OpenBSC - Bug #4094

multiple crashes due to connection failures / drops

07/09/2019 07:39 PM - Hoernchen

Status:	Closed	**Start date:**	07/09/2019
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:			
Target version:			
Resolution:		**Spec Reference:**	

Description

osmo-bsc offers some new and exciting crashes when interfering with rsl/oml connections, they all appear to be related to improper removal of old links from linked lists after a line was e1inp_line_put().

Related issues:

Related to OsmoBTS - Bug #3612: osmo-bts-trx: heap-use-after-free in e1inp_si...	**Resolved**	**10/02/2018**
Related to OsmoBTS - Bug #4709: osmo-bts-trx (latest version 1.2.1) crashes i...	**Resolved**	**08/13/2020**

History

#1 - 07/09/2019 07:39 PM - Hoernchen

The first free happens within the same call of ipaccess_sign_link_down as the second erroneous free.

```
<0015> input/ipa.c:270 0.0.0.0:3002 accept()ed new link from 127.0.0.1:39984
<0015> ipa.c:481 Cannot send ID_ACK message. Reason: Broken pipe
<0015> input/ipaccess.c:154 Unexpected return from ipa_ccm_rcvmsg_base (ret=-32)
<0015> input/ipaccess.c:440 failed to send A-bis IPA signalling message. Reason: Broken pipe
<0015> input/ipaccess.c:87 Forcing socket shutdown with no signal link set
<0015> bts_ipaccess_nanobts.c:416 (bts=0) Dropping OML link: link down
<0015> bts_ipaccess_nanobts.c:397 (bts=0,trx=0) Dropping RSL link: OML link drop
=================================================================
==22092==ERROR: AddressSanitizer: heap-use-after-free on address 0x62e00000caa8 at pc 0x7ffff592a5cd bp 0x7fff
ffffd510 sp 0x7fffffffd500
WRITE of size 8 at 0x62e00000caa8 thread T0
    #0 0x7ffff592a5cc in __llist_del /usr/local/include/osmocom/core/linuxlist.h:117
    #1 0x7ffff592a6e3 in llist_del /usr/local/include/osmocom/core/linuxlist.h:129
    #2 0x7ffff592def4 in e1inp_sign_link_destroy /home/phi/sysmo/lime/libosmo-abis/src/e1_input.c:551
    #3 0x5555559cdb82 in ipaccess_drop_rsl /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/bts_ipaccess_nanobts.c:3
98
    #4 0x5555559cdfda in ipaccess_drop_oml /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/bts_ipaccess_nanobts.c:4
23
    #5 0x5555559d0bf5 in ipaccess_sign_link_down /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/bts_ipaccess_nanob
ts.c:612
    #6 0x7ffff5947329 in ipaccess_drop input/ipaccess.c:98
    #7 0x7ffff594af22 in __handle_ts1_write input/ipaccess.c:457
    #8 0x7ffff594aff9 in handle_ts1_write input/ipaccess.c:466
    #9 0x7ffff594b106 in ipaccess_fd_cb input/ipaccess.c:484
    #10 0x7ffff5c86658 in osmo_fd_disp_fds /home/phi/sysmo/lime/libosmocore/src/select.c:223
    #11 0x7ffff5c86959 in osmo_select_main /home/phi/sysmo/lime/libosmocore/src/select.c:263
    #12 0x555555ae65d4 in main /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/osmo_bsc_main.c:932
    #13 0x7ffff413bb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #14 0x5555558e7109 in _start (/usr/local/bin/osmo-bsc+0x393109)

0x62e00000caa8 is located 1704 bytes inside of 48080-byte region [0x62e00000c400,0x62e000017fd0)
freed by thread T0 here:
    #0 0x7ffff6ef87b8 in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xde7b8)
    #1 0x7ffff67e114f in _talloc_free (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x7b14f)
    #2 0x7ffff592d7c1 in e1inp_line_put /home/phi/sysmo/lime/libosmo-abis/src/e1_input.c:448
    #3 0x7ffff592e2f4 in e1inp_sign_link_destroy /home/phi/sysmo/lime/libosmo-abis/src/e1_input.c:563
    #4 0x5555559cde54 in ipaccess_drop_oml /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/bts_ipaccess_nanobts.c:4
17
    #5 0x5555559d0bf5 in ipaccess_sign_link_down /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/bts_ipaccess_nanob
ts.c:612
    #6 0x7ffff5947329 in ipaccess_drop input/ipaccess.c:98
```

```
    #7 0x7ffff594af22 in __handle_ts1_write input/ipaccess.c:457
    #8 0x7ffff594aff9 in handle_ts1_write input/ipaccess.c:466
    #9 0x7ffff594b106 in ipaccess_fd_cb input/ipaccess.c:484
    #10 0x7ffff5c86658 in osmo_fd_disp_fds /home/phi/sysmo/lime/libosmocore/src/select.c:223
    #11 0x7ffff5c86959 in osmo_select_main /home/phi/sysmo/lime/libosmocore/src/select.c:263
    #12 0x555555ae65d4 in main /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/osmo_bsc_main.c:932
    #13 0x7ffff413bb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)

previously allocated by thread T0 here:
    #0 0x7ffff6ef8b50 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb50)
    #1 0x7ffff67f38f5 in _talloc_zero (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x8d8f5)
    #2 0x7ffff592cec2 in e1inp_line_clone /home/phi/sysmo/lime/libosmo-abis/src/e1_input.c:392
    #3 0x7ffff594bc8d in ipaccess_bsc_oml_cb input/ipaccess.c:569
    #4 0x7ffff59425ab in ipa_server_fd_cb input/ipa.c:272
    #5 0x7ffff5c86658 in osmo_fd_disp_fds /home/phi/sysmo/lime/libosmocore/src/select.c:223
    #6 0x7ffff5c86959 in osmo_select_main /home/phi/sysmo/lime/libosmocore/src/select.c:263
    #7 0x555555ae65d4 in main /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/osmo_bsc_main.c:932
    #8 0x7ffff413bb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)

SUMMARY: AddressSanitizer: heap-use-after-free /usr/local/include/osmocom/core/linuxlist.h:117 in __llist_del
Shadow bytes around the buggy address:
  0x0c5c7fff9900: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7fff9910: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7fff9920: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7fff9930: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7fff9940: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c5c7fff9950: fd fd fd fd fd[fd]fd fd fd fd fd fd fd fd fd fd
  0x0c5c7fff9960: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7fff9970: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7fff9980: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7fff9990: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7fff99a0: 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
==22092==ABORTING
```

