

Audacious - OLD, PLEASE USE GITHUB DISCUSSIONS/ISSUES - Bug #554

Crash in QCocoaMenuBar when switching UI (OS X)

June 19, 2015 20:49 - Ariadne Conill

Status:	Rejected	Start date:	June 19, 2015
Priority:	Minor	Due date:	
Assignee:		% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:			
Affects version:			
Description			
When switching interfaces, if the new interface fails to start, Audacious crashes with a null dereference.			
Presumably it should attempt to recover by switching back to the old interface. An example for reproducing this issue would be to try to switch to the new skins-qt plugin without having any skins installed.			

History

#1 - June 20, 2015 00:18 - John Lindgren

I can't reproduce this on latest Git master. What is the backtrace?

I see:

```
WARNING skin.cc:276 [skin_load]: Unable to load skin (/usr/share/audacious/Skins/Refugee).
WARNING skin.cc:276 [skin_load]: Unable to load skin (/usr/share/audacious/Skins/Default).
ERROR plugin.cc:101 [load_initial_skin]: Unable to load any skin; giving up!
ERROR plugin-init.cc:251 [enable_single]: Winamp Classic Interface failed to start; falling back to Qt Interface.
```

And then the Qt UI comes back as it should.

#2 - June 20, 2015 00:43 - Ariadne Conill

```
INFO plugin-init.cc:233 [enable_single]: Switching from Qt Interface to Winamp Classic Interface.
INFO interface.cc:86 [interface_unload]: Unloading Qt Interface.
INFO plugin-init.cc:233 [enable_single]: Switching from Qt Interface to Winamp Classic Interface.
ERROR plugin-init.cc:251 [enable_single]: Winamp Classic Interface failed to start; falling back to Qt Interface.
INFO interface.cc:69 [interface_load]: Loading Qt Interface.
Process 19158 stopped
* thread #1: tid = 0x143f32b9, 0x0000000010122074a QtCore`QMetaObject::cast(QObject*) const + 26, queue = 'com.apple.main-thread', stop reason = EXC_BAD_ACCESS (code=EXC_I386_GPFLT)
    frame #0: 0x0000000010122074a QtCore`QMetaObject::cast(QObject*) const + 26
QtCore`QMetaObject::cast:
-> 0x10122074a <+26>: callq    *(%rax)
    0x10122074c <+28>: movq    %rax, %rcx
```

```

    0x10122074f <+31>: xorl    %eax, %eax
    0x101220751 <+33>: nopw    %cs:(%rax,%rax)
(lldb) bt all
* thread #1: tid = 0x143f32b9, 0x000000010122074a QtCore`QMetaObject::cast(QObject*) const + 26, queue = 'com.apple.main-thread', stop reason = EXC_BAD_ACCESS (code=EXC_I386_GPFLT)
  * frame #0: 0x000000010122074a QtCore`QMetaObject::cast(QObject*) const + 26
    frame #1: 0x00000001077f89de libqcocoa.dylib`QtPrivate::QVariantValueHelper<QObject*>::object(QVariant const&) + 94
      frame #2: 0x00000001077f9431 libqcocoa.dylib`QCocoaMenuItem::sync() + 945
      frame #3: 0x00000001077f7796 libqcocoa.dylib`QCocoaMenu::syncMenuItem(QPlatformMenuItem*) + 454
      frame #4: 0x00000001077fbbb6 libqcocoa.dylib`QCocoaMenuBar::syncMenu(QPlatformMenuItem*) + 358
      frame #5: 0x00000001077fac0b libqcocoa.dylib`QCocoaMenuBar::updateMenuBarImmediately() + 411
      frame #6: 0x0000000107832bb1 libqcocoa.dylib`QCocoaNativeInterface::qt_static_metacall(QObject*, QMetaObject::Call, int, void**) + 65
      frame #7: 0x000000010124d7ab QtCore`QMetaObject::activate(QObject*, int, int, void**) + 2987
      frame #8: 0x0000000100a58a3d QtGui`QGuiApplicationPrivate::processActivatedEvent(QWindowSystemInterfacePrivate::ActivatedWindowEvent*) + 765
      frame #9: 0x0000000100a54ef5 QtGui`QGuiApplicationPrivate::processWindowSystemEvent(QWindowSystemInterfacePrivate::WindowSystemEvent*) + 1525
      frame #10: 0x0000000100a422da QtGui`QWindowSystemInterface::sendWindowSystemEvents(QFlags<QEventLoop::ProcessEventsFlag>) + 346
