OsmoMSC - Bug #2667

osm-msc reports "invalid or out-of-range index"

11/20/2017 07:08 PM - laforge

Status:	Closed	**Start date:**	11/20/2017
Priority:	Normal	**Due date:**	
Assignee:	neels	**% Done:**	100%
Category:			
Target version:			
Resolution:		**Spec Reference:**	

Description

When starting osmo-msc on Debian unstable with no sms.db file, I get:

```
<000d> db.c:188 DBI: -6: An invalid or out-of-range index was passed to libdbi
<000d> backtrace.c:45 backtrace() returned 11 addresses
<000d> backtrace.c:55   ./osmo-msc(+0xe3d1) [0x5579ad1f43d1]
<000d> backtrace.c:55   /usr/lib/x86_64-linux-gnu/libdbi.so.1(_error_handler+0x99) [0x7f5688a94c39
]
<000d> backtrace.c:55   /usr/lib/x86_64-linux-gnu/libdbi.so.1(dbi_result_next_row+0x3d) [0x7f5688a
9685d]
<000d> backtrace.c:55   ./osmo-msc(+0xf973) [0x5579ad1f5973]
<000d> backtrace.c:55   ./osmo-msc(+0x1cb5c) [0x5579ad202b5c]
<000d> backtrace.c:55   ./osmo-msc(+0x1cc96) [0x5579ad202c96]
<000d> backtrace.c:55   ./osmo-msc(+0x1d672) [0x5579ad203672]
<000d> backtrace.c:55   ./osmo-msc(+0xa6dc) [0x5579ad1f06dc]
<000d> backtrace.c:55   /lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf1) [0x7f56887122e1]
<000d> backtrace.c:55   ./osmo-msc(+0xaa0a) [0x5579ad1f0a0a]
```

Associated revisions

Revision 0642e33a - 12/06/2017 12:45 AM - Neels Hofmeyr

add debian-sid-build, osmo-dev-on-debian-sid

Aim: build Osmocom CellNet from source on debian-sid

Related: OS#2667

History

#1 - 12/06/2017 12:54 AM - neels

- Status changed from New to In Progress

- % Done changed from 0 to 20

was able to reproduce that error message using a docker image based on debian-sid (see http://git.osmocom.org/docker-playground/commit/?id=0642e33a371782771bf4effbbb90d689f99f3b1c "add debian-sid-build, osmo-dev-on-debian-sid")

#2 - 12/06/2017 01:59 AM - neels

- Status changed from In Progress to Feedback

- Assignee changed from neels to laforge

- % Done changed from 20 to 90

with https://gerrit.osmocom.org/5205 I get:

```
20171206012939521 DDB <000d> ../../../../src/osmo-msc/src/libmsc/db.c:188 Running query: SELECT * FROM SMS WHE
RE sent IS NULL AND dest_addr > '' AND deliver_attempts <= 9 ORDER BY dest_addr, id LIMIT 1
20171206012939523 DDB <000d> ../../../../src/osmo-msc/src/libmsc/db.c:218 DBI: -6: An invalid or out-of-range
index was passed to libdbi
```

With further investigation, it becomes clear that the error log comes from

```
if (!dbi_result_next_row(result)) {
```

i.e. from precisely the line that should determine whether any results have been returned. It is thus puzzling why the error cb is invoked here.

Even when I change it to a nonempty string, I get the error:

```
20171206014418800 DDB <000d> ../../../../src/osmo-msc/src/libmsc/db.c:188 Running query: SELECT * FROM SMS WHE
RE sent IS NULL AND dest_addr > '0' AND deliver_attempts <= 9 ORDER BY dest_addr, id LIMIT 1
20171206014418802 DDB <000d> ../../../../src/osmo-msc/src/libmsc/db.c:910 1
20171206014418802 DDB <000d> ../../../../src/osmo-msc/src/libmsc/db.c:913 2
20171206014418802 DDB <000d> ../../../../src/osmo-msc/src/libmsc/db.c:218 DBI: -6: An invalid or out-of-range
index was passed to libdbi
20171206014418802 DDB <000d> ../../../src/libosmocore/src/backtrace.c:47 backtrace() returned 11 addresses
```

My initial conclusion is that this error is not caused by osmo-msc, but rather from an unstable libdbi.

However, I notice that the API offers dbi_result_*has*_next_row(), and if I call that before dbi_result_next_row(), the error output does not occur. But we actually never do this elsewhere: we always just see whether the result is NULL, and if not go on to dbi_result_next_row() right away, relying on that return value.

I could write up a patch that adds this step everywhere, simple enough:

```
        if (!dbi_result_has_next_row(result)
            || !dbi_result_next_row(result)) {
                dbi_result_free(result);
                return NULL;
        }
```

OTOH I guess it this not important enough, after all it's just dbi, and it's just debian-unstable. What do you think?

#3 - 12/06/2017 06:48 PM - alteholz

neels wrote:

> My initial conclusion is that this error is not caused by osmo-msc, but rather from an unstable libdbi.

recently there was a "fix" in libdbi. In case of an invalid index, the error handler was not called (the original call was commented out by error) and 0 was returned as a result of calling dbi_result_next_row() instead.
I think the error is due to result being 0 if the last row was already fetched and thus the preceding call to dbi_result_has_next_row() seems good.

> OTOH I guess it this not important enough, after all it's just dbi, and it's just debian-unstable. What do you think?

debian unstable will become stable sooner or later ...

#4 - 12/06/2017 07:20 PM - laforge

I think this discussion is one more sign we want to get rid of libdbi rather sooner
than later. Unfortunately we have way too few developers for way too much work
as-is :/

#5 - 12/10/2017 01:51 PM - neels

- Status changed from Feedback to In Progress

- Assignee changed from laforge to neels

actually now my laptop has moved to debian testing and I don't want to see these useless warnings all the time, hence submitted
https://gerrit.osmocom.org/5265

#6 - 12/10/2017 03:34 PM - laforge

- Status changed from In Progress to Closed

- % Done changed from 90 to 100