Ruby trunk - Bug #8000

"require 'tk'" segfaults on 64-bit linux with Tk 8.6

03/02/2013 02:43 PM - edmccard (Ed McCardell)

Status:	Closed		
Priority:	Normal		
Assignee:	nagai (Hidetoshi Nagai)		
Target version:			
ruby -v:	ruby 1.9.3p392 (2013-02-22 revision 39386) [x86_64-linux]	**Backport:**	2.0.0: REQUIRED, 2.1: DONE

Description

Using ruby 1.9.3p392 and Tk 8.6.0 on 64-bit Arch Linux, attempting to "require 'tk'" causes a segfault.

To reproduce:
ruby -e "require 'tk'"

The crash log is in the attached file.

Notes:

- I've heard from a Gentoo user who is having the same problem.
- On 32-bit Arch Linux, there is no problem.

Related issues:

Related to Backport200 - Backport #10400: Ruby/Tk patch for Tcl/Tk8.6	**Rejected**	
Related to Backport193 - Backport #10399: Ruby/Tk patch for Tcl/Tk8.6	**Rejected**	**10/19/2014**
Related to Backport21 - Backport #10401: Ruby/Tk patch for Tcl/Tk8.6	**Closed**	

History

#1 - 03/04/2013 02:49 PM - jonforums (Jon Forums)

Did you build tcltk, or install binaries via pacman? This seems wacky if you used pacman, but does file prove /usr/lib/libtcl8.6.so and /usr/lib/libtk8.6.so are 64bit?

Since it crashes so easily, fire up gdb via something like

gdb --args ruby -e "require 'tk'"

run it, and attach the backtrace.

#2 - 03/06/2013 04:25 AM - ponimas (Alexander Ponimaskin)

- File bt.txt added

All packages are installed via packman

/usr/lib/libtcl8.6.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, BuildID[sha1]=0x31a66c5d6eacb77f2a9a220bff2e78a88821167e, not stripped

/usr/lib/libtk8.6.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, BuildID[sha1]=0xdfa2df7ef1e30e3fbe510a294f8fe781415ee964, not stripped

#3 - 03/08/2013 07:45 AM - jonforums (Jon Forums)

One of the committers please assign this to Hidetoshi NAGAI.

Too bad tcltklib.so is stripped and the bt is weak. I bet no one on ruby-core has an Arch x64 system to try to repro/debug the issue, so we need to get better debug info. (Or reproduce it on a Ubuntu x64 system)

Are you able to build ruby? If you did a pacman install of Arch's ruby 1.9.3_p392 package, you should be able to build from source, and tweak configure's optflags and debugflags to build tcltklib.so with debug info. The default install is to /usr/local so your Arch pkg won't get clobbered if you don't use --prefix.

My Arch x64 system is cmd line only. When I tried to cheat a repro/debug by installing tcl/tk add it's 15 friends, ruby -e "require 'tk'" rightfully failed due to no display. I don't know whether it failed before or after your segv. When I get time, I'll standup a new ArchBang install and try again. It looks as if

tcltklib.so could be passing a bad value into the tcl library. Hard to tell from the bt.

Before you try building from source have you pinged the Arch Forum? I'd skimmed posts on Newbie Corner and Installation and didn't see mention of this issue. Have you contacted Arch's ruby packager (Thomas Dziedzic) to confirm whether he's seeing the issue? Given it fails so quickly, I was surprised not to find it in the forums.

Then again, Nagai-san may soon see this issue and swoop in with the solution ;)

#4 - 03/08/2013 02:08 PM - nagai (Hidetoshi Nagai)

First of all, current Ruby/Tk cannot support Tcl/Tk8.6. Please see [ruby-talk:395829].
But, I don't know whether this trouble belongs to the "tailcall" problem or not.
Does the same trouble occur with Tcl/Tk8.5 ? If so, tcltklib may not follow the changes on Ruby's core.

Of course, I must fix this bug and should support Tcl/Tk8.6.
However, I don't have enough time to work on it,
and unfortunately I have no idea to avoid the "tailcall" problem now.

#5 - 03/08/2013 04:25 PM - edmccard (Ed McCardell)

Jon: I've just posted to Newbie Corner on the Arch forums. The only other place on the internet that I've seen this is in the forums for the Coursera Programming languages class I'm taking, where several other users have reported it. I'll build ruby/tcl/tk from source tonight with debug info and get a better trace.

Nagai-san: Using the latest version of Arch linux ruby that was built against Tcl/Tk 8.5 works fine (that's ruby 1.9.3 p127). I don't know about the tailcall problem, but on 32-bit Arch linux with Tcl/Tk 8.6, the ruby/tk scripts I run are working without segfault.

#6 - 03/08/2013 05:55 PM - edmccard (Ed McCardell)

- File bt-debug.txt added

Now that I've tried a few more ruby/tk scripts, I see that only a limited subset of tk works on 32-bit under Tk8.6. But in case it's still useful, I've attached a backtrace from gdb using ruby1.9.3p392/tcl8.6/tk8.6 with debug info on 64-bit.

#7 - 03/08/2013 11:24 PM - jonforums (Jon Forums)

> First of all, current Ruby/Tk cannot support Tcl/Tk8.6. Please see [ruby-talk:395829].
> But, I don't know whether this trouble belongs to the "tailcall" problem or not.

