469593184, name = 0x7ffff6683ae0 <osmo_mgcpc
_ep_fsm> "\200\223\024\367\377\177", module_name = 0x7fffffffc750 "te-read-heap-use-after-free",
                        has_dynamic_init = 140737323082285, location = 0x2300000001, odr_indic
ator = 106790066847904}}, reg_sites = {4133788192, 32767, 0, 0}, access_size = 8589935339, size =
80 'P'},
                    addr = 0}}}, size = 140737488342592}, BadParamsToAnnotateContiguousContainer
 = {<__asan::ErrorBase> = {scariness = {score = 51,
                    descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177
\000\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\
000\000\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\3
77\377\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q
\005\000\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\
000\000\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000
\000\006\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, stack = 0x2, beg
 = 108508053768832, end = 0, old_mid = 0, new_mid = 3098476548018143233}, ODRViolation = {<__asan:
:ErrorBase> = {scariness = {score = 51,
                    descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177
\000\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\
000\000\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\3
77\377\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q
\005\000\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\
000\000\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000
\000\006\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, global1 = {beg =
 2, size = 108508053768832, size_with_redzone = 0, name = 0x0,
                  module_name = 0x2b00000105800001 <error: Cannot access memory at address 0x2b000
00105800001>, has_dynamic_init = 108508053768832, location = 0x880, odr_indicator = 10850805376665
6},
                global2 = {beg = 25216, size = 73014429286, size_with_redzone = 106790066870560, n
ame = 0x555555e053e0 "ASSIGNMENT", module_name = 0x622000001960 "\360\001",
                  has_dynamic_init = 140737488340688, location = 0x10000, odr_indicator = 93825001
346016}, stack_id1 = 1, stack_id2 = 0}, InvalidPointerPair = {<__asan::ErrorBase> = {scariness = {
                    score = 51,
                    descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177
\000\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\
000\000\005--Type <RET> for more, q to quit, c to continue without paging--
\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\377\377\377\
177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q\005\000\00
0\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\000\000\000
```

\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000\000\006\00
0\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, pc = 2, bp = 10850805376883
2, sp = 0, addr1_description = {data = {kind = __asan::kAddressKindWild, {shadow = {addr = 3098476
548018143233,
kind = (unknown: -128), shadow_byte = 10 '\n'}, heap = {addr = 30984765480
18143233, alloc_tid = 108508053768832, free_tid = 2176, alloc_stack_id = 512, free_stack_id = 2526
4,
chunk_access = {bad_addr = 25216, offset = 73014429286, chunk_begin = 1067
90066870560, chunk_size = 93825001346016, access_type = 0, alloc_type = 0}}, stack = {
addr = 3098476548018143233, tid = 108508053768832, offset = 2176, frame_pc
= 108508053766656, access_size = 25216, frame_descr = 0x10ffffc666 ""}, global = {
addr = 3098476548018143233, static kMaxGlobals = 4, globals = {{beg = 1085
08053768832, size = 2176, size_with_redzone = 108508053766656,
name = 0x6280 <error: Cannot access memory at address 0x6280>, module_
name = 0x10ffffc666 "", has_dynamic_init = 106790066870560, location = 0x555555e053e0,
odr_indicator = 107889578482016}, {beg = 140737488340688, size = 65536
, size_with_redzone = 93825001346016, name = 0x1 <error: Cannot access memory at address 0x1>,
module_name = 0x7fffffffc6d0 "P\307\377\377\377\177", has_dynamic_init
= 140737323068233, location = 0x7ffff6649a20, odr_indicator = 8927766694574236160}, {beg = 687194
77483,
size = 140737323773664, size_with_redzone = 140737296415096, name = 0x