#2 - 07/09/2019 07:40 PM - Hoernchen

```
<0004> abis_nm.c:472 BTS0 reported variant: omso-bts-trx
<0004> abis_nm.c:494 BTS0 Attribute Manufacturer Dependent State is unreported
<0004> abis_nm.c:560 OC=BASEBAND-TRANSCEIVER(04) INST=(00,00,ff): BTS0: ARI reported sw[0/1]: TRX_PHY_VERSION
is Unknown
<0004> abis_nm.c:2884 (bts=0,trx=0) IPA RSL CONNECT IP=0.0.0.0 PORT=3003 STREAM=0x00
<0015> input/ipa.c:270 0.0.0.0:3003 accept()ed new link from 127.0.0.1:59734
<0003> osmo_bsc_main.c:285 bootstrapping RSL for BTS/TRX (0/0) on ARFCN 871 using MCC-MNC 001-01 LAC=1 CID=0 B
SIC=63
<0000> chan_alloc.c:128 (bts=0) bogus channel load sample (used=0 / total=0)
<0015> input/ipa.c:270 0.0.0.0:3002 accept()ed new link from 127.0.0.1:40070
<0015> ipa.c:481 Cannot send ID_ACK message. Reason: Broken pipe
<0015> input/ipaccess.c:154 Unexpected return from ipa_ccm_rcvmsg_base (ret=-32)
<0015> input/ipaccess.c:87 Forcing socket shutdown with no signal link set
<0015> bts_ipaccess_nanobts.c:416 (bts=0) Dropping OML link: link down
<0015> bts_ipaccess_nanobts.c:397 (bts=0,trx=0) Dropping RSL link: OML link drop
=================================================================
==23613==ERROR: AddressSanitizer: heap-use-after-free on address 0x62e00003caa8 at pc 0x7ffff592a5cd bp 0x7fff
ffffd460 sp 0x7fffffffd450
WRITE of size 8 at 0x62e00003caa8 thread T0
```

```
    #0 0x7ffff592a5cc in __llist_del /usr/local/include/osmocom/core/linuxlist.h:117
    #1 0x7ffff592a6e3 in llist_del /usr/local/include/osmocom/core/linuxlist.h:129
    #2 0x7ffff592def4 in e1inp_sign_link_destroy /home/phi/sysmo/lime/libosmo-abis/src/e1_input.c:551
    #3 0x5555559cdb82 in ipaccess_drop_rsl /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/bts_ipaccess_nanobts.c:3
98
    #4 0x5555559cdfda in ipaccess_drop_oml /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/bts_ipaccess_nanobts.c:4
23
    #5 0x5555559d0bf5 in ipaccess_sign_link_down /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/bts_ipaccess_nanob
ts.c:612
    #6 0x7ffff5947329 in ipaccess_drop input/ipaccess.c:98
    #7 0x7ffff5947581 in ipa_bsc_keepalive_timeout_cb input/ipaccess.c:116
    #8 0x7ffff5945f95 in ipa_ka_fsm_timer_cb input/ipa_keepalive.c:162
    #9 0x7ffff5c9ac05 in fsm_tmr_cb /home/phi/sysmo/lime/libosmocore/src/fsm.c:287
    #10 0x7ffff5c83c30 in osmo_timers_update /home/phi/sysmo/lime/libosmocore/src/timer.c:257
    #11 0x7ffff5c86939 in osmo_select_main /home/phi/sysmo/lime/libosmocore/src/select.c:260
    #12 0x555555ae65d4 in main /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/osmo_bsc_main.c:932
    #13 0x7ffff413bb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #14 0x5555558e7109 in _start (/usr/local/bin/osmo-bsc+0x393109)

0x62e00003caa8 is located 1704 bytes inside of 48080-byte region [0x62e00003c400,0x62e000047fd0)
freed by thread T0 here:
    #0 0x7ffff6ef87b8 in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xde7b8)
