libosmocore - Bug #4646

SEGV when bringing up Nokia InSite

07/04/2020 08:17 AM - laforge

Status:	Resolved	**Start date:**	07/04/2020
Priority:	Low	**Due date:**	
Assignee:	laforge	**% Done:**	100%
Category:	libosmogsm		
Target version:			
Spec Reference:			

Description

This is with "OpenBSC version 1.3.2.3-e811" and current libosmocore/libosmo-abis

```
root@sysmo-e1-tracer:~/git/openbsc/openbsc/src/osmo-nitb# LD_PRELOAD=/usr/lib/x86_64-linux-gnu/lib
asan.so.5  ./osmo-nitb -c ./openbsc-insite.cfg
<001e> telnet_interface.c:104 Available via telnet 127.0.0.1 4242
<001f> input/lapd.c:251 (0:1-T1-S62): LAPD Allocating SAP for SAPI=62 / TEI=1 (dl=0x615000001500,
sap=0x6150000014e0)
<001f> input/lapd.c:261 (0:1-T1-S62): k=1 N200=3 N201=260 T200=1.0 T203=10.0
<001f> input/lapd.c:524 (0:1-T1-S62): LAPD DL-ESTABLISH request TEI=1 SAPI=62
<0025> control_if.c:911 CTRL at 127.0.0.1 4249
DB: Database initialized.
DB: Database prepared.
<001f> input/lapd.c:660 ((0:1-T1-S62)) LAPD DL-ESTABLISH confirm TEI=1 SAPI=62
<0005> bts_nokia_site.c:56 bootstrapping OML for BTS 0
Getting attributes from BTS0 type nokia_site is not supported.
Getting attributes from BTS0 type nokia_site is not supported.
<0005> bts_nokia_site.c:1677 ABIS_OM_MDISC_FOM
<0005> bts_nokia_site.c:1505 (0x81) NOKIA_BTS_ACK
<0005> bts_nokia_site.c:1537 ACK = 1
<001f> input/lapd.c:551 (0:1-T1-S62): LAPD DL-RELEASE request TEI=1 SAPI=62
<001f> input/lapd.c:664 ((0:1-T1-S62)) LAPD DL-RELEASE confirm TEI=1 SAPI=62
<001f> input/lapd.c:289 (0:1-T1-S62): LAPD Freeing SAP for SAPI=62 / TEI=1 (dl=0x615000001500, sap
=0x6150000014e0)
AddressSanitizer:DEADLYSIGNAL
=================================================================
==28749==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000010 (pc 0x7f399d918633 bp 0x6
1600000b1e0 sp 0x7ffe298a0580 T0)
==28749==The signal is caused by a READ memory access.
==28749==Hint: address points to the zero page.
    #0 0x7f399d918632 in lapd_send_i src/gsm/lapd_core.c:1797
    #1 0x7f399d91b167 in lapd_rx_i src/gsm/lapd_core.c:1601
    #2 0x7f399d91b167 in lapd_ph_data_ind src/gsm/lapd_core.c:1642
    #3 0x7f399d7c787e in lapd_receive input/lapd.c:501
    #4 0x7f399d79a167 in e1inp_rx_ts_lapd /root/git/libosmo-abis/src/e1_input.c:708
    #5 0x7f399d7efd1f in handle_ts1_read input/dahdi.c:194
    #6 0x7f399d7efd1f in dahdi_fd_cb input/dahdi.c:484
    #7 0x7f399d8c54f3 in osmo_fd_disp_fds src/select.c:227
    #8 0x7f399d8c54f3 in _osmo_select_main src/select.c:265
    #9 0x7f399d8c5c05 in osmo_select_main src/select.c:274
    #10 0x563d2ab5335b in main /root/git/openbsc/openbsc/src/osmo-nitb/bsc_hack.c:400
    #11 0x7f399d32a09a in __libc_start_main ../csu/libc-start.c:308
    #12 0x563d2ab535d9 in _start (/root/git/openbsc/openbsc/src/osmo-nitb/osmo-nitb+0x125d9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV src/gsm/lapd_core.c:1797 in lapd_send_i
==28749==ABORTING
```

Related issues:

Related to libosmocore - Bug #1982: LAPD: segfault in lapd_est_req function	**Resolved**	**03/14/2017**
Related to libosmocore - Bug #1760: LAPD: segfault in T200 call-back	**Closed**	**07/03/2016**