7ffff664bce0 "WAIT_MGW_RESPONSE", module_name = 0x1 <error: Cannot access memory at address 0x1>,
has_dynamic_init = 106446469593184, location = 0x60d00001e680, odr_ind
icator = 140737339683169}, {beg = 106446469593184, size = 140737327413984,
size_with_redzone = 140737488340816, name = 0x7ffff626222d <_osmo_fsm_
inst_term+12102> "\213@\b\205\300t8fH\215=\244\214\n", module_name = 0x2300000001 "",
has_dynamic_init = 106790066847904, location = 0x7ffff6649a20, odr_ind
icator = 0}}, reg_sites = {747, 2, 4133599312, 32767}, access_size = 140737488342592, size = 48 '0
'},
addr = 3098476548018143233}}}, addr2_description = {data = {kind = 8, {shado
w = {addr = 140737340699588, kind = __asan::kShadowKindLow, shadow_byte = 253 '\375'}, heap = {
addr = 140737340699588, alloc_tid = 140737488354560, free_tid = 0, alloc_s
tack_id = 0, free_stack_id = 0, chunk_access = {bad_addr = 0, offset = 0, chunk_begin = 0, chunk_s
ize = 0,
access_type = 0, alloc_type = 0}}, stack = {addr = 140737340699588, tid
= 140737488354560, offset = 0, frame_pc = 0, access_size = 0, frame_descr = 0x0}, global = {
addr = 140737340699588, static kMaxGlobals = 4, globals = {{beg = 14073748
8354560, size = 0, size_with_redzone = 0, name = 0x0, module_name = 0x0, has_dynamic_init = 0,
location = 0x0, odr_indicator = 0}, {beg = 0, size = 0, size_with_redz
one = 0, name = 0x0, module_name = 0x0, has_dynamic_init = 0, location = 0x0, odr_indicator = 0},
{
beg = 140737340571560, size = 3621364556, size_with_redzone = 14073735
0584160, name = 0x7fffffffce90 "\340d\002", module_name = 0x0, has_dynamic_init = 0, location = 0x
0,
odr_indicator = 0}, {beg = 1384, size = 1256, size_with_redzone = 1256
, name = 0x568 <error: Cannot access memory at address 0x568>,
module_name = 0x1a <error: Cannot access memory at address 0x1a>, has_
dynamic_init = 1256, location = 0x4e8, odr_indicator = 140737340922304}}, reg_sites = {4146210054,
32767,
156800, 24992}, access_size = 107339822818416, size = 128 '\200'}, addr
= 140737340699588}}}}, Generic = {<__asan::ErrorBase> = {scariness = {score = 51,
descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177
\000\000espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\
000\000\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\3
77\377\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q
\005\000\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\
000\000\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000
\000\006\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, addr_description
= {data = {kind = __asan::kAddressKindHeap, {shadow = {addr = 108508053768832, kind = __asan::kSh
adowKindLow, shadow_byte = 0 '\000'},
heap = {addr = 108508053768832, alloc_tid = 0, free_tid = 0, alloc_stack_id
= 92274689, free_stack_id = 721420289, chunk_access = {bad_addr = 108508053768832, offset = 2176,
chunk_begin = 108508053766656, chunk_size = 25216, access_type = 2, allo
c_type = 1}}, stack = {addr = 108508053768832, tid = 0, offset = 0, frame_pc = 3098476548018143233
,
access_size = 108508053768832, frame_descr = 0x880 <error: Cannot access m
emory at address 0x880>}, global = {addr = 108508053768832, static kMaxGlobals = 4, globals = {{be

```
g = 0,
                            size = 0, size_with_redzone = 3098476548018143233, name = 0x62b000000a
80 "`\002", module_name = 0x880 <error: Cannot access memory at address 0x880>,
                            has_dynamic_init = 108508053766656, location = 0x6280, odr_indicator =
 73014429286}, {beg = 106790066870560, size = 93825001346016, size_with_redzone = 107889578482016,
                            name = 0x7fffffffc6d0 "P\307\377\377\377\177", module_name = 0x10000 <
error: Cannot access memory at address 0x10000>, has_dynamic_init = 93825001346016, location = 0x1
,
                            odr_indicator = 140737488340688}, {beg = 140737323068233, size = 14073
7327176224, size_with_redzone = 8927766694574236160, name = 0x10000002eb "",
                            module_name = 0x7ffff630aee0 "\003", has_dynamic_init = 14073729641509
6, location = 0x7ffff664bce0, odr_indicator = 1}, {beg = 106446469593184, size = 106446469588608,
