OsmocomBB - Bug #3629

mobile aborting after 'test re-selection 1' on vty

10/04/2018 02:55 PM - roh

Status:	New	**Start date:**	10/04/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:			
Target version:			
Resolution:		**Spec Reference:**	

Description

```
.....
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI c7dc0057 (not for us)
<000b> gsm48_rr.c:2308  TMSI dec9307f (not for us)
<000b> gsm48_rr.c:2319  TMSI 4f4f724b (not for us)
<000b> gsm48_rr.c:2330  TMSI cfbd1151 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI d6b320fb (not for us)
<000b> gsm48_rr.c:2308  TMSI f6beb2a8 (not for us)
<000b> gsm48_rr.c:2319  TMSI f9b722ca (not for us)
<000b> gsm48_rr.c:2330  TMSI e5b4e117 (not for us)
<000b> gsm48_rr.c:2149 PAGING REQUEST 1
<000b> gsm48_rr.c:2107  TMSI e6c15278 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI ebd3408d (not for us)
<000b> gsm48_rr.c:2308  TMSI ebb808ae (not for us)
<000b> gsm48_rr.c:2319  TMSI edc3e833 (not for us)
<000b> gsm48_rr.c:2330  TMSI dbb040f6 (not for us)
<000b> gsm48_rr.c:2204 PAGING REQUEST 2
<000b> gsm48_rr.c:2227  TMSI d8af781a (not for us)
<000b> gsm48_rr.c:2238  TMSI f1da701a (not for us)
<000b> gsm48_rr.c:2116  IMSI 262011406448616 (not for us)
<000b> gsm48_rr.c:2204 PAGING REQUEST 2
<000b> gsm48_rr.c:2227  TMSI e7dd9110 (not for us)
<000b> gsm48_rr.c:2238  TMSI cdb343e1 (not for us)
<000b> gsm48_rr.c:2107  TMSI f4d568f9 (not for us)
<0001> gsm48_rr.c:2425 IMMEDIATE ASSIGNMENT:
<0001> gsm48_rr.c:2448  (ta 1/553m ra 0x7d chan_nr 0x0e ARFCN 56 TS 6 SS 0 TSC 4)
<0001> gsm48_rr.c:2453 Not for us, no request.
<0001> gsm48_rr.c:665 MON: f=56 lev=-73 snr= 0 ber= 30 LAI=262 01 1406 ID=ddc8
<0001> gsm48_rr.c:2425 IMMEDIATE ASSIGNMENT:
<0001> gsm48_rr.c:2448  (ta 1/553m ra 0x7d chan_nr 0x0e ARFCN 56 TS 6 SS 0 TSC 4)
<0001> gsm48_rr.c:2453 Not for us, no request.
<0001> gsm48_rr.c:2425 IMMEDIATE ASSIGNMENT:
<0001> gsm48_rr.c:2448  (ta 1/553m ra 0x7d chan_nr 0x0e ARFCN 56 TS 6 SS 0 TSC 4)
<0001> gsm48_rr.c:2453 Not for us, no request.
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI 5056eff9 (not for us)
<000b> gsm48_rr.c:2308  TMSI f8d5f816 (not for us)
<000b> gsm48_rr.c:2319  TMSI c2a970b3 (not for us)
<000b> gsm48_rr.c:2330  TMSI fac7a0f9 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI c3b16112 (not for us)
<000b> gsm48_rr.c:2308  TMSI ceb8b000 (not for us)
<000b> gsm48_rr.c:2319  TMSI c0ce7a11 (not for us)
<000b> gsm48_rr.c:2330  TMSI 725305e3 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI e6bb843b (not for us)
<000b> gsm48_rr.c:2308  TMSI e6c628f6 (not for us)
<000b> gsm48_rr.c:2319  TMSI e5cfc012 (not for us)
<000b> gsm48_rr.c:2330  TMSI e9ce71e8 (not for us)
```

```
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI d5d67042 (not for us)
<000b> gsm48_rr.c:2308  TMSI d0dd710e (not for us)
<000b> gsm48_rr.c:2319  TMSI e6d90165 (not for us)
<000b> gsm48_rr.c:2330  TMSI e6a93071 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI cbd3083e (not for us)
<000b> gsm48_rr.c:2308  TMSI fdabc8c5 (not for us)
<000b> gsm48_rr.c:2319  TMSI f6bed0db (not for us)
