Audacious - Bug #245

Memory corruption

January 27, 2013 12:58 - Marcin Kocur

Status:	Closed	**Start date:**	January 27, 2013
Priority:	Major	**Due date:**	
Assignee:		**% Done:**	100%
Category:	plugins/ffaudio	**Estimated time:**	0.00 hour
Target version:	3.3.4		
Affects version:	3.3.3		

Description

Hey, my audacious recently became to behave strangely. I was using it for few days and it was doing what it supposed to do, however one day after changing a song to a next one, it crashed. When I run it again, I could listen to the track played before, but when I was trying to change the song to any other, audacious core dumped again. So, audacious could play only one song from my playlist without a crash.

I have removed a playlist ~/.config/audacious/playlist.xspf, created a new one and it was fine for few days, until situation described above happened again.

So today I removed ~/.config/audacious/, ~/.local/share/audacious, reinstalled audacious and audacious-plugins and started again (look at the bash input, I set en_US locale:

http://img.koci.net.pl/images/screen213.png
http://pokazywarka.pl/asbfsf/

Again:

http://img.koci.net.pl/images/screen214.png

[mk@linux ~]$ audacious

(process:9429): Gtk-WARNING **: Locale not supported by C library.
Using the fallback 'C' locale.
(bootstrap.c:60) [mowgli_init]: mowgli_init() is a deprecated function, provided only for backwards compatibility with Mowgli-1. You should remove it if you no longer support using Mowgli-1.

It seems inspite of this warning, it works. I've reverted LANG variable to default just by closing console tab:
[mk@linux ~]$ echo $LANG
pl_PL.UTF-8

and started over again:

[mk@linux ~]$ audacious
(bootstrap.c:60) [mowgli_init]: mowgli_init() is a deprecated function, provided only for backwards compatibility with Mowgli-1. You should remove it if you no longer support using Mowgli-1.
pulseaudio: Failed to connect to server: Connection refused
Naruszenie ochrony pamięci (core dumped) [in English: memory access violation]

Then I make sure audacious isn't running anymore, removed .config/audacious/lock and started again:

[mk@linux ~]$ audacious
(bootstrap.c:60) [mowgli_init]: mowgli_init() is a deprecated function, provided only for backwards compatibility with Mowgli-1. You should remove it if you no longer support using Mowgli-1.
pulseaudio: Failed to connect to server: Connection refused **
GLib-GObject:ERROR:gtype.c:1991:type_iface_vtable_base_init_Wm: assertion failed: (iface->data && entry && entry->vtable == NULL && iholder && iholder->info)
Przerwane (core dumped)

Repeating the same gives the same result but without GLib-GObject line.

Over again, with gdb:

http://pokazywarka.pl/l0j0ol/

Again, strace -o strace.log audacious:
http://koci.net.pl/upload/uploads/strace.log

I wish I could be more helpful but I don't exactly know how to debug an app :)
I think it's the same issue as here: https://bugs.archlinux.org/task/31774

I use up-to-date Archlinux 64bit.

History

#1 - January 27, 2013 13:02 - Marcin Kocur

I'm sorry for the first listing (http://pokazywarka.pl/asbfsf/), it should be just
[mk@linux ~]$ export LANG=en_US.UTF-8
[mk@linux ~]$ audacious

#2 - January 27, 2013 15:33 - John Lindgren

Please attach a backtrace (Google "gdb backtrace").

#3 - January 27, 2013 17:45 - John Lindgren

- Subject changed from Core dumped (mowgli_init() is a deprecated function...) to Various crashes

- Category deleted (core)