                            size_with_redzone = 140737339683169, name = 0x60d00001f860 "mgw-endpoi
nt(conn2)[0x6120000060a0]", module_name = 0x7ffff6683ae0 <osmo_mgcpc_ep_fsm> "\200\223\024\367\377
\177",
                            has_dynamic_init = 140737488340816, location = 0x7ffff626222d <_osmo_f
sm_inst_term+12102>, odr_indicator = 150323855361}}, reg_sites = {160, 24864, 4133788192, 32767},
                      access_size = 0, size = 235 '\353'}, addr = 108508053768832}}}, pc = 14073
7326987344, bp = 140737488342592, sp = 140737488342576, access_size = 8,
                bug_descr = 0x7ffff732f3c4 "heap-use-after-free", is_write = false, shadow_val = 2
53 '\375'}}}, halt_on_error_ = true}
        error = {<__asan::ErrorBase> = {scariness = {score = 51,
              descr = "8-byte-read-heap-use-after-free\000\377\177\000\000\366!'\366\377\177\000\0
00espin/deR\370\377\377\377\017\000\000\220\302\377\377\377\177\000\000\000\"\251\343\343\a\000\00
0\005\000\000\000\006\000\000\000\300\304\357UUU\000\000\240p.\366\377\177\000\000\220\302\377\377
\377\177\000\000\022\022\320\\\000\000\000\000\345*\003\000\000\000\000\000\000\000\000\000Q\005\0
00\000\340\267\352UUU\000\000\001\000\000\000\020\000\000\000\240\000\000\000 a\000\000\005\000\00
0\000\327\000\000\000\327\000\000\000)\017\000\000\006\000\000\000\065\000\000\000\f\000\000\000\0
06\000\000\000\004\000\000\000w\000\000\000\001\000\000\000"...}, tid = 0}, addr_description = {da
ta = {kind = __asan::kAddressKindHeap, {shadow = {addr = 108508053768832, kind = __asan::kShadowKi
ndLow, shadow_byte = 0 '\000'}, heap = {
                  addr = 108508053768832, alloc_tid = 0, free_tid = 0, alloc_stack_id = 92274689,
free_stack_id = 721420289, chunk_access = {bad_addr = 108508053768832, offset = 2176,
                    chunk_begin = 108508053766656, chunk_size = 25216, access_type = 2, alloc_type
 = 1}}, stack = {addr = 108508053768832, tid = 0, offset = 0, frame_pc = 3098476548018143233,
--Type <RET> for more, q to quit, c to continue without paging--
                  access_size = 108508053768832, frame_descr = 0x880 <error: Cannot access memory
at address 0x880>}, global = {addr = 108508053768832, static kMaxGlobals = 4, globals = {{beg = 0,
                    size = 0, size_with_redzone = 3098476548018143233, name = 0x62b000000a80 "`\
002", module_name = 0x880 <error: Cannot access memory at address 0x880>,
                    has_dynamic_init = 108508053766656, location = 0x6280, odr_indicator = 73014
429286}, {beg = 106790066870560, size = 93825001346016, size_with_redzone = 107889578482016,
                    name = 0x7fffffffc6d0 "P\307\377\377\377\177", module_name = 0x10000 <error:
 Cannot access memory at address 0x10000>, has_dynamic_init = 93825001346016, location = 0x1,
                    odr_indicator = 140737488340688}, {beg = 140737323068233, size = 14073732717
6224, size_with_redzone = 8927766694574236160, name = 0x10000002eb "", module_name = 0x7ffff630aee
0 "\003",
                    has_dynamic_init = 140737296415096, location = 0x7ffff664bce0, odr_indicator
 = 1}, {beg = 106446469593184, size = 106446469588608, size_with_redzone = 140737339683169,
                    name = 0x60d00001f860 "mgw-endpoint(conn2)[0x6120000060a0]", module_name = 0
x7ffff6683ae0 <osmo_mgcpc_ep_fsm> "\200\223\024\367\377\177", has_dynamic_init = 140737488340816,
                    location = 0x7ffff626222d <_osmo_fsm_inst_term+12102>, odr_indicator = 15032
3855361}}, reg_sites = {160, 24864, 4133788192, 32767}, access_size = 0, size = 235 '\353'},
                addr = 108508053768832}}}, pc = 140737326987344, bp = 140737488342592, sp = 140737
488342576, access_size = 8, bug_descr = 0x7ffff732f3c4 "heap-use-after-free", is_write = false,
          shadow_val = 253 '\375'}
#6  0x00007ffff72f841c in __asan::__asan_report_load8 (addr=<optimized out>) at /build/gcc/src/gcc
/libsanitizer/asan/asan_rtl.cc:112
        bp = 140737488342592
        pc = <optimized out>
        local_stack = 140737488345168
        sp = 140737488342576
#7  0x00007ffff661b850 in osmo_mgcpc_ep_check_ci (ci=0x62b000000a80) at /git/osmo-mgw/src/libosmo-
mgcp-client/mgcp_client_endpoint_fsm.c:139
No locals.