      frame #11: 0x00000001077f3411 libqcocoa.dylib`QCocoaEventDispatcherPrivate::postedEventsSourceCallback(void*) + 33
      frame #12: 0x00007fff8946ea01 CoreFoundation`__CFRunLoop_IS_CALLING_OUT_TO_A_SOURCE0_PERFORM_FUNCTION__ + 17
      frame #13: 0x00007fff89460c5c CoreFoundation`__CFRunLoopDoSources0 + 476
      frame #14: 0x00007fff894601bf CoreFoundation`__CFRunLoopRun + 927
      frame #15: 0x00007fff8945fbd8 CoreFoundation`CFRunLoopRunSpecific + 296
      frame #16: 0x00007fff9049656f HIToolbox`RunCurrentEventLoopInMode + 235
      frame #17: 0x00007fff904961ee HIToolbox`ReceiveNextEventCommon + 179
      frame #18: 0x00007fff9049612b HIToolbox`BlockUntilNextEventMatchingListInModeWithFilter + 71
      frame #19: 0x00007fff840af9bb AppKit`_DPSNextEvent + 978
      frame #20: 0x00007fff840aef68 AppKit`-[NSApplication nextEventMatchingMask:untilDate:inMode:dequeue:] + 34
6
      frame #21: 0x00007fff840a4bf3 AppKit`-[NSApplication run] + 594
      frame #22: 0x00000001077f22fd libqcocoa.dylib`QCocoaEventDispatcher::processEvents(QFlags<QEventLoop::ProcessEventsFlag>) + 2189
      frame #23: 0x000000010121837d QtCore`QEventLoop::exec(QFlags<QEventLoop::ProcessEventsFlag>) + 381
      frame #24: 0x000000010121b35a QtCore`QCoreApplication::exec() + 346
      frame #25: 0x0000000100041e0f libaudcore.3.dylib`interface_run() + 159 at interface.cc:166
      frame #26: 0x0000000100057827 libaudcore.3.dylib`aud_run() + 55 at runtime.cc:321
      frame #27: 0x000000010000133a audacious`main(argc=2, argv=<unavailable>) + 1930 at main.cc:374
      frame #28: 0x00007fff8d9a55c9 libdyld.dylib`start + 1

thread #2: tid = 0x143f34c3, 0x00007fff8993775a libsystem_kernel.dylib`__sigwait + 10
  frame #0: 0x00007fff8993775a libsystem_kernel.dylib`__sigwait + 10
  frame #1: 0x00007fff89898c8e libsystem_pthread.dylib`sigwait + 61
  frame #2: 0x00000001000017aa audacious`signal_thread(data=<unavailable>) + 26 at signals.cc:35
  frame #3: 0x00007fff89895268 libsystem_pthread.dylib`_pthread_body + 131
  frame #4: 0x00007fff898951e5 libsystem_pthread.dylib`_pthread_start + 176
  frame #5: 0x00007fff8989341d libsystem_pthread.dylib`thread_start + 13

thread #3: tid = 0x143f34c4, 0x00007fff89938232 libsystem_kernel.dylib`kevent64 + 10, queue = 'com.apple.libdispatch-manager'
  frame #0: 0x00007fff89938232 libsystem_kernel.dylib`kevent64 + 10
  frame #1: 0x00007fff8a0a8d91 libdispatch.dylib`_dispatch_mgr_invoke + 247
  frame #2: 0x00007fff8a0a8a6a libdispatch.dylib`_dispatch_mgr_thread + 52

thread #4: tid = 0x143f34c5, 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
  frame #0: 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
  frame #1: 0x00007fff898956c3 libsystem_pthread.dylib`_pthread_wqthread + 869
  frame #2: 0x00007fff8989340d libsystem_pthread.dylib`start_wqthread + 13

thread #6: tid = 0x143f34c7, 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
  frame #0: 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
  frame #1: 0x00007fff898956c3 libsystem_pthread.dylib`_pthread_wqthread + 869
  frame #2: 0x00007fff8989340d libsystem_pthread.dylib`start_wqthread + 13

thread #8: tid = 0x143f34c9, 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
  frame #0: 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
  frame #1: 0x00007fff898956c3 libsystem_pthread.dylib`_pthread_wqthread + 869
  frame #2: 0x00007fff8989340d libsystem_pthread.dylib`start_wqthread + 13

thread #9: tid = 0x143f34d2, 0x00007fff89937136 libsystem_kernel.dylib`__psynch_cvwait + 10
  frame #0: 0x00007fff89937136 libsystem_kernel.dylib`__psynch_cvwait + 10

