Smuxi - Bug # 806: Crash when connecting to smuxi-server on Windows

Status:	Closed	**Priority:**	Immediate
Author:	Mirco Bauer	**Category:**	Frontend GNOME
Created:	01/28/2013	**Assigned to:**	Mirco Bauer
Updated:	05/20/2013	**Due date:**	
Complexity:	High		
Found in Version:	0.8.11-dev (2013-01-13)		
Subject:	Crash when connecting to smuxi-server on Windows		
Description:			

Associated revisions

05/20/2013 10:17 PM - Mirco Bauer

[Win32-Installer] Bumped minimum GTK# version to 2.12.20 to fix crash with vertical tabs (closes: #806)

History

01/28/2013 04:26 AM - Mirco Bauer

- File smuxi-crash.png added

- Priority changed from Normal to Immediate

01/28/2013 04:36 AM - Mirco Bauer

- Found in Version changed from 0.8.11-dev (2013-01-28) to 0.8.11-dev (2013-01-13)

OS: Windows 7 64-bit

01/28/2013 08:10 AM - Mirco Bauer

<pre>

0:000> ~* kp

. 0 Id: 163c.de0 Suspend: 0 Teb: 7efdd000 Unfrozen

ChildEBP RetAddr

0024d228 77e4d564 ntdll!ZwTerminateProcess+0x12

0024d244 75d77362 ntdll!RtlExitUserProcess+0x85

0024d258 714242f0 KERNEL32!ExitProcessStub+0x12

0024d4c8 71431f25 mscoreei!RuntimeDesc::ShutdownAllActiveRuntimes+0x29c

0024d4dc 714986ad mscoreei!CorExitProcess+0x26

0024d4f0 765709c8 MSCOREE!ShellShim_CorExitProcess+0x94

0024d4fc 765aa79c msvcrt!__crtCorExitProcess+0x29

0024d534 765cb2f1 msvcrt!_cinit+0x62

0024d548 765c8f7b msvcrt!_exit+0x11

*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Program Files (x86)\GtkSharp\2.12\bin\libglib-2.0-0.dll -

0024d880 68610083 msvcrt!abort+0x116

*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Program Files (x86)\GtkSharp\2.12\bin\libgdk-win32-2.0-0.dll -

WARNING: Stack unwind information not available. Following frames may be wrong.

0024d900 6c378375 libglib_2_0_0!g_assertion_message+0xf3

0024d940 6c378948 libgdk_win32_2_0_0!gdk_fontset_load_for_display+0x7f5

*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Program Files (x86)\GtkSharp\2.12\lib\gtk-2.0\2.10.0\engines\libwimp.dll -

0024d9a0 053e8e64 libgdk_win32_2_0_0!gdk_win32_hdc_get+0x58

0024da20 053e4441 libwimp!theme_init+0x484

*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Program Files (x86)\GtkSharp\2.12\bin\libgtk-win32-2.0-0.dll -