#8  0x00007ffff662264b in osmo_mgcpc_ep_ci_request (ci=0x62b000000a80, verb=MGCP_VERB_DLCX, verb_i
nfo=0x0, notify=0x0, event_success=0, event_failure=0, notify_data=0x0)
```

```
    at /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:536
        ep = 0x0
        fi = 0x0
        cleared_ci = {ep = 0x7fffffffd300, occupied = 84,
          label = "\372\377\377\377\017\000\000\240\322\377\377\377\177\000\000 \360\352UUU\000\00
0 \323\377\377\377\177\000\000\240\000\000\000 a\000\000 \323\377\377\377\177\000\000_-'\366\377\1
77\000\000\320\322\377\377\377\177\000\000\200", mgcp_client_fi = 0x7ffff62df2e0, pending = false,
 sent = false, verb = 520, verb_info = {addr = " \036\354UUU\000\000\001\000\000\000\020\000\000",
 port = 0,
            endpoint = "\000\000\000\000\000\000\300\373\066\366\377\177\000\000\240\000\000\000 a
\000\000\300\373\066\366\377\177\000\000\263\212\265A\000\000\000\000\200t.\366\377\177\000\000:)'
\366\377\177\000\000\300\373\066\366\377\177\000\000\060\000\000\000\060\000\000\000\270\324\377\3
77\377\177\000\000\300\323\377\377\377\177\000\000\200t.\366\377\177\000\000:)'\366\377\177\000\00
0\000\000\000\000\b\002\000\000\060\000\000\000\060\000\000\000\000\"\251\343\201\314\345{`\323\37
7\377\377\177\000\0001\372\377\377\377\017\000\000`\323\377\377\377\177\000\000\000\"\251\343\201\
314\345{\220\324\377\377\377\177\000\000\300\323\377\377\377\177\000\000 \324\377\377\377\177\000\
000x\372\377\377\377\017\000\000\300\323\377\377\377\177\000\000\340\365"..., call_id = 32767, pti
me = 3819512320, codecs = {2078657665,
              4129763189, 32767, 1, CODEC_PCMU_8000_1, 128, 24704, 32, 24704, CODEC_PCMU_8000_1},
codecs_len = 0, ptmap = {{codec = 787758704, pt = 0}, {codec = 1256, pt = 0}, {codec = 4128504658,
                pt = 32767}, {codec = 1160, pt = 0}, {codec = 3819512320, pt = 2078657665}, {codec
 = 4294956336, pt = 32767}, {codec = 1160, pt = 0}, {codec = CODEC_PCMU_8000_1, pt = 0}, {codec =
1,
                pt = 0}, {codec = CODEC_PCMU_8000_1, pt = 0}}, ptmap_len = 194016, x_osmo_ign = 24
784, x_osmo_osmux_use = 96, x_osmo_osmux_cid = 32767, conn_mode = 281992, param_present = 224, par
am = {
              amr_octet_aligned_present = 96, amr_octet_aligned = false}}, notify = 0x61a0000264e0
, notify_success = 158432, notify_failure = 24992, notify_data = 0x7fffffffd550, got_port_info = 3
8,
          rtp_info = {addr = "\377\177\000\000\210M\004\000\340`\000\000\000\"\251", <incomplete s
equence \343>, port = 52353,
            endpoint = "\345{\000\000\000\000\000\000\000\000@\001\000\000\000\000\000\000\001\000
\000\000\000\000\000\020\327\377\377\377\177\000\000\300\325\377\377\377\177\000\000\364x\t\367\37
7\177\000\000\320\325\377\377\377\177\000\000\340j\002\000\240a\000\000\002\000\000\000\000\000\00
0\000\000`M\004\000\340`\000\000\200\312\000\000\340b\000\000\340\357\024\367\377\177\000\000\340\
