

Audacious - OLD, PLEASE USE GITHUB DISCUSSIONS/ISSUES - Bug #40

Invalid free() in pa_context_new()

January 09, 2012 23:52 - Joe Giampaoli

Status:	Closed	Start date:	January 09, 2012
Priority:	Minor	Due date:	
Assignee:		% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:			
Affects version:			
Description			
Sometimes when I double click on a song in the list in the GTK interface Audacious crashes. This happens with latest 3.1.2 self compiled.			
Thanks			
Joe			

History

#1 - January 10, 2012 00:25 - Joe Giampaoli

Here's a backtrace I got when I double clicked on a song in the list to jump to it:

joe@ghubuntu1:~\$ audacious

- glibc detected * **audacious: free(): invalid next size (normal): 0xac245f28** * ===== Backtrace: =====
/lib/tls/i686/cmov/libc.so.6(+0x6b591)[0xb6e52591]
/lib/tls/i686/cmov/libc.so.6(+0x6cde8)[0xb6e53de8]
/lib/tls/i686/cmov/libc.so.6(cfree+0x6d)[0xb6e56ecd]
/usr/lib/libX11.so.6(_XFreeDisplayStructure+0x226)[0xb6c7cc26]
/usr/lib/libX11.so.6(XCloseDisplay+0xe1)[0xb6c69321]
/usr/lib/libpulse.so.0(+0x38252)[0xb2290252]
/usr/lib/libpulse.so.0(pa_context_new_with_proplist+0x19b)[0xb2265a2b]
/usr/lib/libpulse.so.0(pa_context_new+0x2c)[0xb2265b3c]
/usr/local/lib/audacious/Output/pulse_audio.so(+0x2e5f)[0xb2208e5f]
audacious[0x805abad]
/usr/local/lib/audacious/Input/madplug.so(+0x2578)[0xb57b6578]
audacious[0x805c206]
/lib/tls/i686/cmov/libpthread.so.0(+0x596e)[0xb6f5696e]
/lib/tls/i686/cmov/libc.so.6(clone+0x5e)[0xb6eb4a4e] ===== Memory map: =====
08048000-0807f000 r-xp 00000000 08:05 1968482 /usr/local/bin/audacious
0807f000-08080000 r--p 00036000 08:05 1968482 /usr/local/bin/audacious
08080000-08082000 rw-p 00037000 08:05 1968482 /usr/local/bin/audacious
08082000-08085000 rw-p 00000000 00:00 0
09aeb000-09ea5000 rw-p 00000000 00:00 0 [heap]
a91fc000-a91fd000 ---p 00000000 00:00 0
a91fd000-a99fd000 rw-p 00000000 00:00 0
ab200000-ab239000 rw-p 00000000 00:00 0
ab239000-ab300000 ---p 00000000 00:00 0
ab3fc000-ab3fd000 ---p 00000000 00:00 0
ab3fd000-abbfd000 rw-p 00000000 00:00 0
ac200000-ac280000 rw-p 00000000 00:00 0
ac280000-ac300000 ---p 00000000 00:00 0
ac314000-ac3ac000 r--p 00000000 08:05 1992225 /usr/share/fonts/truetype/ttf-dejavu/DejaVuSans.ttf
ac3fe000-ac3ff000 ---p 00000000 00:00 0
ac3ff000-acbff000 rw-p 00000000 00:00 0
acbff000-acc00000 ---p 00000000 00:00 0
acc00000-ad400000 rw-p 00000000 00:00 0
ad400000-ad448000 rw-p 00000000 00:00 0
ad448000-ad500000 ---p 00000000 00:00 0
ad52d000-ad54e000 rw-p 00000000 00:00 0
ad573000-ad574000 ---p 00000000 00:00 0
ad574000-add74000 rw-p 00000000 00:00 0
adda5000-addc4000 r-xp 00000000 08:05 1834897 /usr/lib/libjpeg.so.62.0.0
addc4000-addc5000 r--p 0001e000 08:05 1834897 /usr/lib/libjpeg.so.62.0.0
addc5000-addc6000 rw-p 0001f000 08:05 1834897 /usr/lib/libjpeg.so.62.0.0

```

adde4000-adde8000 r-xp 00000000 08:05 1844146 /usr/lib/gtk-2.0/2.10.0/loaders/libpixbufloader-jpeg.so
adde8000-adde9000 r--p 00003000 08:05 1844146 /usr/lib/gtk-2.0/2.10.0/loaders/libpixbufloader-jpeg.so
adde9000-addea000 rw-p 00004000 08:05 1844146 /usr/lib/gtk-2.0/2.10.0/loaders/libpixbufloader-jpeg.so
addea000-addeb000 ---p 00000000 00:00 0
addeb000-ae5eb000 rw-p 00000000 00:00 0
ae5eb000-ae624000 r-xp 00000000 08:05 1834844 /usr/lib/libibus.so.1.0.0
ae624000-ae625000 r--p 00039000 08:05 1834844 /usr/lib/libibus.so.1.0.0
ae625000-ae626000 rw-p 0003a000 08:05 1834844 /usr/lib/libibus.so.1.0.0
ae638000-ae644000 r--p 00000000 08:05 2386437 /usr/share/fonts/truetype/Other/BRATLBS0.TTF
ae644000-ae649000 r-xp 00000000 08:05 1838609 /usr/lib/gtk-2.0/2.10.0/immodules/im-ibus.so