0024db20 6188bd1c libwimp+0x4441

0024dba0 6188c5a6 libgtk_win32_2_0_0!gtk_notebook_new+0x4fec

0024dc50 61868e63 libgtk_win32_2_0_0!gtk_notebook_new+0x5876

*** ERROR: Symbol file could not be found. Defaulted to export symbols for C:\Program Files (x86)\GtkSharp\2.12\bin\libgobject-2.0-0.dll -
0024dc90 0438404a libgtk_win32_2_0_0!gtk_marshal_BOOLEAN__VOID+0x41b3
0024dd10 0439758c libgobject_2_0_0!g_closure_invoke+0xca
0024de00 0439892b libgobject_2_0_0!g_signal_handlers_destroy+0xa6c
0024df30 04398fc6 libgobject_2_0_0!g_signal_emit_valist+0x62b
0024df50 61985ec1 libgobject_2_0_0!g_signal_emit+0x26
0024dfa0 617d38cb libgtk_win32_2_0_0!gtk_widget_class_list_style_properties+0x451
0024dff0 617d5808 libgtk_win32_2_0_0!gtk_container_propagate_expose+0x1ab
0024e010 6179dfcd libgtk_win32_2_0_0!gtk_container_child_type+0x198
0024e050 617d44f7 libgtk_win32_2_0_0!gtk_box_pack_start_defaults+0xc0d
0024e080 617d57a3 libgtk_win32_2_0_0!gtk_container_forall+0x87
0024e0c0 61868e63 libgtk_win32_2_0_0!gtk_container_child_type+0x133
0024e100 0438404a libgtk_win32_2_0_0!gtk_marshal_BOOLEAN__VOID+0x41b3
0024e180 0439758c libgobject_2_0_0!g_closure_invoke+0xca
0024e270 0439892b libgobject_2_0_0!g_signal_handlers_destroy+0xa6c
0024e3a0 04398fc6 libgobject_2_0_0!g_signal_emit_valist+0x62b
0024e3c0 61985ec1 libgobject_2_0_0!g_signal_emit+0x26
0024e410 617d38cb libgtk_win32_2_0_0!gtk_widget_class_list_style_properties+0x451
0024e460 617d5808 libgtk_win32_2_0_0!gtk_container_propagate_expose+0x1ab
0024e480 617d44f7 libgtk_win32_2_0_0!gtk_container_child_type+0x198
0024e4b0 617d57a3 libgtk_win32_2_0_0!gtk_container_forall+0x87
0024e4f0 61868e63 libgtk_win32_2_0_0!gtk_container_child_type+0x133
0024e530 04384124 libgtk_win32_2_0_0!gtk_marshal_BOOLEAN__VOID+0x41b3
0024e5b0 0439758c libgobject_2_0_0!g_closure_invoke+0x1a4
0024e6a0 0439892b libgobject_2_0_0!g_signal_handlers_destroy+0xa6c
0024e7d0 04398fc6 libgobject_2_0_0!g_signal_emit_valist+0x62b
0024e7f0 61985ec1 libgobject_2_0_0!g_signal_emit+0x26
0024e840 618623b4 libgtk_win32_2_0_0!gtk_widget_class_list_style_properties+0x451
0024e8a0 6c35c271 libgtk_win32_2_0_0!gtk_main_do_event+0x5c4
0024e940 6c35cbe8 libgdk_win32_2_0_0!gdk_window_is_viewable+0x231
0024e980 617d490e libgdk_win32_2_0_0!gdk_window_process_all_updates+0x108
0024e9c0 6c34150d libgtk_win32_2_0_0!gtk_container_check_resize+0x37e
0024e9e0 685eb50b libgdk_win32_2_0_0!gdk_threads_add_timeout_seconds+0xbd
0024ea60 685ee5f5 libglib_2_0_0!g_main_context_dispatch+0x19b
0024eae0 685ee9e4 libglib_2_0_0!g_main_context_prepare+0x895
0024eb20 618625dc libglib_2_0_0!g_main_loop_run+0x164
0024ec24 678421bb libgtk_win32_2_0_0!gtk_main+0xac
0024ec28 6784e0a1 clr!CallDescrWorker+0x33
0024ecdc 6786c283 clr!SigParser::GetElemType+0x28
0024ecf4 0024eddc clr!MetaSig::MetaSig+0x3c
0024ed68 6784e9d9 0x24eddc
0024edd0 00000000 clr!MethodDesc::GetSigFromMetadata+0x21

</pre>

01/29/2013 04:27 AM - Mirco Bauer

<pre>
04:18:23 <meebey> ohhh I found something, Gdk.Pixbuf used in non-GUI thread, I wonder I wonder if that is what makes it crash
04:18:46 <meebey> GDK is supposed to be thread-safe but this looks like a candidate
04:19:50 <meebey> blez`: on windows or in general?
04:20:12 <meebey> ServerIconPixbuf = new Gdk.Pixbuf(iconPath, 16, 16);
04:20:12 <meebey> GLib.Idle.Add(delegate {
04:20:12 <meebey> TabImage.Pixbuf = ServerIconPixbuf;

04:20:30 <meebey> I will simply move that Gdk.Pixbuf line into the GUI thread scope
04:20:36 <meebey> and see if the crash goes away
04:24:43 <meebey> OOOOOOOH!!!
04:24:55 <meebey> "Unfortunately the above holds with the X11 backend only. With the Win32 backend, GDK calls should not be attempted from multiple threads at all."
04:24:57 <meebey> FUCK! :)
04:25:18 <meebey> GDK is thread-safe only Linux-only, lol
04:25:25 <meebey> so I guess I found the crasher
04:25:36 <meebey> thats straight from GTK+ docs: http://developer.gnome.org/gdk/unstable/gdk-Threads.html
</pre>

05/20/2013 12:37 PM - Mirco Bauer

The issue doesn't seem to happen with a daily build from 2012-09-09

05/20/2013 02:59 PM - Mirco Bauer

Regression happened somewhere between the 2012-09-09 and 2013-01-13:
git log --stat 7e42694c49ecfef2c346a448f5e3346165e29a92..918ef3ef4feb7955660b48be7bc9b1bbcfed6d8b -- src/Frontend-GNOME/

05/20/2013 10:13 PM - Mirco Bauer

This is a bug in the GTK+ theme engine triggered by vertical tabs. With horizontal tabs it works just fine. Thus is not a Smuxi regression! This issue happens on GTK# 2.12.10 and works fine on GTK# 2.12.20, thus I am going to fix this issue by bumping the minimum required GTK# version to 2.12.20

05/20/2013 11:33 PM - Mirco Bauer

- Status changed from New to Closed

- % Done changed from 0 to 100

Applied in changeset commit:"bf5cbd6db2a34efb78bb16dd2dbb176b0aa3ba33".

Files

smuxi-crash.png	61.8 KB	01/28/2013	Mirco Bauer