```

```

    frame #1: 0x00007fff89895e0c libsystem_pthread.dylib`_pthread_cond_wait + 693
    frame #2: 0x00000001016d0f2b coreaudio.bundle`CoreAudioPlugin::period_wait(this=<unavailable>) + 155 at co
reaudio.cc:385
    frame #3: 0x0000000100044b75 libaudcore.3.dylib`write_output_raw(data=<unavailable>) + 549 at output.cc:25
3
    frame #4: 0x0000000100044062 libaudcore.3.dylib`output_write_audio(void const*, int, int) [inlined] write_
output(data=0x0000000100000000, size=1065353216, stop_time=<unavailable>) + 946 at output.cc:286
    frame #5: 0x0000000100043e3e libaudcore.3.dylib`output_write_audio(data=0x0000000100000000, size=106535321
6, stop_time=<unavailable>) + 398 at output.cc:369
    frame #6: 0x0000000100045cd1 libaudcore.3.dylib`InputPlugin::write_audio(data=0x000000010545bdb8, length=1
6384) + 113 at playback.cc:556
    frame #7: 0x00000001023dd55c madplug.bundle`MPG123Plugin::play(this=<unavailable>, filename=0x000000010222
1935, file=0x000000010007b5b8) + 908 at mpg123.cc:362
    frame #8: 0x00000001000456f7 libaudcore.3.dylib`playback_thread(void*) + 43 at playback.cc:338
    frame #9: 0x00000001000456cc libaudcore.3.dylib`playback_thread((null)=<unavailable>) + 1276 at playback.c
c:409
    frame #10: 0x00007fff89895268 libsystem_pthread.dylib`_pthread_body + 131
    frame #11: 0x00007fff898951e5 libsystem_pthread.dylib`_pthread_start + 176
    frame #12: 0x00007fff8989341d libsystem_pthread.dylib`thread_start + 13

thread #12: tid = 0x143f3585, 0x00007fff899324de libsystem_kernel.dylib`mach_msg_trap + 10
    frame #0: 0x00007fff899324de libsystem_kernel.dylib`mach_msg_trap + 10
    frame #1: 0x00007fff8993164f libsystem_kernel.dylib`mach_msg + 55
    frame #2: 0x00007fff89460eb4 CoreFoundation`__CFRunLoopServiceMachPort + 212
    frame #3: 0x00007fff8946037b CoreFoundation`__CFRunLoopRun + 1371
    frame #4: 0x00007fff8945fbd8 CoreFoundation`CFRunLoopRunSpecific + 296
    frame #5: 0x00007fff8417766b AppKit`_NSEventThread + 137
    frame #6: 0x00007fff89895268 libsystem_pthread.dylib`_pthread_body + 131
    frame #7: 0x00007fff898951e5 libsystem_pthread.dylib`_pthread_start + 176
    frame #8: 0x00007fff8989341d libsystem_pthread.dylib`thread_start + 13

thread #13: tid = 0x143f38d1, 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
    frame #0: 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
    frame #1: 0x00007fff898956c3 libsystem_pthread.dylib`_pthread_wqthread + 869
    frame #2: 0x00007fff8989340d libsystem_pthread.dylib`start_wqthread + 13

thread #14: tid = 0x143f38d2, 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
    frame #0: 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
    frame #1: 0x00007fff898956c3 libsystem_pthread.dylib`_pthread_wqthread + 869
    frame #2: 0x00007fff8989340d libsystem_pthread.dylib`start_wqthread + 13

thread #15: tid = 0x143f38d3, 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
    frame #0: 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
    frame #1: 0x00007fff898956c3 libsystem_pthread.dylib`_pthread_wqthread + 869
    frame #2: 0x00007fff8989340d libsystem_pthread.dylib`start_wqthread + 13

thread #16: tid = 0x143f38de, 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
    frame #0: 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
    frame #1: 0x00007fff898956c3 libsystem_pthread.dylib`_pthread_wqthread + 869
    frame #2: 0x00007fff8989340d libsystem_pthread.dylib`start_wqthread + 13

thread #17: tid = 0x143f38df, 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
    frame #0: 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
    frame #1: 0x00007fff898956c3 libsystem_pthread.dylib`_pthread_wqthread + 869
    frame #2: 0x00007fff8989340d libsystem_pthread.dylib`start_wqthread + 13

thread #18: tid = 0x143f38e2, 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
    frame #0: 0x00007fff8993794a libsystem_kernel.dylib`__workq_kernreturn + 10
    frame #1: 0x00007fff898956c3 libsystem_pthread.dylib`_pthread_wqthread + 869
    frame #2: 0x00007fff8989340d libsystem_pthread.dylib`start_wqthread + 13
(11ldb)

```

#3 - June 20, 2015 00:47 - Ariadne Conill

If you were wondering, ``%rax` is a nullptr.

#4 - June 20, 2015 04:18 - John Lindgren

Does this commit help?

<https://github.com/audacious-media-player/audacious/commit/ff06739ec7f0886e823ed356b998a587ce10d8c8>

#5 - June 20, 2015 04:44 - Ariadne Conill

No, I am still seeing the same backtrace on a clean build.

#6 - June 20, 2015 07:00 - John Lindgren

That's unfortunate. My guess is, it's a bug in Qt.

#7 - June 20, 2015 07:03 - John Lindgren

- *Subject changed from Audacious 3.7-devel crashes when a new interface fails to start to Audacious 3.7-devel crashes when a new interface fails to start (OS X only)*

#8 - September 21, 2015 22:26 - John Lindgren

- *Subject changed from Audacious 3.7-devel crashes when a new interface fails to start (OS X only) to Crash in QCocoaMenuBar when switching UI (OS X)*

#9 - January 29, 2017 19:39 - John Lindgren

- *Status changed from New to Rejected*

Closing OS X-specific bugs since development on that OS seems to have stalled.