

Tvheadend - Bug #1226

Crash when started "Map DVB services to channels"

2012-09-15 18:38 - Hernán R

Status:	Fixed	Start date:	2012-09-15
Priority:	Normal	Due date:	
Assignee:		% Done:	100%
Category:	DVB	Estimated time:	0.00 hour
Target version:	3.2	Affected Versions:	3.2, 3.4
Found in version:	3.1.677		

Description

I've compiled it from git today and started testing it, then had this error every time:

After successfully adding DVB Network by location, and after waiting for all services to be detected, as soon as I click on "Map DVB services to channels" tvheadend crashes with this log:

```
{}{}
Sep 15 13:20:02 tvheadend kernel: [ 2545.900486] mb86a20s: mb86a20s_read_status: val = 8, status = 0x1f
Sep 15 13:20:02 tvheadend tvheadend1516: TS: ISDBT/539,142 kHz: Transport error indicator
Sep 15 13:20:02 tvheadend kernel: [ 2545.998886] mb86a20s: mb86a20s_read_status:
Sep 15 13:20:02 tvheadend kernel: [ 2545.999366] mb86a20s: mb86a20s_read_status: val = 8, status = 0x1f
Sep 15 13:20:02 tvheadend kernel: [ 2545.999380] mb86a20s: mb86a20s_read_signal_strength:
Sep 15 13:20:02 tvheadend tvheadend1516: TS: ISDBT/539,142 kHz: H264 #352: Continuity counter error
Sep 15 13:20:02 tvheadend kernel: [ 2546.021482] mb86a20s: mb86a20s_read_signal_strength: signal strength = 4096
Sep 15 13:20:03 tvheadend tvheadend[1516]: TS: ISDBT/539,142 kHz: Transport error indicator, 58 duplicate log lines suppressed
Sep 15 13:20:03 tvheadend tvheadend[1516]: TS: ISDBT/539,142 kHz: H264 #352: Continuity counter error, 13 duplicate log lines suppressed
Sep 15 13:20:03 tvheadend tvheadend1516: TS: ISDBT/539,142 kHz: AAC #353: Continuity counter error
Sep 15 13:20:03 tvheadend tvheadend[1516]: TS: ISDBT/539,142 kHz: H264 #352: Corrupted PES header
Sep 15 13:20:03 tvheadend tvheadend1516: subscription: "serviceprobe" unsubscribing
Sep 15 13:20:03 tvheadend tvheadend1516: serviceprobe: (null): mapped to channel "(null)"
Sep 15 13:20:03 tvheadend tvheadend1516: CRASH: Signal: 11 in PRG: /usr/bin/tvheadend (3.1.677.g65a53.dirty)
[fd25a386e59fff0ad01197f53af1c9fae7e9b7a0] CWD: /
Sep 15 13:20:03 tvheadend tvheadend1516: CRASH: Fault address 0x140 (Address not mapped)
Sep 15 13:20:03 tvheadend tvheadend1516: CRASH: Loaded libraries: /lib/x86_64-linux-gnu/libcrypto.so.1.0.0
/lib/x86_64-linux-gnu/libz.so.1 /usr/lib/x86_64-linux-gnu/libavahi-common.so.3 /usr/lib/x86_64-linux-gnu/libavahi-client.so.3
/lib/x86_64-linux-gnu/librt.so.1 /lib/x86_64-linux-gnu/libdl.so.2 /lib/x86_64-linux-gnu/libpthread.so.0 /lib/x86_64-linux-gnu/libc.so.6
/lib/x86_64-linux-gnu/libdbus-1.so.3 /lib64/ld-linux-x86-64.so.2 /lib/x86_64-linux-gnu/libnss_compat.so.2
/lib/x86_64-linux-gnu/libnsl.so.1 /lib/x86_64-linux-gnu/libnss_nis.so.2 /lib/x86_64-linux-gnu/libnss_files.so.2
Sep 15 13:20:03 tvheadend tvheadend1516: CRASH: Register dump [23]: 0000000000000005 000000000000009b
6863206f74206465 0000000000000001 000000000207eb80 00007f6f65a32e58 0000000000000000 00007f6f48000e60
0000000000000000 0000000001fc6810 0000000001fc6810 0000000000000000 0000000000000001 0000000001fc6810
0000000000000000 00007f6f65a32d90 0000000000414a12 0000000000010202 0000000000000033 0000000000000004
000000000000000e ffffffff7ffbfa17 0000000000000140
Sep 15 13:20:03 tvheadend tvheadend1516: CRASH: STACKTRACE
Sep 15 13:20:03 tvheadend tvheadend1516: CRASH: 0x424c7b
Sep 15 13:20:03 tvheadend tvheadend1516: CRASH: 0x7f6f6834ccb0
Sep 15 13:20:03 tvheadend tvheadend1516: CRASH: 0x414a12
Sep 15 13:20:03 tvheadend tvheadend1516: CRASH: 0x420509
Sep 15 13:20:03 tvheadend tvheadend1516: CRASH: 0x7f6f68344e9a
Sep 15 13:20:03 tvheadend tvheadend1516: CRASH: clone+0x6d (/lib/x86_64-linux-gnu/libc.so.6)
Sep 15 13:20:03 tvheadend kernel: [ 2546.265617] tvheadend1523: segfault at 140 ip 0000000000414a12 sp 00007f6f65a32d90 error
4 in tvheadend[400000+81000]
Sep 15 13:20:03 tvheadend kernel: [ 2546.304872] cx231xx #0: cx231xx_stop_stream(): ep_mask = 1
{}{}