History

#1 - 07/04/2020 08:21 AM - laforge

- Related to Bug #1982: LAPD: segfault in lapd_est_req function added

#2 - 07/04/2020 08:26 AM - laforge

```
Program received signal SIGSEGV, Segmentation fault.
0x00007ffff7168633 in lapd_send_i (line=line@entry=1601, lctx=<optimized out>, lctx=<optimized out>)
    at lapd_core.c:1797
1797    lapd_core.c: No such file or directory.
(gdb) bt
#0  0x00007ffff7168633 in lapd_send_i (line=line@entry=1601, lctx=<optimized out>, lctx=<optimized out>)
    at lapd_core.c:1797
#1  0x00007ffff716b168 in lapd_rx_i (lctx=0x7fffffffe4a0, msg=0x61600000b1e0) at lapd_core.c:1601
#2  lapd_ph_data_ind (msg=msg@entry=0x61600000b1e0, lctx=lctx@entry=0x7fffffffe4a0) at lapd_core.c:1642
#3  0x00007ffff701787f in lapd_receive (li=<optimized out>, msg=msg@entry=0x61600000b1e0,
    error=error@entry=0x7fffffffe570) at input/lapd.c:501
#4  0x00007ffff6fea168 in e1inp_rx_ts_lapd (e1i_ts=e1i_ts@entry=0x62f0000004b0,
    msg=msg@entry=0x61600000b1e0) at e1_input.c:708
#5  0x00007ffff703fd20 in handle_ts1_read (bfd=0x62f000000a50) at input/dahdi.c:194
#6  dahdi_fd_cb (bfd=0x62f000000a50, what=<optimized out>) at input/dahdi.c:484
#7  0x00007ffff71154f4 in osmo_fd_disp_fds (_eset=<optimized out>, _wset=<optimized out>,
    _rset=<optimized out>) at select.c:227
#8  _osmo_select_main (polling=0) at select.c:265
#9  0x00007ffff7115c06 in osmo_select_main (polling=<optimized out>) at select.c:274
#10 0x000055555556635c in main (argc=3, argv=0x7fffffffea18) at bsc_hack.c:400
(gdb) frame 1
#1  0x00007ffff716b168 in lapd_rx_i (lctx=0x7fffffffe4a0, msg=0x61600000b1e0) at lapd_core.c:1601
1601    in lapd_core.c
(gdb) p dl->tx_hist
$4 = (struct lapd_history *) 0x0
```

#3 - 07/04/2020 08:42 AM - laforge

I somehow have a deja-vu. Didn't we fix this kind of bug already at some point? The order of events appears to be:

- we receive an I-frame on an established LAPD data link (MF_EST)
- we are somewhere in lapd_rx_i() from where we dispatch the frame to the application (L3 and higher)
- while in that call-back, the application decised to destroy the data link (DL-RELEASE.req)
- after processing that, we resume processing in lapd_rx_i()

#4 - 07/04/2020 08:44 AM - laforge

laforge wrote:

> I somehow have a deja-vu. Didn't we fix this kind of bug already at some point?

See #1760 + https://gerrit.osmocom.org/c/libosmocore/+/451

#5 - 07/04/2020 08:44 AM - laforge

- Related to Bug #1760: LAPD: segfault in T200 call-back added

#6 - 07/04/2020 08:45 AM - laforge

- Related to Bug #1761: LAPD: segfault when bootstrapping Nokia InSite added

#7 - 07/04/2020 08:46 AM - laforge

- Assignee set to laforge

- % Done changed from 0 to 20

ok #1761 is the exact duplicate. We just fixed it in osmo-bsc but not in osmo-nitb.

#8 - 07/04/2020 08:56 AM - laforge

- % Done changed from 20 to 60

proposed fix in https://gerrit.osmocom.org/c/libosmocore/+/19130 - it is the only situation where we do anything after dispatching a L3 payload up the stack.

#9 - 07/04/2020 09:02 AM - laforge

- Project changed from OsmoNITB to libosmocore

- Category set to libosmogsm

- Status changed from New to In Progress

- % Done changed from 60 to 90

patch confirmed to fix the problem on an InSite.

#10 - 07/04/2020 09:23 AM - laforge

- Status changed from In Progress to Resolved

- % Done changed from 90 to 100

merged