OsmoMSC - Bug #3053

sanitizer issue uncovered by msc_vlr_test_gsm_ciph on gcc (Debian 7.2.0-18) 7.2.0

03/10/2018 04:21 AM - neels

Status:	Resolved	**Start date:**	03/10/2018
Priority:	High	**Due date:**	
Assignee:	neels	**% Done:**	100%
Category:			
Target version:			
Resolution:			

Description

Build with --enable-sanitize on a debian 9, and you'll get

```
- needs ciph, not yet accepted
msc_subscr_conn_is_accepted() == false
  requests shall be thwarted
DRLL Dispatching 04.08 message GSM48_MT_CC_SETUP (0x3:0x5)
DRLL subscr IMSI:901700000004620: Message not permitted for initial conn: GSM48_MT_CC_SETUP
DRLL Dispatching 04.08 message unknown 0x33 (0x5:0x33)
DRLL subscr IMSI:901700000004620: Message not permitted for initial conn: unknown 0x33
DRLL Dispatching 04.08 message GSM48_MT_RR_SYSINFO_1 (0x6:0x19)
DRLL subscr IMSI:901700000004620: Message not permitted for initial conn: GSM48_MT_RR_SYSINFO_1
DRLL Dispatching 04.08 message SMS:0x01 (0x9:0x1)
DRLL subscr IMSI:901700000004620: Message not permitted for initial conn: SMS:0x01
  lu_result_sent == 0
DREF VLR subscr IMSI:901700000004620 usage increases to: 2
  vsub->imeisv[0] == 0
DREF VLR subscr IMSI:901700000004620 usage decreases to: 1
- MS sends Ciphering Mode Complete with IMEISV, VLR accepts and sends GSUP LU Req to HLR
  MSC <--RAN_GERAN_A-- MS: GSM48_MT_RR_CIPH_M_COMPL
DRR IMSI:901700000004620: CIPHERING MODE COMPLETE
DVLR vlr_lu_fsm(901700000004620){VLR_ULA_S_WAIT_CIPH}: Received Event VLR_ULA_E_CIPH_RES
=================================================================
==9522==ERROR: AddressSanitizer: stack-use-after-scope on address 0x7ffcc6a2a1c0 at pc 0x7f0d2aa85
203 bp 0x7ffcc6a28550 sp 0x7ffcc6a27d00
READ of size 18 at 0x7ffcc6a2a1c0 thread T0
    #0 0x7f0d2aa85202  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x71202)
    #1 0x7f0d2aaf7d07  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xe3d07)
    #2 0x7f0d2aa8538b  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x7138b)
    #3 0x7f0d2aab1015 in vsnprintf (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x9d015)
    #4 0x7f0d29f3416f in _output ../../../src/libosmocore/src/logging.c:424
    #5 0x7f0d29f345e2 in osmo_vlogp ../../../src/libosmocore/src/logging.c:525
    #6 0x7f0d29f34707 in logp2 ../../../src/libosmocore/src/logging.c:558
    #7 0x55bdaa0ead54 in lu_fsm_wait_ciph ../../../../src/osmo-msc/src/libvlr/vlr_lu_fsm.c:1155
    #8 0x7f0d29f312de in _osmo_fsm_inst_dispatch ../../../src/libosmocore/src/fsm.c:509
    #9 0x55bdaa0d71e6 in vlr_subscr_rx_ciph_res ../../../../src/osmo-msc/src/libvlr/vlr.c:1097
    #10 0x55bdaa0a1216 in msc_cipher_mode_compl ../../../../src/osmo-msc/src/libmsc/osmo_msc.c:199
    #11 0x55bdaa05976f in rx_from_ms ../../../../src/osmo-msc/tests/msc_vlr/msc_vlr_tests.c:230
    #12 0x55bdaa059a11 in ms_sends_msg ../../../../src/osmo-msc/tests/msc_vlr/msc_vlr_tests.c:245
    #13 0x55bdaa03639b in test_ciph_imeisv ../../../../src/osmo-msc/tests/msc_vlr/msc_vlr_test_gsm
_ciph.c:641
    #14 0x55bdaa0574f4 in run_tests ../../../../src/osmo-msc/tests/msc_vlr/msc_vlr_tests.c:865
    #15 0x55bdaa02e9b1 in main ../../../../src/osmo-msc/tests/msc_vlr/msc_vlr_tests.c:925
    #16 0x7f0d28097560 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x20560)
    #17 0x55bdaa02f2b9 in _start (/n/s/dev/make/osmo-msc/tests/msc_vlr/msc_vlr_test_gsm_ciph+0x10a
2b9)

Address 0x7ffcc6a2a1c0 is located in stack of thread T0 at offset 96 in frame
    #0 0x55bdaa0a0f1f in msc_cipher_mode_compl ../../../../src/osmo-msc/src/libmsc/osmo_msc.c:157

  This frame has 3 object(s):
```

```
    [32, 48) 'ciph_res'
    [96, 128) 'imeisv' <== Memory access at offset 96 is inside this variable
    [160, 4256) 'tp'
HINT: this may be a false positive if your program uses some custom stack unwind mechanism or swap
context
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-use-after-scope (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x71202)
Shadow bytes around the buggy address:
  0x100018d3d3e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100018d3d3f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100018d3d400: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100018d3d410: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100018d3d420: 00 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1
=>0x100018d3d430: 00 00 f2 f2 f2 f2 f2 f2[f8]f8 f8 f8 f2 f2 f2 f2
  0x100018d3d440: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8
  0x100018d3d450: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8
  0x100018d3d460: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8
  0x100018d3d470: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8
  0x100018d3d480: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8
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
==9522==ABORTING
```

History

#1 - 03/13/2018 12:29 AM - neels

- Status changed from New to In Progress

- % Done changed from 0 to 90

https://gerrit.osmocom.org/7264

#2 - 03/28/2018 01:35 PM - neels

- Status changed from In Progress to Resolved

- % Done changed from 90 to 100

merged two weeks ago