OsmoBSC - Bug #5190

segfault with osmo-e1d

07/01/2021 08:14 PM - keith

<table>
<thead>
<tr>
<th>Status:</th>
<th>In Progress</th>
<th>Start date:</th>
<th>07/01/2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td>laforge</td>
<td>% Done:</td>
<td>0%</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
<td>Spec Reference:</td>
<td></td>
</tr>
</tbody>
</table>

Description

- The e1 hardware becomes unresponsive.. (why?) [soft reboot does not help]
- osmo-e1d starts but has no interface
- osmo-bsc crashes.

Program received signal SIGSEGV, Segmentation fault.
0x00007fffff7e8abf0 in eld_line_update (line=0x555555948af0) at input/eld.c:370
    input/eld.c: No such file or directory.
(gdb) bt
#0 0x00007fffff7e8abf0 in eld_line_update (line=0x555555948af0) at input/eld.c:370
#1 0x00007fffff7e84e7c in elinp_line_update (line=0x555555948af0) at el_input.c:929
#2 0x00005555555bc3d8 in ?? ()
#3 0x00005555555737ea in ?? ()
#4 0x00007fffff7e6409b in __libc_start_main (main=0x555555573050, argc=1, argv=0x7fffffffde5e, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fffffffe8e8) at ../csu/libc-start.c:308
#5 0x0000555555574098a in ?? ()
(gdb) quit
A debugging session is active.

Inferior 1 [process 2230] will be killed.

Quit anyway? (y or n) y
root@tosepan:/etc/osmocom# lsusb
Bus 001 Device 002: ID 8087:8000 Intel Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 003 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 002 Device 002: ID 067b:2303 Prolific Technology, Inc. PL2303 Serial Port
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub

History

#1 - 07/02/2021 08:15 AM - laforge
- Status changed from New to In Progress
- Assignee set to laforge

Hi Keith,

as usual, the more context provided in a bug report, the more likely it is fixed.

As you describe it, this is actually at least two if not more bugs. Please file them separately.

1. icE1usb hardware becomes unresponsive (separate issue, likely root cause/trigger)
2. osmo-e1d starts but has no interface
   - does this imply the unresponsive hardware makes osmo-e1d crash or stop and it is restarted e.g. by systemd?
   - If the hardware is gone from USB (see your lsusb), it's obvious that it has no interface :
3. osmo-bsc crashes. That is the actual issue here in the osmo-bsc project

#2 - 07/02/2021 08:16 AM - laforge
- Description updated

08/08/2021
The segfault appears in line 370, which is the LOGPITS statement below:

```c
if (e1i_ts->type != E1INP_TS_TYPE_NONE && ts >= num_ts_info) {
    LOGPITS(e1i_ts, DLINP, LOGL_ERROR, "Timeslot configured, but not existent 
    "on E1D side; skipping\n");
```

So the code correctly detects that osmo-bsc has configuration for a timeslot that does not exist on the e1d side. But somehow it crashes during logging :/

That macro is defined as:

```c
#define LOGPITS(els, ss, level, fmt, args ...) \ 
    LOGP(ss, level, "E1TS(%u:%u) " fmt, (els)->line->num, (els)->num, ## args)
```

So we are de-referencing e1ts->line and e1ts->num. As e1i_ts exists (we just checked for e1i_ts->type successfully, and it is a static member of 'line'), the e1i_ts->line might be NULL or an invalid pointer, resulting in the line->num deref to go wrong.

The 'line' member is set at e1inp_ts_config_{trau,i460,sign,raw,hdlc}() so it shouldn't be NULL.

I guess we should simply introduce a NULL check in the logging macro...

```c
#4 - 07/02/2021 08:26 AM - laforge
```

Actually, the 'line' back-pointer of every timeslot is also set in e1inp_line_create(), so I'm having a hard time understanding how it should be NULL or pointing to invalid memory.

```c
#5 - 07/02/2021 08:33 AM - laforge
```

In any case, we can try to make osmo-bsc not crash in this case, but it still wouldn't help you with your actual problem: the icE1usb gone from USB.

You could make sure to use a USB hub (on mainboard or external) that provides 'per-port power switching'. In those cases, you can use tools like 'uhubctl' to actually physically power-cycle the USB port, which would be a power-cycle of the icE1usb. Most cheap hubs either don't have power switching at all, or they have 'ganged' power switching, where you must disable all downstream ports (and not just one) to actually make the power go off.

Of course it shouldn't just disappear from the bus like it does, but debugging this can be hard. Meanwhile, a quick work-around is this kind of problem is the usb power cycling.

```c
#6 - 07/02/2021 08:40 AM - tnt
```

- Did 'dmesg' show anything ?
- If you have a debug uart, connect it to the ice1usb debug port and log that.

```c
#7 - 07/02/2021 09:00 AM - tnt
```

Oh and if you have a uart console (1Mbaud), you can also use some of the commands :

- 'd' Forces a USB disconnect
- 'c' To reconnect after the disconnect.
- 'b' will force boot to bootloader (and you can then use 'b' again in the bootloader to boot application image or use `dfu-util -e` for that).

```c
#8 - 07/02/2021 05:50 PM - keith
```

laforge wrote:

Hi Keith,

as usual, the more context provided in a bug report, the more likely it is fixed.

As you describe it, this is actually at least two if not more bugs. Please file them separately.
Hey Harald.. While working under some considerable pressure in the field, it's not always possible to file the optimal bug report, but rather I considered to quickly note something that was observed, so as not to let it pass by.

I should have assigned the ticket to myself to make that more clear.

#9 - 07/02/2021 05:56 PM - keith

laforge wrote:

  Of course it shouldn't just disappear from the bus like it does, but debugging this can be hard. Meanwhile, a quick work-around is this kind of problem is the usb power cycling.

Yep. Thanks for the attention to it. I'm quite aware that TIC needs to implement some method to be able to remote power reset the e1 usb in order to fix a situation like this, without having somebody physically go to the tower.

It actually hasn't happened much and I cannot reproduce it on demand. Anyway, I really didn't want to give the impression that this is urgent by making an issue, I just thought that at the very least, we shouldn't crash, hence I filed the ticket. There are a considerable amount or more urgent issues I am facing in relation to the RBS.

Thanks.