<000b> gsm48_rr.c:2330  TMSI e7d8488d (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI d2ad8024 (not for us)
<000b> gsm48_rr.c:2308  TMSI ccb198f7 (not for us)
<000b> gsm48_rr.c:2319  TMSI c4b4ebe1 (not for us)
<000b> gsm48_rr.c:2330  TMSI c2b94054 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI c1bbd866 (not for us)
<000b> gsm48_rr.c:2308  TMSI 4f4f724b (not for us)
<000b> gsm48_rr.c:2319  TMSI fbb3286a (not for us)
<000b> gsm48_rr.c:2330  TMSI e1cc5089 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI c3cd801d (not for us)
<000b> gsm48_rr.c:2308  TMSI 89586d39 (not for us)
<000b> gsm48_rr.c:2319  TMSI e7bf1a63 (not for us)
<000b> gsm48_rr.c:2330  TMSI c6b6c808 (not for us)
<000b> gsm48_rr.c:2149 PAGING REQUEST 1
<000b> gsm48_rr.c:2107  TMSI e6c15278 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI ecaea29d (not for us)
<000b> gsm48_rr.c:2308  TMSI ebd3408d (not for us)
<000b> gsm48_rr.c:2319  TMSI dbb040f6 (not for us)
<000b> gsm48_rr.c:2330  TMSI d2aabb7c (not for us)
<000b> gsm48_rr.c:2204 PAGING REQUEST 2
<000b> gsm48_rr.c:2227  TMSI d8d02804 (not for us)
<000b> gsm48_rr.c:2238  TMSI c9d9b800 (not for us)
<000b> gsm48_rr.c:2116  IMSI 262011406448616 (not for us)
<000b> gsm48_rr.c:2149 PAGING REQUEST 1
<000b> gsm48_rr.c:2116  IMSI 262017246007073 (not for us)
<000b> gsm48_rr.c:2107  TMSI daad40ee (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI e5afc3d4 (not for us)
<000b> gsm48_rr.c:2308  TMSI f8bc0825 (not for us)
<000b> gsm48_rr.c:2319  TMSI cdb343e1 (not for us)
<000b> gsm48_rr.c:2330  TMSI e7dd9110 (not for us)
<000b> gsm48_rr.c:2204 PAGING REQUEST 2
<000b> gsm48_rr.c:2227  TMSI e9b0f8e6 (not for us)
<000b> gsm48_rr.c:2238  TMSI d1c39191 (not for us)
<000b> gsm48_rr.c:2107  TMSI f6b43002 (not for us)
<000b> gsm48_rr.c:2149 PAGING REQUEST 1
<000b> gsm48_rr.c:2107  TMSI f9bf40dc (not for us)
<000b> gsm48_rr.c:2204 PAGING REQUEST 2
<000b> gsm48_rr.c:2227  TMSI eab2c809 (not for us)
<000b> gsm48_rr.c:2238  TMSI e3acba24 (not for us)
<000b> gsm48_rr.c:2107  TMSI ddb7407a (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI e4cf59b1 (not for us)
<000b> gsm48_rr.c:2308  TMSI ecce49a9 (not for us)
<000b> gsm48_rr.c:2319  TMSI 5056eff9 (not for us)
<000b> gsm48_rr.c:2330  TMSI 5056eff9 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI 1545f55c (not for us)
<000b> gsm48_rr.c:2308  TMSI 115eecc4 (not for us)
<000b> gsm48_rr.c:2319  TMSI 15635214 (not for us)
<000b> gsm48_rr.c:2330  TMSI f3bd1031 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI d3bd7963 (not for us)
<000b> gsm48_rr.c:2308  TMSI f0cd3163 (not for us)
```

```
<000b> gsm48_rr.c:2319  TMSI ffc5f136 (not for us)
<000b> gsm48_rr.c:2330  TMSI ded22813 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI c8ac4103 (not for us)
<000b> gsm48_rr.c:2308  TMSI d5bec118 (not for us)
<000b> gsm48_rr.c:2319  TMSI d5d67042 (not for us)
<000b> gsm48_rr.c:2330  TMSI d0dd710e (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI cfcdd9b1 (not for us)
<000b> gsm48_rr.c:2308  TMSI d4d33909 (not for us)
<000b> gsm48_rr.c:2319  TMSI cbd3083e (not for us)
<000b> gsm48_rr.c:2330  TMSI fdabc8c5 (not for us)
<000b> gsm48_rr.c:2204 PAGING REQUEST 2