325\377\377\377\177\000\000`M\004\000\340`\000\000\340\325\377\377\377\177\000\000\027y\t\367\377\
177\000\000@\001\000\000\000\000\000\000\340j\002\000\240a\000\000 \326\377\377\377\177\000\000G\3
41\257UUU\000\000\263\212\265A\000\000\000\000x\236\t\362\377\177\000\000\340j\002\000\240a\000\00
0\350k\002\000\240a\000\000\001\000\000\000\000\000\000\000"..., call_id = 4294956960, ptime = 327
67, codecs = {4130024341, 32767,
              CODEC_PCMU_8000_1, CODEC_PCMU_8000_1, 3819512320, 2078657665, 1, CODEC_PCMU_8000_1,
CODEC_PCMU_8000_1, CODEC_PCMU_8000_1}, codecs_len = 1440616128, ptmap = {{codec = 21845, pt = 1},
{
                codec = CODEC_PCMU_8000_1, pt = 129952}, {codec = 24784, pt = 124544}, {codec = 24
784, pt = 4294957040}, {codec = 32767, pt = 4129676564}, {codec = 32767, pt = 1361}, {
                codec = CODEC_PCMU_8000_1, pt = 5}, {codec = CODEC_PCMU_8000_1, pt = 0}, {codec =
3111, pt = 1447134624}, {codec = 1361, pt = 1441445856}}, ptmap_len = 21845, x_osmo_ign = 2,
            x_osmo_osmux_use = false, x_osmo_osmux_cid = 3111, conn_mode = 8, param_present = 32,
param = {amr_octet_aligned_present = 77, amr_octet_aligned = false}},
          mgcp_ci_str = " a\000\000P\330\377\377\377\177\000\000}7+\366\377\177\000\000\340\267\35
2UUU\000\000\005\000\000\000"}
#9  0x0000555555b33bdc in osmo_mgcpc_ep_ci_dlcx (ci=0x62b000000a80) at /build/new/out/include/osmo
com/mgcp_client/mgcp_client_endpoint_fsm.h:37
No locals.
#10 0x0000555555b34485 in assignment_reset (conn=0x622000001960) at /git/osmo-bsc/src/osmo-bsc/ass
ignment_fsm.c:107
No locals.
--Type <RET> for more, q to quit, c to continue without paging--
#11 0x0000555555b6dc43 in assignment_fsm_cleanup (fi=0x612000005da0, cause=OSMO_FSM_TERM_ERROR) at
 /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:761
        conn = 0x622000001960
#12 0x00007ffff62619ce in _osmo_fsm_inst_term (fi=0x612000005da0, cause=OSMO_FSM_TERM_ERROR, data=
0x0, file=0x555555ddeba0 "/git/osmo-bsc/src/osmo-bsc/assignment_fsm.c", line=127)
    at /git/libosmocore/src/fsm.c:890
        parent = 0x612000005920
        parent_term_event = 6
#13 0x0000555555b35b45 in on_assignment_failure (conn=0x622000001960) at /git/osmo-bsc/src/osmo-bs
```

```
c/assignment_fsm.c:127
        resp = 0x61a000025ee0
#14 0x0000555555b66839 in assignment_fsm_wait_mgw_endpoint_to_msc (fi=0x612000005da0, event=4, dat
a=0x0) at /git/osmo-bsc/src/osmo-bsc/assignment_fsm.c:657
        _conn = 0x622000001960
        conn = 0x622000001960
#15 0x00007ffff625f2d3 in _osmo_fsm_inst_dispatch (fi=0x612000005da0, event=4, data=0x0, file=0x7f
fff6649a20 "/git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c",
    line=374) at /git/libosmocore/src/fsm.c:818
        fsm = 0x555556059460 <assignment_fsm>
        fs = 0x555555f4fe98 <assignment_fsm_states+120>
#16 0x00007ffff661e85e in on_failure (ci=0x62b000000a80) at /git/osmo-mgw/src/libosmo-mgcp-client/