    #1 0x7ffff67e114f in _talloc_free (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x7b14f)
    #2 0x7ffff592d7c1 in e1inp_line_put /home/phi/sysmo/lime/libosmo-abis/src/e1_input.c:448
    #3 0x7ffff592e2f4 in e1inp_sign_link_destroy /home/phi/sysmo/lime/libosmo-abis/src/e1_input.c:563
    #4 0x5555559cde54 in ipaccess_drop_oml /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/bts_ipaccess_nanobts.c:4
17
    #5 0x5555559d0bf5 in ipaccess_sign_link_down /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/bts_ipaccess_nanob
ts.c:612
    #6 0x7ffff5947329 in ipaccess_drop input/ipaccess.c:98
    #7 0x7ffff5947581 in ipa_bsc_keepalive_timeout_cb input/ipaccess.c:116
    #8 0x7ffff5945f95 in ipa_ka_fsm_timer_cb input/ipa_keepalive.c:162
    #9 0x7ffff5c9ac05 in fsm_tmr_cb /home/phi/sysmo/lime/libosmocore/src/fsm.c:287
    #10 0x7ffff5c83c30 in osmo_timers_update /home/phi/sysmo/lime/libosmocore/src/timer.c:257
    #11 0x7ffff5c86939 in osmo_select_main /home/phi/sysmo/lime/libosmocore/src/select.c:260
    #12 0x555555ae65d4 in main /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/osmo_bsc_main.c:932
    #13 0x7ffff413bb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)

previously allocated by thread T0 here:
    #0 0x7ffff6ef8b50 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb50)
    #1 0x7ffff67f38f5 in _talloc_zero (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x8d8f5)
    #2 0x7ffff592cec2 in e1inp_line_clone /home/phi/sysmo/lime/libosmo-abis/src/e1_input.c:392
    #3 0x7ffff594bc8d in ipaccess_bsc_oml_cb input/ipaccess.c:569
    #4 0x7ffff59425ab in ipa_server_fd_cb input/ipa.c:272
    #5 0x7ffff5c86658 in osmo_fd_disp_fds /home/phi/sysmo/lime/libosmocore/src/select.c:223
    #6 0x7ffff5c86959 in osmo_select_main /home/phi/sysmo/lime/libosmocore/src/select.c:263
    #7 0x555555ae65d4 in main /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/osmo_bsc_main.c:932
    #8 0x7ffff413bb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)

SUMMARY: AddressSanitizer: heap-use-after-free /usr/local/include/osmocom/core/linuxlist.h:117 in __llist_del
Shadow bytes around the buggy address:
  0x0c5c7ffff900: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7ffff910: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7ffff920: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7ffff930: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7ffff940: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c5c7ffff950: fd fd fd fd fd[fd]fd fd fd fd fd fd fd fd fd fd
  0x0c5c7ffff960: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7ffff970: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7ffff980: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7ffff990: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7ffff9a0: 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
==23613==ABORTING
```