<000b> gsm48_rr.c:2227  TMSI ead6a05d (not for us)
<000b> gsm48_rr.c:2238  TMSI c8d788b6 (not for us)
<000b> gsm48_rr.c:2116  IMSI 262011402065931 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI caad3023 (not for us)
<000b> gsm48_rr.c:2308  TMSI c7dc0057 (not for us)
<000b> gsm48_rr.c:2319  TMSI dec9307f (not for us)
<000b> gsm48_rr.c:2330  TMSI c1bbd866 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI c3cd801d (not for us)
<000b> gsm48_rr.c:2308  TMSI 89586d39 (not for us)
<000b> gsm48_rr.c:2319  TMSI e7bf1a63 (not for us)
<000b> gsm48_rr.c:2330  TMSI c6b6c808 (not for us)
<000b> gsm48_rr.c:2273 PAGING REQUEST 3
<000b> gsm48_rr.c:2297  TMSI ecaea29d (not for us)
<000b> gsm48_rr.c:2308  TMSI d2aabb7c (not for us)
<000b> gsm48_rr.c:2319  TMSI c3bed234 (not for us)
<000b> gsm48_rr.c:2330  TMSI e3b858ab (not for us)
<0003> gsm322.c:479 Sync to ARFCN=79 rxlev=-64 (No sysinfo yet, ccch mode NONE)
<0003> gsm322.c:2952 Channel synched. (ARFCN=79, snr=16, BSIC=57)
<0001> gsm322.c:2973 using DSC of 90
<0003> gsm322.c:703 Starting CS timer with 2 seconds.
<0003> gsm48_rr.c:4815 Channel provides data.
<0001> sysinfo.c:705 New SYSTEM INFORMATION 3 (mcc 262 mnc 01 lac 0x1406)
<0001> gsm48_rr.c:1907 Changing CCCH_MODE to 1
<0003> gsm322.c:713 stopping pending CS timer.
<0003> gsm322.c:2579 Relevant sysinfo of neighbour cell is now received or updated.
<0003> gsm322.c:479 Sync to ARFCN=58 rxlev=-96 (No sysinfo yet, ccch mode NONE)
<0003> gsm322.c:2952 Channel synched. (ARFCN=58, snr=5, BSIC=23)
<0001> gsm322.c:2973 using DSC of 90
<0003> gsm322.c:703 Starting CS timer with 2 seconds.
<0003> gsm48_rr.c:4815 Channel provides data.
<0001> gsm48_rr.c:1940 New SYSTEM INFORMATION 4 (mcc 262 mnc 01 lac 0x1406)
<0003> gsm322.c:713 stopping pending CS timer.
<0003> gsm322.c:2579 Relevant sysinfo of neighbour cell is now received or updated.
<0003> gsm322.c:479 Sync to ARFCN=72 rxlev=-102 (No sysinfo yet, ccch mode NONE)
<000c> l1ctl.c:99 FBSB RESP: result=255
<0003> gsm322.c:2995 Channel sync error, try again
<0003> gsm322.c:479 Sync to ARFCN=72 rxlev=-102 (No sysinfo yet, ccch mode NONE)
<000c> l1ctl.c:99 FBSB RESP: result=255
<0003> gsm322.c:3008 Channel sync error.
<0003> gsm322.c:3013 free sysinfo ARFCN=72
<0003> gsm322.c:509 Unselecting serving cell.
=================================================================
==837==ERROR: AddressSanitizer: heap-use-after-free on address 0x61b00009aee6 at pc 0x5592b66d6dd5
 bp 0x7fffe10e39c0 sp 0x7fffe10e39b8
WRITE of size 1 at 0x61b00009aee6 thread T0
    #0 0x5592b66d6dd4 in gsm322_unselect_cell /home/osmocom-build/jenkins/workspace/osmo-gsm-teste
r_build-osmocom-bb/osmocom-bb/src/host/layer23/src/mobile/gsm322.c:513
    #1 0x5592b66e7163 in gsm322_nb_trigger_event /home/osmocom-build/jenkins/workspace/osmo-gsm-te
ster_build-osmocom-bb/osmocom-bb/src/host/layer23/src/mobile/gsm322.c:4625
    #2 0x5592b66eac52 in gsm322_nb_synced /home/osmocom-build/jenkins/workspace/osmo-gsm-tester_bu
ild-osmocom-bb/osmocom-bb/src/host/layer23/src/mobile/gsm322.c:4670
    #3 0x5592b66f84f9 in gsm322_l1_signal /home/osmocom-build/jenkins/workspace/osmo-gsm-tester_bu