- Priority changed from Critical to Major

#4 - January 27, 2013 20:14 - Thomas Lange

https://wiki.archlinux.org/index.php/Debug_-_Getting_Traces

#5 - January 29, 2013 01:16 - Marcin Kocur

I run into problems installing glibc. I really do hope non-stripped audacious will be enough:

```
[mk@linux glibc]$ gdb audacious
gdb: warning: error finding working directory: Nie ma takiego pliku ani katalogu
GNU gdb (GDB) 7.5.1
Copyright (C) 2012 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-unknown-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /usr/bin/audacious...done.
(gdb) r
Starting program: /usr/bin/audacious
shell-init: błąd przy określaniu katalogu bieżącego: getcwd: niemożliwy dostęp do katalogów nadrzędnych: Nie m
a takiego pliku ani katalogu
warning: Could not load shared library symbols for linux-vdso.so.1.
Do you need "set solib-search-path" or "set sysroot"?
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/usr/lib/libthread_db.so.1".
Traceback (most recent call last):
  File "/usr/share/gdb/auto-load/usr/lib/libgobject-2.0.so.0.3400.3-gdb.py", line 9, in <module>
    from gobject import register
  File "/usr/share/glib-2.0/gdb/gobject.py", line 3, in <module>
    import gdb.backtrace
ImportError: No module named backtrace
(bootstrap.c:60) [mowgli_init]: mowgli_init() is a deprecated function, provided only for backwards compatibil
ity with Mowgli-1.  You should remove it if you no longer support using Mowgli-1.
[New Thread 0x7fffec5f0700 (LWP 2907)]
Failed to load plugin (/usr/lib/audacious/Container/cue.so): libcue.so.1: nie można otworzyć pliku obiektu dzi
@@elonego: Nie ma takiego pliku ani katalogu
pulseaudio: Failed to connect to server: Connection refused
[New Thread 0x7fffd85d5700 (LWP 2909)]
```

```
[New Thread 0x7fffd7dd4700 (LWP 2910)]
[New Thread 0x7fffd75d3700 (LWP 2911)]
[New Thread 0x7fffd6dd2700 (LWP 2912)]

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff608283b in g_object_newv () from /usr/lib/libgobject-2.0.so.0
```

#6 - January 29, 2013 01:40 - John Lindgren

This isn't a backtrace. Read http://www.cs.cmu.edu/~gilpin/tutorial/ and then try again.

#7 - January 29, 2013 11:14 - Marcin Kocur

Any chance this could be more helpful?:
http://wklej.org/id/941107/

#8 - January 29, 2013 23:57 - John Lindgren

Well, it's a backtrace at least, but not really any more helpful. It's unlikely that any Audacious developer will be able to fix a crash 8 levels deep into GTK+/GLib without being able to reproduce it.

#9 - January 30, 2013 00:30 - Marcin Kocur

So there is no hope? The stupid thing is that my system is not very different from well-maintained Linux box and this crash just happens with default empty config. I suspect there might be some kind of problem with localization but... any suggestion where I can dig to get more info? I have this crazy idea to give you a remote access :>

#10 - January 30, 2013 02:53 - John Lindgren

If the crashes only started happening recently and you can reliably reproduce them, then it is likely that a recent update to either Audacious or GTK+/GLib is to blame. I would try downgrading each of those packages to see if the problem still happens with an older version.

#11 - January 30, 2013 12:09 - Marcin Kocur

Okay, first of all, 3.3.2 works as expected!

I suspected there is something wrong with translation but reverting /usr/share/locale/pl/LC_MESSAGES/audacious-plugins.mo and /usr/share/locale/pl/LC_MESSAGES/audacious.mo back to 3.3.2 version with 3.3.3 installed didn't fix the problem.

Setting LANG variable to en_US.UTF-8 also doesn't help. The only thing I can say for sure is that 3.3.2 is now playing on my computer without any problems.

#12 - January 31, 2013 00:49 - John Lindgren

- File gthreadinit.diff added

Can you try 3.3.3 with this patch?

#13 - January 31, 2013 01:27 - Marcin Kocur

Core dumped again. I'll prepare a backtrace again...

#14 - January 31, 2013 01:36 - Marcin Kocur

Here you have: http://wklej.org/id/943087/

#15 - January 31, 2013 04:11 - John Lindgren

Let me summarize what we have so far:
1. Version 3.3.3, unpatched, crashes in g_object_newv(): http://wklej.org/id/941107/.
2. Version 3.3.3 + the g_thread_init() patch crashes in plugin2_unload(): http://wklej.org/id/943087/.
3. Version 3.3.2 does not crash.

Is that right?