```

I'm testing it on a fresh Ubuntu Server 12.04.1 install: {}{}

```
$ uname -a
```

```
Linux tvheadend 3.2.0-30-generic #48-Ubuntu SMP Fri Aug 24 16:52:48 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux
```

```
{}{}
```

I've compiled it on another similar machine.

My DVB device is detected as `_dev_dvb_adapter0_Fujitsu_mb86A20s`, and in fact it's a Kworld UB430-AF (USB).

Please let me know any other necessary information.

Associated revisions

Revision 31b1d5b5 - 2012-10-31 13:28 - Adam Sutton

Refs #1226 - remove block to creating empty channels.

Revision 72e369a8 - 2012-11-05 11:53 - Adam Sutton

Fix #1226 - remove block to creating empty channels.

(cherry picked from commit 31b1d5b57d0148bad30861f74ba10b3f385a9a73)

History

#1 - 2012-09-18 02:07 - Hernán R

ok, so I did some homework and discovered this is crashing for "services" with empty fields ("service name", "Provider" and "Network").

To confirm I disabled all services with empty fields and after clicking on "Map DVB services to channels" button it didn't crash, and the syslog shows:

```
Sep 17 20:51:50 tvheadend tvheadend[3455]: serviceprobe:          Canal 9 SD: checking...
Sep 17 20:51:50 tvheadend tvheadend[3455]: subscription: "serviceprobe" direct subscription to adapter: "ISDBT
", network: "Canal 9", mux: "Canal 9: 599,142 kHz", provider: "Telearte SD", service: "Canal 9 SD", quality: 1
00
Sep 17 20:51:50 tvheadend tvheadend[3455]: subscription: "serviceprobe" unsubscribing
Sep 17 20:51:50 tvheadend tvheadend[3455]: serviceprobe:          Canal 9 SD: mapped to channel "Canal 9 SD"
Sep 17 20:51:50 tvheadend tvheadend[3455]: serviceprobe:          Canal 9 SD: joined tag "TV channels"
Sep 17 20:51:50 tvheadend tvheadend[3455]: serviceprobe:          Canal 9 SD: joined tag "SDTV"
Sep 17 20:51:50 tvheadend tvheadend[3455]: serviceprobe:          Canal 9 SD: joined tag "Telearte SD"
Sep 17 20:51:50 tvheadend tvheadend[3455]: serviceprobe: Now idle
```

And of course this channel appeared in the Channels tab.

