Audacious - OLD, PLEASE USE GITHUB DISCUSSIONS/ISSUES - Bug #68

Invalid free() in pa_context_new()

February 10, 2012 23:56 - remi p

Status:	Closed		**Start date:**	February 10, 2012
Priority:	Major		**Due date:**	
Assignee:			**% Done:**	0%
Category:			**Estimated time:**	0.00 hour
Target version:				
Affects version:				

Description

Hello,

I am using audacious 3.2 with GTK interface.
When I have a playlist playing, audacious sometimes stops at the end of a song. I attached the log of the segmentation fault to this bug. This happens randomly, in average it occurs after playing about 4 songs in a playlist.

Could you have a look?
Thanks !

History

#1 - February 10, 2012 23:59 - remi p

I am using Ubuntu 10.04 Lucid and I build audacious thanks to the tarball on the website.

#2 - February 11, 2012 07:04 - John Lindgren

- Subject changed from Segmentation fault when changing song in playlist to Invalid free() in pa_context_new()

This is a duplicate of [#40](#40) and still unreproducible. I will close the report unless you have some new information to provide.

#3 - February 11, 2012 07:10 - John Lindgren

Out of curiosity, is there a reason you are using the ALSA output plugin to access PulseAudio via its ALSA emulation layer, rather than using the native PulseAudio output plugin?

#4 - February 11, 2012 12:05 - remi p

Thanks for the reply. The only reason I used ALSA rather than pulseaudio output plugin is that it consumes less CPU. I tried using pulseaudio, and the error occurs less often, but I got a different stack after a while :

```
======= Backtrace: =========
/lib/tls/i686/cmov/libc.so.6(+0x6b591)[0x2ec591]
/lib/tls/i686/cmov/libc.so.6(+0x6cde8)[0x2edde8]
/lib/tls/i686/cmov/libc.so.6(cfree+0x6d)[0x2f0ecd]
/usr/lib/libX11.so.6(XFree+0x1d)[0x51845d]
/usr/lib/libpulsecommon-0.9.21.so(pa_x11_get_prop+0xae)[0xb4648e]
/usr/lib/libpulse.so.0(+0x381a9)[0x7fb1a9]
/usr/lib/libpulse.so.0(pa_context_new_with_proplist+0x19b)[0x7d0a2b]
/usr/lib/libpulse.so.0(pa_context_new+0x2c)[0x7d0b3c]
/usr/local/lib/audacious/Output/pulse_audio.so(+0x2e2f)[0x6e1e2f]
audacious[0x805a28f]
/usr/local/lib/audacious/Input/madplug.so(+0x2438)[0x807438]
audacious[0x805b822]
/lib/tls/i686/cmov/libpthread.so.0(+0x596e)[0x9f496e]
/lib/tls/i686/cmov/libc.so.6(clone+0x5e)[0x34ea4e]
```

Is there any workaround to avoid this ?

#5 - February 11, 2012 14:41 - John Lindgren

Okay, another X11-related crash within pa_context_new(). I searched Google a bit last night, and I think the problem here is that Xlib is not thread-safe. Hence, its use within pa_context_new() (or within an output plugin, period) is dangerous. So this is a problem that needs to be fixed either in PulseAudio (stop using Xlib) or X11 (make Xlib thread-safe). For a workaround, I can't think of much at the moment ... uninstall PulseAudio?

#6 - February 11, 2012 14:47 - John Lindgren

Found this: http://pulseaudio.org/ticket/799

What version of PulseAudio do you have? EDIT: Looked at your backtrace again, you have 0.9.21. Upgrade PulseAudio to 0.9.22 or newer. Closing.

#7 - February 11, 2012 14:48 - John Lindgren

- Status changed from New to Closed

#8 - February 12, 2012 18:50 - remi p

I have 0.9.21 indeed. I will try to upgrade it. Thanks for your support.

#9 - March 03, 2012 21:22 - remi p

Hello,

I uninstalled pulseaudio and chose Alsa as output. I get the same error, here is the backtrace :

======= Backtrace: =========
/lib/tls/i686/cmov/libc.so.6(+0x6b591)[0x782591]
/lib/tls/i686/cmov/libc.so.6(+0x6e395)[0x785395]
/lib/tls/i686/cmov/libc.so.6(__libc_calloc+0xab)[0x78670b]
/usr/lib/libasound.so.2(snd_config_update_r+0x477)[0x137ca17]
/usr/lib/libasound.so.2(snd_config_update+0x48)[0x137cdc8]
/usr/lib/libasound.so.2(snd_pcm_open+0x39)[0x13a3bc9]
/usr/local/lib/audacious/Output/alsa.so(alsa_open_audio+0xd9)[0xe65e79]
audacious[0x805a28f]
/usr/local/lib/audacious/Input/madplug.so(+0x2438)[0x5c3438]
audacious[0x805b822]
/lib/tls/i686/cmov/libpthread.so.0(+0x596e)[0xa6596e]
/lib/tls/i686/cmov/libc.so.6(clone+0x5e)[0x7e4a4e]

Then, still with pulseaudio uninstalled, I tried selecting "No Input" as output. I get the backtrace:

- glibc detected * **audacious: free(): invalid next size (normal): 0xb4cbf148** * ======= Backtrace: =========
  /lib/tls/i686/cmov/libc.so.6(+0x6b591)[0x25f3591]
  /lib/tls/i686/cmov/libc.so.6(+0x6cde8)[0x25f4de8]
  /lib/tls/i686/cmov/libc.so.6(cfree+0x6d)[0x25f7ecd]
  /lib/libglib-2.0.so.0(g_free+0x36)[0x838fc6]
  audacious[0x805960b]
  audacious[0x8059cbb]
  /usr/local/lib/audacious/Input/madplug.so(+0x274f)[0x6ce74f]
  audacious[0x805b822]
  /lib/tls/i686/cmov/libpthread.so.0(+0x596e)[0x2b296e]
  /lib/tls/i686/cmov/libc.so.6(clone+0x5e)[0x2655a4e]

These crashes still happen randomly (every 3-4 songs).
Is this really a pulseaudio-related issue?

#10 - March 10, 2012 21:42 - remi p

Please note that after falling back to audacious 2.5.3, the problem does not occur anymore.

#11 - March 11, 2012 14:17 - John Lindgren

Different backtraces = different problems. Open a new bug report, don't confuse things by commenting on an old one.

Files

audacious_segfault.txt	7.84 KB February 10, 2012	remi p