#16 - January 31, 2013 13:30 - Marcin Kocur

Yeah... but the first one as far as I remember happened while starting, and the second occured while closing audacious, that's why you can be confused. In the evening I'll try to provide something better methodologically organized :)

#17 - February 01, 2013 01:47 - Marcin Kocur

3.3.3 patched, no settings in home dir present, added some files to playlist, crashed while quiting
plugin2_unload (loaded=0x6d4a70) at pluginenum.c:105
http://wklej.org/id/944080/

3.3.3 patched, it's just a next run after attempt above, basic settings in home directory present:
[Inferior 1 (process 4388) exited normally]
http://wklej.org/id/944083/

Then I wanted to break it very badly but couldn't, with settings present audacious exits normally ;)

3.3.3 unpatched, no settings present: it started normally, I added some files to playlist and played, crashed when quitting:
0x0000000000418c57 in _start ()
http://wklej.org/id/944091/

3.3.3 unpatched, no settings present, started normally, I just clicked quit button and got the same:
0x0000000000418c57 in _start ()

3.3.3 unpatched, settings present, started and closed normally

3.3.3 unpatched, complex settings present, crashed while quitting:
#0 0x0000000000418c57 in _start ()
http://wklej.org/id/944097/

After that last crash I can't repeat it with the same settings. Strange.

If you ask me where the g_object_newv() crash came from... sorry, couldn't reproduce it this time. This bugreport is even more odd thanks to that ;]

#18 - February 01, 2013 03:32 - John Lindgren

So, sporadic and varying crashes. It's beginning to sound like memory corruption (which can unfortunately be very difficult to debug).

#19 - February 01, 2013 04:23 - John Lindgren

See if you can capture a crash while running under valgrind:

```
$ valgrind --track-origins=yes audacious 2>valgrind.log
```

#20 - February 01, 2013 20:56 - Marcin Kocur

- File valgrind.log added

Generated from 3.3.3 with patch, no settings, crashed while closing

#21 - February 01, 2013 21:11 - Marcin Kocur

- File valgrind.log.zip added

More detailed log.

#22 - February 01, 2013 23:03 - Marcin Kocur

- File valgrind.log added

Okay, now I do have something interesting... alas! It's glibc-related :/

I've been using 3.3.3 with patch just for daily music listening and the situation described in first message happened again: I can listen only to the track before audacious crashed. Switching to a next one causes another crash.
http://wklej.org/id/944870/

#23 - February 02, 2013 06:00 - John Lindgren

Based on the wide variety of backtraces, the fault probably does not lie in those areas of the code but in some other area that is overwriting memory they use. Sometimes Valgrind can detect that memory corruption but unfortunately did not in this case.

Try using audacious 3.3.3 with audacious-plugins 3.3.2 for a while, and vice versa. That way we can determine whether the problem lies in Audacious core or in some plugin.

#24 - February 02, 2013 18:23 - John Lindgren

This commit could be a fix:
https://github.com/audacious-media-player/audacious-plugins/commit/ce77b1bb7d32a8deca274b5a2f67a9a1ab20cfa1

#25 - February 02, 2013 20:57 - John Lindgren

- Subject changed from Various crashes to Memory corruption

- Category set to plugins/ffaudio

- Status changed from New to Closed

- Target version set to 3.3.4

- % Done changed from 0 to 100

I was able to reproduce the following crash here several times in a row:

```
Program received signal SIGSEGV, Segmentation fault.
plugin2_unload (loaded=0x68f0a0) at pluginenum.c:105
105         switch (header->type)
(gdb) bt
#0  plugin2_unload (loaded=0x68f0a0) at pluginenum.c:105
#1  plugin_system_cleanup () at pluginenum.c:212
#2  0x000000000041b15c in stop_plugins_one () at plugin-init.c:213
#3  0x000000000040ac36 in shut_down () at main.c:527
#4  main (argc=1, argv=0x7fffffffeb98) at main.c:575
```

After commit ce77b1bb, there is no crash, so I am presuming this is fixed.

#26 - February 04, 2013 00:26 - Marcin Kocur

Thank you for your hard work! :) I hope it actually works because I haven't had time to test it yet (exams and so on). I'll let you know as soon as archlinux have the new package in repo.

#27 - February 05, 2013 20:09 - Marcin Kocur

Fixed for me :)

Files

gthreadinit.diff	368 Bytes	January 31, 2013	John Lindgren
valgrind.log	4.62 KB	February 01, 2013	Marcin Kocur
valgrind.log.zip	82.4 KB	February 01, 2013	Marcin Kocur
valgrind.log	4.08 KB	February 01, 2013	Marcin Kocur