mgcp_client_endpoint_fsm.c:374
        notify = 0x612000005da0
        notify_failure = 4
        notify_data = 0x0
#17 0x00007ffff663e5a2 in osmo_mgcpc_ep_fsm_handle_ci_events (fi=0x6120000060a0, event=3, data=0x0
) at /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_endpoint_fsm.c:813
        ci = 0x62b000000a80
        ep = 0x62b000000260
#18 0x00007ffff625f2d3 in _osmo_fsm_inst_dispatch (fi=0x6120000060a0, event=3, data=0x0, file=0x7f
fff66462c0 "/git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_fsm.c", line=264)
    at /git/libosmocore/src/fsm.c:818
        fsm = 0x7ffff6683ae0 <osmo_mgcpc_ep_fsm>
        fs = 0x7ffff6657ce8 <osmo_mgcpc_ep_fsm_states+40>
#19 0x00007ffff626221d in _osmo_fsm_inst_term (fi=0x6120000063a0, cause=OSMO_FSM_TERM_ERROR, data=
0x0,
    file=0x7ffff66462c0 "/git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client_fsm.c", line=264) at /g
it/libosmocore/src/fsm.c:905
        parent = 0x6120000060a0
        parent_term_event = 3
#20 0x00007ffff6614546 in mgw_crcx_resp_cb (r=0x619000006ee0, priv=0x6120000063a0) at /git/osmo-mg
w/src/libosmo-mgcp-client/mgcp_client_fsm.c:264
        fi = 0x6120000063a0
        mgcp_ctx = 0x61b00005b0e0
        rc = 24960
#21 0x00007ffff66058e6 in mgcp_client_handle_response (mgcp=0x618000002ce0, pending=0x60d00001fe10
, response=0x619000006ee0)
    at /git/osmo-mgw/src/libosmo-mgcp-client/mgcp_client.c:206
No locals.
#22 0x00007ffff6608d75 in mgcp_client_rx (mgcp=0x618000002ce0, msg=0x62100000a160) at /git/osmo-mg
w/src/libosmo-mgcp-client/mgcp_client.c:680
        r = 0x619000006ee0
        pending = 0x60d00001fe10
        rc = 0
#23 0x00007ffff66092e9 in mgcp_do_read (fd=0x618000002f08) at /git/osmo-mgw/src/libosmo-mgcp-clien
t/mgcp_client.c:714
        mgcp = 0x618000002ce0
        msg = 0x62100000a160
        ret = 12
#24 0x00007ffff6262b11 in osmo_wqueue_bfd_cb (fd=0x618000002f08, what=1) at /git/libosmocore/src/w
rite_queue.c:51
--Type <RET> for more, q to quit, c to continue without paging--
        queue = 0x618000002f08
        rc = 0
#25 0x00007ffff623b884 in osmo_fd_disp_fds (_rset=0x7fffffffdf50, _wset=0x7fffffffdff0, _eset=0x7f
ffffffe090) at /git/libosmocore/src/select.c:223
        flags = 1
        ufd = 0x618000002f08
        tmp = 0x613000008060
        work = 1
        readset = 0x7fffffffdf50
        writeset = 0x7fffffffdff0
        exceptset = 0x7fffffffe090
#26 0x00007ffff623bbaa in osmo_select_main (polling=0) at /git/libosmocore/src/select.c:263
        readset = {__fds_bits = {0 <repeats 16 times>}}
        writeset = {__fds_bits = {0 <repeats 16 times>}}
```

```
        exceptset = {__fds_bits = {0 <repeats 16 times>}}
        rc = 1
        no_time = {tv_sec = 0, tv_usec = 0}
#27 0x0000555555d4e623 in main (argc=4, argv=0x7fffffffe2c8) at /git/osmo-bsc/src/osmo-bsc/osmo_bs
c_main.c:932
        msc = 0x60f000000198
        data = 0x60f000000190
        rc = 0
(gdb)
```