#3 - 07/09/2019 07:41 PM - Hoernchen

This one is different, ipaccess_sign_link_up instead of ipaccess_sign_link_down, dropping the "old" oml link fails.

```
0015> input/ipa.c:270 0.0.0.0:3002 accept()ed new link from 127.0.0.1:40312
<0007> a_reset.c:106 A-RESET(msc-0)[0x612000004720]{DISC}: (re)sending BSSMAP RESET message...
<0007> osmo_bsc_sigtran.c:101 Sending RESET to MSC: RI=SSN_PC,PC=0.23.1,SSN=BSSAP
<001f> m3ua.c:507 XUA_AS(as-clnt-msc-0)[0x612000003fa0]{AS_INACTIVE}: Event AS-TRANSFER.req not permitted
<0015> input/ipa.c:270 0.0.0.0:3002 accept()ed new link from 127.0.0.1:40314
<0015> ipa.c:481 Cannot send ID_ACK message. Reason: Broken pipe
<0015> input/ipaccess.c:158 Unexpected return from ipa_ccm_rcvmsg_base (ret=-32)
<0007> a_reset.c:106 A-RESET(msc-0)[0x612000004720]{DISC}: (re)sending BSSMAP RESET message...
<0007> osmo_bsc_sigtran.c:101 Sending RESET to MSC: RI=SSN_PC,PC=0.23.1,SSN=BSSAP
<001f> m3ua.c:507 XUA_AS(as-clnt-msc-0)[0x612000003fa0]{AS_INACTIVE}: Event AS-TRANSFER.req not permitted
<0015> bts_ipaccess_nanobts.c:416 (bts=0) Dropping OML link: new OML link
=================================================================
==28715==ERROR: AddressSanitizer: heap-use-after-free on address 0x62e00000c4d0 at pc 0x7ffff592a64d bp 0x7fff
ffffc3a0 sp 0x7fffffffc390
WRITE of size 8 at 0x62e00000c4d0 thread T0
    #0 0x7ffff592a64c in __llist_del /usr/local/include/osmocom/core/linuxlist.h:117
    #1 0x7ffff592a763 in llist_del /usr/local/include/osmocom/core/linuxlist.h:129
    #2 0x7ffff592df74 in e1inp_sign_link_destroy /home/phi/sysmo/lime/libosmo-abis/src/e1_input.c:551
    #3 0x5555559cde54 in ipaccess_drop_oml /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/bts_ipaccess_nanobts.c:4
17
    #4 0x5555559cf465 in ipaccess_sign_link_up /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/bts_ipaccess_nanobts
.c:540
    #5 0x7ffff59481d7 in ipaccess_rcvmsg input/ipaccess.c:197
    #6 0x7ffff59499ac in handle_ts1_read input/ipaccess.c:325
    #7 0x7ffff594b1d5 in ipaccess_fd_cb input/ipaccess.c:486
    #8 0x7ffff5c86658 in osmo_fd_disp_fds /home/phi/sysmo/lime/libosmocore/src/select.c:223
    #9 0x7ffff5c86959 in osmo_select_main /home/phi/sysmo/lime/libosmocore/src/select.c:263
    #10 0x555555ae65d4 in main /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/osmo_bsc_main.c:932
    #11 0x7ffff413bb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #12 0x5555558e7109 in _start (/usr/local/bin/osmo-bsc+0x393109)

0x62e00000c4d0 is located 208 bytes inside of 48080-byte region [0x62e00000c400,0x62e000017fd0)
freed by thread T0 here:
    #0 0x7ffff6ef87b8 in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xde7b8)
    #1 0x7ffff67e114f in _talloc_free (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x7b14f)
    #2 0x7ffff592d841 in e1inp_line_put /home/phi/sysmo/lime/libosmo-abis/src/e1_input.c:448 <----------------