```

```
ild-osmocom-bb/osmocom-bb/src/host/layer23/src/mobile/gsm322.c:3030
    #4 0x7fde91715563 in osmo_signal_dispatch (/usr/lib/x86_64-linux-gnu/libosmocore.so.11+0xa563)
    #5 0x5592b67bf6dc in rx_l1_fbsb_conf /home/osmocom-build/jenkins/workspace/osmo-gsm-tester_bui
ld-osmocom-bb/osmocom-bb/src/host/layer23/src/common/l1ctl.c:102
    #6 0x5592b67bf6dc in l1ctl_recv /home/osmocom-build/jenkins/workspace/osmo-gsm-tester_build-os
mocom-bb/osmocom-bb/src/host/layer23/src/common/l1ctl.c:906
    #7 0x5592b67c3901 in layer2_read /home/osmocom-build/jenkins/workspace/osmo-gsm-tester_build-o
smocom-bb/osmocom-bb/src/host/layer23/src/common/l1l2_interface.c:85
    #8 0x7fde91719332 in osmo_wqueue_bfd_cb (/usr/lib/x86_64-linux-gnu/libosmocore.so.11+0xe332)
    #9 0x7fde91715151 in osmo_select_main (/usr/lib/x86_64-linux-gnu/libosmocore.so.11+0xa151)
    #10 0x5592b66d26b6 in main /home/osmocom-build/jenkins/workspace/osmo-gsm-tester_build-osmocom
-bb/osmocom-bb/src/host/layer23/src/mobile/main.c:277
    #11 0x7fde8fdd62e0 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x202e0)
    #12 0x5592b66d2f59 in _start (/root/osmocom-bb/bin/mobile+0x1adf59)

0x61b00009aee6 is located 102 bytes inside of 1548-byte region [0x61b00009ae80,0x61b00009b48c)
freed by thread T0 here:
    #0 0x7fde91c08a10 in free (/usr/lib/x86_64-linux-gnu/libasan.so.3+0xc1a10)
    #1 0x7fde9193786a in _talloc_free (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x486a)

previously allocated by thread T0 here:
    #0 0x7fde91c08d28 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.3+0xc1d28)
    #1 0x7fde91939acd in _talloc_zero (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x6acd)

SUMMARY: AddressSanitizer: heap-use-after-free /home/osmocom-build/jenkins/workspace/osmo-gsm-test
er_build-osmocom-bb/osmocom-bb/src/host/layer23/src/mobile/gsm322.c:513 in gsm322_unselect_cell
Shadow bytes around the buggy address:
  0x0c368000b580: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c368000b590: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c368000b5a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c368000b5b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c368000b5c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c368000b5d0: fd fd fd fd fd fd fd fd fd fd fd fd[fd]fd fd fd
  0x0c368000b5e0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c368000b5f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c368000b600: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c368000b610: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c368000b620: 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
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==837==ABORTING
```

build used: https://jenkins.osmocom.org/jenkins/view/osmo-gsm-tester/job/osmo-gsm-tester_build-osmocom-bb/427/

History

#1 - 10/04/2018 02:58 PM - roh

things i forgot to add:

device used: C118 with kevins power-board modified for high-side power switching

mobile.cfg: copy from examples

L1:

```
./sbin/osmocon -p /dev/ttyUSB0 -m c123xor opt/osmocom-bb/target/firmware/board/compal_e88/layer1.compalram.bin
```