Audacious - Bug #599

Playing this stream seg-faults immediately when playing http://s4.viastreaming.net:9040/

November 29, 2015 07:10 - Jim Turner

Status:	Closed	**Start date:**	November 29, 2015
Priority:	Minor	**Due date:**	
Assignee:		**% Done:**	100%
Category:	plugins/adplug	**Estimated time:**	0.00 hour
Target version:	3.7.1		
Affects version:	3.7-beta1		

Description

Attempting to play this particular stream w/AdPlug plugin turned on causes immediate seg-fault. Unchecking AdPlug plays fine. I'm using ALSA with "Default PCM Device". I've included a backtrace which also includes all output from "VVV" option in audacious. Ask me if you need any additional information or would like me to perform any additional tests.

Regards,

Jim

History

#1 - December 02, 2015 06:05 - John Lindgren

I can't reproduce here. The segfault occurred in malloc(), which probably indicates that the heap was already corrupt when the call was made. Can you run within Valgrind and see what errors are logged?

#2 - December 02, 2015 08:53 - Jim Turner

- File x_adplug added

- File x_control added

Sure. Pbm. is is that it doesn't seg-fault under Valgrind, but plays successfully, but with lots of "underrun occurred" and choppy sound (as one might expect under the extra load on an old system). Anyway, I ran both w/Adplug on and with it off for comparison (over 200 errors in both), see attached.

#3 - December 02, 2015 14:49 - John Lindgren

See if this commit helps:
https://github.com/audacious-media-player/audacious-plugins/commit/eb7e35d858889f768173ff98b7fab4764fed3572

Also, have you made changes to the skinned UI? Valgrind reports a use-after-free in main.cc:title_change(), but I can't reproduce it, and the line numbers in the backtrace don't really match up either.

#4 - December 02, 2015 18:34 - Jim Turner

Yes, that seems to have fixed it. Before making your fix, I tried it on another box and it worked there (w/o the fix), so pbm seems to have only been on my main box.

To your question, yes I did make a change a long time ago to fix an issue I was having with some streams where the title would get blanked out after a while in the playlist, if that stream was not the one currently playing. There was also another issue between Audacious's window-title changin' and focusing not playing nice with my window-manager "Afterstep". Those changes, though "hacks" have worked for a long time (for me) and haven't caused my any other issues though (though I recently synced everything up with your latest GIT a cpl. weeks ago):

```
main.cc:
225c225,229
<         mainwin_set_song_title (aud_drct_get_title ());
---
>     {
```

```
>         const char * newtitle = aud_drct_get_title ();   /* JWT:ONLY CHANGE SONG TITLE IF NOT EMPTY! */
>         if (strlen(newtitle) > 0)
>             mainwin_set_song_title (aud_drct_get_title ());
>     }
1109c1113,1115
<     g_signal_connect (w, "window-state-event", (GCallback) state_cb, nullptr);
---
>     gboolean afterstep = aud_get_bool ("skins", "afterstep");  /* JWT:HANDLE OUR RICKITY OL' WINDOWMANAGER (
ie. TO NOT UNSTICK WINDOW ON FOCUS, ETC. */
>     if (! afterstep)   /* Afterstep seems to be broken handling window events */
>         g_signal_connect (w, "window-state-event", (GCallback) state_cb, nullptr);
```

Anyway, it does appear that your fix seems to have worked and that the issue is likely something on my end after all (though I NEVER TOUCHED AdPlug! ;) I did the valgrind test just b4 going to bed and, had you not responded so quickly w/a fix, was going to try rebuilding from scratch w/a clean unmodified GIT download and testing again just to make sure it wasn't something here. Talk a/b quantum entanglement, I hesitated to file this bug, but I was convinced that this was an AdPlug issue. It did not occur to me at first that a change here would've shown up affecting AdPlug, but yes, Audacious and C++ are extremely complex! From now on, I will not report an issue until I've verified that it indeed fails the same way with your GIT! I still wish there was a way to install both your git (in /usr) and my modified ("fauxdacious") version (in /usr/local) at the same time just for sitches like this, but even when configured for the two different locations, they both want to point at certain libs in the same place, so I have to completely uninstall one and rebuild and install the other. So, if you get another bug from me, it should be truly "leGIT!" :D

Go ahead and close this bug as fixed. Thanks again!

Jim

#5 - December 03, 2015 02:12 - John Lindgren

- Status changed from New to Closed

- Target version set to 3.7.1

- % Done changed from 0 to 100

If you change <const char * newtitle> to <String newtitle>, that will fix the use-after-free. As your code is now, the String object returned by aud_drct_get_title gets destroyed too early, and you're left with only a pointer to that (now freed) memory. It's a subtle bug that may not be causing any visible problems now, but so was the AdPlug bug--and "sleeping" bugs like that can suddenly wake up and start causing trouble at a later date, triggered by some unrelated change.

As a side note, it's quite possible to install and run multiple versions of Audacious on the same system; I have half a dozen under /opt right now. All you need to do is set the PKG_CONFIG_PATH variable when compiling the plugins (so that they link to the right libraries) and LD_LIBRARY_PATH when running the alternate version.

Files

audacious_dbg.txt	93.2 KB	November 29, 2015	Jim Turner
x_adplug	225 KB	December 02, 2015	Jim Turner
x_control	220 KB	December 02, 2015	Jim Turner