-------------------------
    #3 0x7ffff5949259 in ipaccess_rcvmsg input/ipaccess.c:287
    #4 0x7ffff59499ac in handle_ts1_read input/ipaccess.c:325
    #5 0x7ffff594b1d5 in ipaccess_fd_cb input/ipaccess.c:486
    #6 0x7ffff5c86658 in osmo_fd_disp_fds /home/phi/sysmo/lime/libosmocore/src/select.c:223
    #7 0x7ffff5c86959 in osmo_select_main /home/phi/sysmo/lime/libosmocore/src/select.c:263
    #8 0x555555ae65d4 in main /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/osmo_bsc_main.c:932
    #9 0x7ffff413bb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)

previously allocated by thread T0 here:
    #0 0x7ffff6ef8b50 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb50)
    #1 0x7ffff67f38f5 in _talloc_zero (/usr/lib/x86_64-linux-gnu/libtalloc.so.2+0x8d8f5)
    #2 0x7ffff592cf42 in e1inp_line_clone /home/phi/sysmo/lime/libosmo-abis/src/e1_input.c:392
    #3 0x7ffff594bd7b in ipaccess_bsc_oml_cb input/ipaccess.c:573
    #4 0x7ffff594262b in ipa_server_fd_cb input/ipa.c:272
    #5 0x7ffff5c86658 in osmo_fd_disp_fds /home/phi/sysmo/lime/libosmocore/src/select.c:223
    #6 0x7ffff5c86959 in osmo_select_main /home/phi/sysmo/lime/libosmocore/src/select.c:263
    #7 0x555555ae65d4 in main /home/phi/sysmo/lime/osmo-bsc/src/osmo-bsc/osmo_bsc_main.c:932
    #8 0x7ffff413bb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)

SUMMARY: AddressSanitizer: heap-use-after-free /usr/local/include/osmocom/core/linuxlist.h:117 in __llist_del
Shadow bytes around the buggy address:
  0x0c5c7fff9840: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5c7fff9850: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5c7fff9860: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
  0x0c5c7fff9870: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c5c7fff9880: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c5c7fff9890: fd fd fd fd fd fd fd fd fd[fd]fd fd fd fd fd
  0x0c5c7fff98a0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7fff98b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7fff98c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7fff98d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c5c7fff98e0: 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
==28715==ABORTING
```

#4 - 07/09/2019 07:45 PM - Hoernchen

- Related to Bug #3612: osmo-bts-trx: heap-use-after-free in e1inp_sign_link_destroy added

#5 - 06/08/2020 06:42 PM - pespin

- Status changed from New to Closed

Fixed by:
https://gerrit.osmocom.org/c/libosmo-abis/+/18730 e1_input: refcount inc line during e1_sign_link_create, not during line update

Since this ticket is a duplicate of an older one (#3612), I'm closing this one and keeping the other open until fix is merged.

#6 - 08/13/2020 07:52 AM - laforge

- Related to Bug #4709: osmo-bts-trx (latest version 1.2.1) crashes in ttcn3-bts-test-latest added