Hope this helps.

Hernán.-

#2 - 2012-09-19 11:15 - Adam Sutton

- Category set to DVB

- Status changed from New to Need feedback

Can you get a gdb trace for the crash?

It'll save me digging through the code to find the point of failure. And I'm quite busy at the moment.

Adam

#3 - 2012-09-25 01:06 - Hernán R

I've followed this instructions: <https://www.lonelycoder.com/redmine/projects/tvheadend/wiki/Tvheadendcrash>

And it doesn't crash while running under gdb. It only shows:

```
Sep 24 20:02:38 [INFO]:serviceprobe: Starting
Sep 24 20:02:38 [INFO]:serviceprobe:          (null): checking...
Sep 24 20:02:38 [INFO]:subscription: "serviceprobe" unsubscribing
Sep 24 20:02:38 [INFO]:subscription: "serviceprobe" direct subscription failed -- No hardware present
Sep 24 20:02:38 [INFO]:serviceprobe:          (null): could not subscribe
Sep 24 20:02:38 [INFO]:serviceprobe: Now idle
```

However, my hardware is properly detected, and running without gdb crashes as it was mentioned above.

Anything else I should try ?

Thanks,

Hernán.-

#4 - 2012-09-25 10:35 - Adam Sutton

Hernan,

When you run under gdb and it crashes you need to run the gdb command "bt full" and provide that output.

Regards
Adam

#5 - 2012-10-24 11:35 - Adam Sutton

Hernan,

Is this still happening (or has it happened again). Since there has been no update in a month I'm inclined to close this.

Adam

#6 - 2012-10-28 15:15 - Hernán R

- *File services.png added*

Yes, this is still happening, and it's easy to reproduce:

You have to have a service with no 'service name' and no 'channel name' as it's shown on the attached screenshot. As soon as you click on 'Map DVB services to channels' the software crashes. On the latest builds, this crash could go unnoticed as tvheadend restarts itself.

Following this test case, if you add something to 'channel name' it doesn't crash. If 'service name' has something filled in, it doesn't crash.

So, it crashes with no 'service name' and no 'channel name'.

Regarding gdb, sorry but I was not able to capture this issue with it. I was able to run tvheadend under gdb, using same user/configuration, but it gives me some other errors as I've noted on <https://www.lonelycoder.com/redmine/issues/1226#note-3>. Therefore, I was not able to make it crash under gdb.

If there is anything else I could try to help resolve this issue I will be pleased to do so.

Thanks,
Hernán.-

#7 - 2012-10-30 18:06 - Adam Sutton

- *Status changed from Need feedback to Accepted*

- *Target version set to 3.2*

- *Affected Versions 3.2, 3.4 added*

No,

I'll re-visit the code and see if I can replicate myself.

Adam

#8 - 2012-10-31 11:49 - Adam Sutton

I think I can see what is probably happening here. I think I added code to stop channels being created with an empty name, since this generally isn't a good idea and causes things to get very confused.

But I don't think the serviceprobe code expects the channel lookup function to return NULL, so it doesn't check the return and blindly uses the ptr.

I will give it some thought.

Adam

#9 - 2012-10-31 14:50 - Adam Sutton

- *Status changed from Accepted to Resolved*

Hernan,

I think my latest commit should resolve this issue, if you could check I'd appreciate that (in git master at the moment).

Adam

#10 - 2012-11-05 13:02 - Adam Sutton

- *Status changed from Resolved to Fixed*

- % Done changed from 0 to 100

Applied in changeset [72e369a839ef7f5c97be431c153769029db8fa4e](#).

Files

services.png	11.6 KB	2012-10-28	Hernán R
--------------	---------	------------	----------