Audacious - Bug #518

Audacious 3.6 crashes on song change

March 08, 2015 10:42 - Nicholas N

Status:	Closed	**Start date:**	March 08, 2015
Priority:	Major	**Due date:**	
Assignee:		**% Done:**	100%
Category:	libaudcore	**Estimated time:**	0.00 hour
Target version:	3.6.1		
Affects version:	3.6		

Description

System: Linux PMM 3.18.6-1-ARCH #1 SMP PREEMPT Sat Feb 7 08:44:05 CET 2015 x86_64 GNU/Linux
Tested sofware: audacious-plugins-3.6-2-x86_64

Backtrace on crash:
...
Program received signal SIGSEGV, Segmentation fault.
0x00007ffff685fb0e in *strstr_sse2 () from /usr/lib/libc.so.6*
(gdb) set logging off
Done logging to aud-trace.log.
(gdb) bt full
#0 0x00007ffff685fb0e in _strstr_sse2 () from /usr/lib/libc.so.6
No symbol table info available.
#1 0x00007ffff7ba94db in strstr (_needle=0x7ffff7bc9b01 "://", __haystack=0x0) at /usr/include/string.h:336
No locals.
#2 *uri_get_scheme (uri=uri@entry=0x0) at audstrings.cc:590*
No locals.
#3 *0x00007ffff7bc5097 in VFSFile::VFSFile (this=0x7fffffffdba0, filename=0x0, mode=0x7fffd83c5da6 "r") at vfs.cc:63*
scheme = {stack = 0x7fffffffdbb0, m_data = 0x7ffff7bab470 <add_cb(void const, void*)>*
"AUATUSH\211\365H\203\354\030dH\213\004%(", m_len = 6627328}
sub = 0x7fffffffdbb0 ""
nosub = {stack = 0x7fffffffdb80, m_data = 0xd8b94cca183aeb00 <error: Cannot access memory at address 0xd8b94cca183aeb00>,
m_len = 16288448}
#4 *0x00007fffd83bf651 in equalizerwin_read_aud_preset (filename=filename@entry=0x0) at ui_equalizer.cc:435*
preset = {name = {raw = 0x0}, preamp = 2.41585812e-24, bands = {-1.62991566e+15, -6.31313253e+26, 0, -8.28228877e+14,
4.59163468e-41, -8.28334573e+14, 4.59163468e-41, 0, 0, -8.9908515e+33}}
file = {m_filename = {raw = 0x0}, m_error = {raw = 0x0}, m_impl = {ptr = 0x0}}
#5 *0x00007fffd83bf8f1 in load_auto_preset (filename=0x0) at ui_equalizer.cc:470*
eq_file = 0x0
success = <optimized out>
folder = <optimized out>
base = <optimized out>
#6 *playback_begin_cb () at ui_equalizer.cc:497*
No locals.
#7 *0x00007ffff7baf1c4 in hook_call (name=<optimized out>, data=0x0) at hook.cc:112*
item = {func = 0x7fffd83bf870 <playback_begin_cb(void, void*)>, user = 0x0}*
i = 1
key = {raw = 0xf82b05 "playback begin"}
#8 *0x00007ffff7bb95f9 in playlist_next_song (playlist_num=0, repeat=<optimized out>) at playlist.cc:2077*
playlist = <optimized out>
hint = <optimized out>
change = NextSong
#9 *0x00007ffff7bac5d5 in aud_drct_pl_next () at drct.cc:116*
playlist = <optimized out>
#10 *0x00007fffd83bc6b5 in seek_release (rewind=0, event=<optimized out>, widget=<optimized out>) at ui_main.cc:616*
No locals.
#11 *0x00007fffd83b6709 in button_release (button=0xe181c0, event=0x1016330) at ui_skinned_button.cc:112*
data = 0xf85430
__PRETTY_FUNCTION__ = "gboolean button_release(GtkWidget*, GdkEventButton*)"
#12 0x00007fffe646590f in ?? () from /usr/lib/libgtk-x11-2.0.so.0
No symbol table info available.

#13 0x00007ffff73c3175 in g_closure_invoke () from /usr/lib/libgobject-2.0.so.0
No symbol table info available.
#14 0x00007ffff73d4a5c in ?? () from /usr/lib/libgobject-2.0.so.0
No symbol table info available.
#15 0x00007ffff73dd205 in g_signal_emit_valist () from /usr/lib/libgobject-2.0.so.0
No symbol table info available.
#16 0x00007ffff73dd95f in g_signal_emit () from /usr/lib/libgobject-2.0.so.0
No symbol table info available.
#17 0x00007fffe657cb9c in ?? () from /usr/lib/libgtk-x11-2.0.so.0
No symbol table info available.
#18 0x00007fffe6464054 in gtk_propagate_event () from /usr/lib/libgtk-x11-2.0.so.0
No symbol table info available.
#19 0x00007fffe64644eb in gtk_main_do_event () from /usr/lib/libgtk-x11-2.0.so.0
No symbol table info available.
#20 0x00007fffe60d92cc in ?? () from /usr/lib/libgdk-x11-2.0.so.0
No symbol table info available.
#21 0x00007ffff70ee71d in g_main_context_dispatch () from /usr/lib/libglib-2.0.so.0
No symbol table info available.
#22 0x00007ffff70eea08 in ?? () from /usr/lib/libglib-2.0.so.0
No symbol table info available.
#23 0x00007ffff70eed32 in g_main_loop_run () from /usr/lib/libglib-2.0.so.0
No symbol table info available.
#24 0x00007fffe6463467 in gtk_main () from /usr/lib/libgtk-x11-2.0.so.0
No symbol table info available.
#25 0x00007ffff7bb0128 in interface_run () at interface.cc:166
No locals.
#26 0x00007ffff7bc11e8 in aud_run () at runtime.cc:320
autosave = {serial = 1, _running = true}
#27 0x0000000004052fc in main (argc=<optimized out>, argv=<optimized out>) at main.cc:370
FUNCTION = "main"

Here is log of gdb:

Starting program: /usr/bin/audacious
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/usr/lib/libthread_db.so.1".
[New Thread 0x7fffefffff700 (LWP 28834)]
[New Thread 0x7ffff4b2b700 (LWP 28833)]
[New Thread 0x7ffff532c700 (LWP 28832)]
[New Thread 0x7fffec9a3700 (LWP 28836)]
[Thread 0x7ffff4b2b700 (LWP 28833) exited]
[New Thread 0x7fffe7dfb700 (LWP 28872)]
[New Thread 0x7fffcfffe700 (LWP 28841)]
[New Thread 0x7fffe175a700 (LWP 28838)]

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff685fb0e in __strstr_sse2 () from /usr/lib/libc.so.6

History

#1 - March 09, 2015 15:50 - Thomas Lange

I could reproduce the segfault when using the Winamp interface and enabled auto presets.
Until it is fixed you should disable auto presets (AUTO button in the equalizer window).

#2 - March 09, 2015 16:15 - Nicholas N

Thomas Lange wrote:

> I could reproduce the segfault when using the Winamp interface and enabled auto presets.
> Until it is fixed you should disable auto presets (AUTO button in the equalizer window).

I'm simply using 3.5.2 version.

#3 - March 10, 2015 23:54 - John Lindgren

- Category set to libaudcore

- Status changed from New to Closed

- Target version set to 3.6.1

- % Done changed from 0 to 100

Fixed.