# OsmocomBB - Bug #2690

## ASAN issue on shutdown/no shutdown SYSINFO access

11/29/2017 09:33 AM - zecke

| | | | |
|---|---|---|---|
| **Status:** | New | **Start date:** | 11/29/2017 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | | **% Done:** | 0% |
| **Category:** | | | |
| **Target version:** | | | |
| **Resolution:** | | **Spec Reference:** | |

**Description**

Hard to reproduce (only happens once). Using a script to issue "shutdown/no shutdown" with a timer...

```
<0002> gsm322.c:5123 exit PLMN process
<0003> gsm322.c:5124 exit Cell Selection process
<0003> gsm322.c:834 new state 'C3 camped normally' -> 'C0 null'
<0003> gsm322.c:5138 free sysinfo ARFCN=514(DCS)
<0003> gsm322.c:5169 Write stored BA list (mcc=000 mnc=000  Marshall Islands, 000)
<0005> gsm48_mm.c:1342 exit Mobility Management process
<0005> gsm48_mm.c:487 stopping pending (periodic loc. upd. delay) timer T3212
<0001> gsm48_rr.c:5515 exit Radio Ressource process
<0001> gsm48_rr.c:822 stopping pending timer T_meas
<0006> gsm48_cc.c:74 exit Call Control processes for 1
<0007> gsm480_ss.c:240 exit SS processes for 1
<001a> gsm411_sms.c:73 exit SMS processes for 1
<000f> sim.c:1243 exit SIM client
<0013> @foo.lua:37 MS shutdown    0    ->    2
<0011> app_mobile.c:179 Power off! (MS 1)
<0013> @foo.lua:95 END    0
<0013> @foo.lua:98 After timeout2!!!
<0013> @foo.lua:99 000000000000000
<0012> primitives.c:90 Creating timer with reference: 18446744072442999032
=================================================================
==26249==ERROR: AddressSanitizer: heap-use-after-free on address 0xb2807f2d at pc 0xb7ab6429 bp 0x
bfffe9a8 sp 0xbfffe580
READ of size 23 at 0xb2807f2d thread T0
    #0 0xb7ab6428 in __interceptor_memcmp (/usr/lib/i386-linux-gnu/libasan.so.3+0x8f428)
    #1 0x8006ea61 in gsm48_rr_rx_sysinfo4 /media/sf_source/gsm/osmocom-bb/src/host/layer23/src/mob
ile/gsm48_rr.c:1931
    #2 0x8006ed2b in gsm48_rr_rx_bcch /media/sf_source/gsm/osmocom-bb/src/host/layer23/src/mobile/
gsm48_rr.c:4707
    #3 0x80085f79 in gsm48_rr_unit_data_ind /media/sf_source/gsm/osmocom-bb/src/host/layer23/src/m
obile/gsm48_rr.c:4841
    #4 0x80068c76 in gsm48_rcv_rll /media/sf_source/gsm/osmocom-bb/src/host/layer23/src/mobile/gsm
48_rr.c:5319
    #5 0x800862df in gsm48_rcv_rsl /media/sf_source/gsm/osmocom-bb/src/host/layer23/src/mobile/gsm
48_rr.c:5376
    #6 0x80086363 in gsm48_rsl_dequeue /media/sf_source/gsm/osmocom-bb/src/host/layer23/src/mobile
/gsm48_rr.c:563
    #7 0x80023def in mobile_work /media/sf_source/gsm/osmocom-bb/src/host/layer23/src/mobile/app_m
obile.c:68
    #8 0x80024136 in l23_app_work /media/sf_source/gsm/osmocom-bb/src/host/layer23/src/mobile/app_
mobile.c:389
    #9 0x80023c1e in main /media/sf_source/gsm/osmocom-bb/src/host/layer23/src/mobile/main.c:283
    #10 0xb777b275 in __libc_start_main (/lib/i386-linux-gnu/libc.so.6+0x18275)
    #11 0x80023130  (/media/sf_source/gsm/osmocom-bb/src/host/layer23/src/mobile/mobile+0x23130)

0xb2807f2d is located 173 bytes inside of 1500-byte region [0xb2807e80,0xb280845c)
freed by thread T0 here:
    #0 0xb7ae4e5c in free (/usr/lib/i386-linux-gnu/libasan.so.3+0xbde5c)
    #1 0xb7a15e72 in _talloc_free (/usr/lib/i386-linux-gnu/libtalloc.so.2+0x3e72)
```

```
previously allocated by thread T0 here:
    #0 0xb7ae5194 in malloc (/usr/lib/i386-linux-gnu/libasan.so.3+0xbe194)
    #1 0xb7a18276 in _talloc_zero (/usr/lib/i386-linux-gnu/libtalloc.so.2+0x6276)

SUMMARY: AddressSanitizer: heap-use-after-free (/usr/lib/i386-linux-gnu/libasan.so.3+0x8f428) in _
_interceptor_memcmp
Shadow bytes around the buggy address:
  0x36500f90: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x36500fa0: fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa fa
  0x36500fb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x36500fc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x36500fd0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x36500fe0: fd fd fd fd fd[fd]fd fd fd fd fd fd fd fd fd fd
  0x36500ff0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x36501000: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x36501010: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x36501020: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x36501030: 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
==26249==ABORTING
```