Audacious - OLD, PLEASE USE GITHUB DISCUSSIONS/ISSUES - Bug #356

NULL pointer segfault due to vfs async race

October 06, 2013 12:41 - Michael Schwendt

Status:	Closed	**Start date:**	October 06, 2013
Priority:	Minor	**Due date:**	
Assignee:		**% Done:**	100%
Category:	plugins/lyricwiki	**Estimated time:**	0.00 hour
Target version:	3.4.2		
Affects version:	3.4.1		

Description

Ran into this with a temporary config which has the lyricswiki plugin enabled. Might be a known issue, since there's a "FIXME" comment in lyricwiki_playback_began() which seems related.

The strcmp() call in the get_lyrics_step_3() async method crashes easily with state.uri being a NULL ptr when lyricwiki_playback_began() unrefs it and resets it to NULL while the vfs async operation hasn't finished yet.

The smallest test-case is to add two unknown .ogg files to the playlist, then start playback and switch between the two tracks forth and back. Lyricswiki redirects to the 40KB edit page, and vfs async access takes more time than switching tracks.

```
Breakpoint 1, get_lyrics_step_3 (buf=0x7fffc4025da0, len=40916,
    requri=0xc88665) at lyricwiki.c:196
196     {
(gdb) print len
$1 = 40916
(gdb) print requri
$2 = (void *) 0xc88665
(gdb) print (char*)requri
$3 = 0xc88665 "http://lyrics.wikia.com/index.php?action=edit&title=index.php?title=Aleksi_Aubry-Ca
rlson:Main+Theme&amp;action=edit"
(gdb) print state
$4 = {
  filename = 0xa1b615 "file:///home/ms19f/Music/INCOMING/after_full_moon_piano.ogg", title = 0xa1b
6d5 "after_full_moon_piano",
  artist = 0x0, uri = 0x0}
(gdb)
```

History

#1 - October 08, 2013 21:20 - John Lindgren

I've been waiting for this to be reported. :(vfs_async has always been a half-baked design.

#2 - October 31, 2013 00:38 - John Lindgren

- Target version set to 3.4.2

- % Done changed from 0 to 100

Going for the quick fix:
https://github.com/audacious-media-player/audacious-plugins/commit/67cea8509a74422e57c123f7321fe9284f02e681
https://github.com/audacious-media-player/audacious-plugins/commit/55b41a09a40b0d14aeb5eee2734097c58244d47d

#3 - October 31, 2013 00:39 - John Lindgren

- Status changed from New to Closed