ae649000-ae64a000 r--p 00004000 08:05 1838609 /usr/lib/gtk-2.0/2.10.0/immodules/im-ibus.so
ae64a000-ae64b000 rw-p 00005000 08:05 1838609 /usr/lib/gtk-2.0/2.10.0/immodules/im-ibus.so
ae64b000-ae6ab000 rw-s 00000000 00:04 3768341 /SYSV00000000 (deleted)
ae6ab000-ae70b000 rw-s 00000000 00:04 3735572 /SYSV00000000 (deleted)
ae70b000-ae725000 r--s 00000000 08:05 1962423 /usr/share/mime/mime.cache
ae725000-ae72f000 r-xp 00000000 08:05 3793724 /lib/libudev.so.0.6.1
ae72f000-ae730000 r--p 00009000 08:05 3793724 /lib/libudev.so.0.6.1
ae730000-ae731000 rw-p 0000a000 08:05 3793724 /lib/libudev.so.0.6.1
ae731000-ae745000 r-xp 00000000 08:05 1832600 /usr/lib/libgvfscommon.so.0.0.0
ae745000-ae746000 r--p 00013000 08:05 1832600 /usr/lib/libgvfscommon.so.0.0.0
ae746000-ae747000 rw-p 00014000 08:05 1832600 /usr/lib/libgvfscommon.so.0.0.0
ae752000-ae763000 r-xp 00000000 08:05 1834976 /usr/lib/gio/modules/libgioremote-volume-monitor.so
ae763000-ae764000 r--p 00011000 08:05 1834976 /usr/lib/gio/modules/libgioremote-volume-monitor.so
ae764000-ae765000 rw-p 00012000 08:05 1834976 /usr/lib/gio/modules/libgioremote-volume-monitor.so
ae765000-ae789000 r-xp 00000000 08:05 1834977 /usr/lib/gio/modules/libgvfsdbus.so
ae789000-ae78a000 r--p 00023000 08:05 1834977 /usr/lib/gio/modules/libgvfsdbus.so
ae78a000-ae78b000 rw-p 00024000 08:05 1834977 /usr/lib/gio/modules/libgvfsdbus.so
ae78b000-ae7da000 r--p 00000000 08:05 1992227 /usr/share/fonts/truetype/ttf-dejavu/DejaVuSansMono.ttf
ae7da000-aede7000 r--p 00000000 08:05 2117160 /usr/share/icons/hicolor/icon-theme.cache
aede7000-af445000 r--p 00000000 08:05 2491677 /usr/local/share/icons/hicolor/icon-theme.cache
af445000-afc19000 r--p 00000000 08:05 2107596 /usr/share/icons/gnome/icon-theme.cache
afc19000-afc25000 r--p 00000000 08:05 2385865 /usr/share/fonts/truetype/Other/BRATLRS0.TTF
afc25000-afc27000 r-xp 00000000 08:05 1964913 /usr/lib/pango/1.6.0/modules/pango-basic-fc.so
afc27000-afc28000 r--p 00001000 08:05 1964913 /usr/lib/pango/1.6.0/modules/pango-basic-fc.so
afc28000-afc29000 rw-p 00002000 08:05 1964913 /usr/lib/pango/1.6.0/modules/pango-basic-fc.so
afc29000-afc2a000 r--s 00000000 08:05 926494 /var/cache/fontconfig/26de28bc8622bbc1fb67fd234c21975f-le32d4.cache-3
afc2a000-afc2c000 r--s 00000000 08:05 923895 /var/cache/fontconfig/b2373b1a2f4d1b1789f2980b7c93313d-le32d4.cache-3
afc2c000-afc2d000 r--s 00000000 08:05 924024 /var/cache/fontconfig/c05880de57d1f5e948fdacc138775d9-le32d4.cache-3
afc2d000-afc33000 r--s 00000000 08:05 915782 /var/cache/fontconfig/945677eb7aeaf62f1d50efc3fb3ec7d8-le32d4.cache-3
afc33000-afc35000 r--s 00000000 08:05 924022 /var/cache/fontconfig/99e8ed0e538f840c565b6ed5dad60d56-le32d4.cache-3
afc35000-afc38000 r--s 00000000 08:05 924021 /var/cache/fontconfig/e383d7ea5f6e662a33d9b44caf393297-le32d4.cache-3
afc38000-afc3e000 r--s 00000000 08:05 924020 /var/cache/fontconfig/401a5dd6b567794a1d18dd9342dfa604-le32d4.cache-3
afc3e000-afc3f000 r--s 00000000 08:05 924018 /var/cache/fontconfig/e7071f4a29fa870f4323321c154eba04-le32d4.cache-3
afc3f000-afc42000 r--s 00000000 08:05 924016 /var/cache/fontconfig/6eb3985aa4124903f6ff08ba781cd364-le32d4.cache-3
afc42000-afc43000 r--s 00000000 08:05 924015 /var/cache/fontconfig/4c73fe0c47614734b17d736dbde7580a-le32d4.cache-3
afc43000-afc44000 r--s 00000000 08:05 924014 /var/cache/fontconfig/0d8c3b2ac0904cb8a57a757ad11a4a08-le32d4.cache-3
afc44000-afc45000 r--s 00000000 08:05 924012 /var/cache/fontconfig/6a53c69dea097a2d716e069445527da8-le32d4.cache-3
afc45000-afc49000 r--s 00000000 08:05 924011 /var/cache/fontconfig/a755afe4a08bf5b97852ceb7400b47bc-le32d4.cache-3
joe@ghubuntu1:~$

```

#2 - January 10, 2012 02:37 - John Lindgren

Based on the backtrace, this looks more like a problem in PulseAudio or possibly even X11 than in Audacious.

#3 - January 10, 2012 02:37 - John Lindgren

For a workaround you could use ALSA output.

#4 - January 10, 2012 02:38 - John Lindgren

- Subject changed from Audacious crashes when jumping to new song to Invalid free() in pa_context_new()

#5 - January 10, 2012 03:32 - Joe Giampaoli

Just changed to ALSA output in Audacious preferneces and got same result with different backtrace:

```
joe@ghubuntu1:~$ audacious
alsa: snd_pcm_recover failed: Input/output error.
alsa: snd_pcm_recover failed: Input/output error.
alsa: snd_pcm_recover failed: Input/output error.
audacious: malloc.c:3096: sYSMALLOc: Assertion `(old_top < (((mbinptr) (((char *) &((av)->bins[((1) - 1) * 2])) - __builtin_offsetof (struct malloc_chunk, fd)))) && old_size > 0) || ((unsigned long) (old_size) >= (unsigned long) (((__builtin_offsetof (struct malloc_chunk, fd_nextsize)) + ((2 * (sizeof(size_t))) - 1)) & ~((2 * (sizeof(size_t))) - 1))) && ((old_top)->size & 0x1) && ((unsigned long)old_end & pagemask) == 0)' failed.
Aborted
joe@ghubuntu1:~$
```

#6 - January 10, 2012 04:28 - John Lindgren

Try running Audacious in Valgrind to see if it can pick up any errors.

#7 - January 10, 2012 07:30 - Joe Giampaoli

- File valgrind-log-001 added

Ok I'm attaching file "valgrind-log-001"

I ran audacious from zero (preferences deleted from home dir), and recorded all this output with loading some mp3's and played a few (pulse audio was selected), strangely nothing happened, no crash when jumping from song to song, the I wen to preferences and changed to ALSA and suddenly Audacious crashed.

Thanks.

#8 - January 11, 2012 15:12 - John Lindgren

Well, you have three apparently unrelated crashes here. I'm afraid I can't be of any more help without being able to reproduce any of them. Let us know if you find out the cause.

#9 - January 19, 2012 13:58 - John Lindgren

- Status changed from New to Closed

Cannot reproduce, closing.

valgrind-log-001	218 KB	January 10, 2012	Joe Giampaoli
------------------	--------	------------------	---------------