Nagai-san: thanks for the info. FYI, while it's not really relevant to Ed's Arch issue, I'm running Tcl/Tk8.6 on Win7 32bit on ruby 1.9.3p393 and ruby 2.0.0p19 built with mingw-w64 4.7.2 and I've not yet seen any problems with test scripts like http://pastie.org/6420781

#8 - 03/19/2013 10:53 AM - nagai (Hidetoshi Nagai)

Could you test the following script?

---

module TkCore; RUN_EVENTLOOP_ON_MAIN_THREAD = true; end
require 'tk'
Tk.mainloop

If it works, a bug may exist on handling a Thread.

From: "edmccard (Ed McCardell)" edmccard@hotmail.com
Subject: [ruby-core:53226] [ruby-trunk - Bug #8000] "require 'tk'" segfaults on 64-bit linux with Tk 8.6
Date: Fri, 8 Mar 2013 17:55:30 +0900
Message-ID: redmine.journal-37386.20130308175529@ruby-lang.org

> Issue #8000 has been updated by edmccard (Ed McCardell).
>
> File bt-debug.txt added
>
> ## Now that I've tried a few more ruby/tk scripts, I see that only a limited subset of tk works on 32-bit under Tk8.6. But in case it's still useful, I've attached a backtrace from gdb using ruby1.9.3p392/tcl8.6/tk8.6 with debug info on 64-bit.
>
> Bug #8000: "require 'tk'" segfaults on 64-bit linux with Tk 8.6
> https://bugs.ruby-lang.org/issues/8000#change-37386

Author: edmccard (Ed McCardell)
Status: Open
Priority: Normal
Assignee:
Category:
Target version:
ruby -v: ruby 1.9.3p392 (2013-02-22 revision 39386) [x86_64-linux]

Using ruby 1.9.3p392 and Tk 8.6.0 on 64-bit Arch Linux, attempting to "require 'tk'" causes a segfault.

To reproduce:
ruby -e "require 'tk'"

The crash log is in the attached file.

Notes:

- I've heard from a Gentoo user who is having the same problem.
- On 32-bit Arch Linux, there is no problem.

--
http://bugs.ruby-lang.org/

#9 - 03/19/2013 11:09 AM - edmccard (Ed McCardell)

That script,

module TkCore; RUN_EVENTLOOP_ON_MAIN_THREAD = true; end
require 'tk'
Tk.mainloop

---

gives the result:

called Tcl_FindHashEntry on deleted table
Aborted (core dumped)

The same thing happens if the final line is commented out.

#10 - 03/19/2013 11:21 AM - hsbt (Hiroshi SHIBATA)

- Assignee set to nagai (Hidetoshi Nagai)

#11 - 03/19/2013 03:04 PM - edmccard (Ed McCardell)

- File crash-2.txt added

Attached is the gdb backtrace from running nagai's test script.

#12 - 06/17/2013 02:20 PM - nagai (Hidetoshi Nagai)

Currently, Ruby/Tk cannot support Tcl/Tk8.6. Please use Tcl/Tk8.5.
I want to add Tcl/Tk8.6 to supported version. But it is a future work.

#13 - 05/21/2014 01:05 PM - vo.x (Vit Ondruch)

Fedora has accepted Tcl/Tk 8.6 for F21 [1]. Is there any chance this will get resolved? Is there any repository with adjustments for 8.6 compatibility?
Is there something I can help (having just limited knowledge)?

[1] https://fedoraproject.org/wiki/Changes/f21tcl86

#14 - 08/07/2014 08:16 AM - h.shirosaki (Hiroshi Shirosaki)

- File 0001-Fix-tk-crash-with-Tk-8.6.1-on-Ubuntu.patch added

I see the crash with ruby trunk and Tk 8.6.1 on Ubuntu Linux x86_64.
It seems calling __orig_namespace_command__ causes access violation. objClientData memory looks freed.
Instead using rename command to create __orig_namespace_command__ works without crash.
I tested it with some files in ext/tk/sample.
I attached a patch.

#15 - 08/24/2014 02:00 PM - nagachika (Tomoyuki Chikanaga)

- Status changed from Open to Assigned

#16 - 10/09/2014 02:37 PM - codebykevin (Kevin Walzer)

If this patch fixes the crash on Ubuntu, can it be generalized to support Ti 8.6 across platforms? Tk 8.5 is going to be EOL'ed at some point soon and it is very important that Ruby work with 8.6.

#17 - 10/09/2014 02:50 PM - codebykevin (Kevin Walzer)

To generalize further, is it even necessary to do platform tests? Could the simple change:

- Tcl_Eval(interp, "rename namespace **orig_namespace_command**");

  Tcl_CreateObjCommand(interp, "namespace", ip_rbNamespaceObjCmd,
  (ClientData) 0, (Tcl_CmdDeleteProc *)NULL);

be applied to implement 8.6 support across the board?

#18 - 10/19/2014 12:55 PM - nagai (Hidetoshi Nagai)

- File tk-diff-ruby-2.0.0-p576 added

- File tk-diff-ruby-2.1.3-p242 added

- Status changed from Assigned to Closed

- File tk-diff-ruby-1.9.3-p547 added

Please apply the attached patch.

#19 - 10/19/2014 01:17 PM - usa (Usaku NAKAMURA)

Hidetoshi Nagai wrote:

> Please apply the attached patch.

I guess that these patches are corresponding to r48018 in trunk.
However, they contain not only the fix of the SEGV but also many new features, aren't they?

Unless there is a very compelling reason, it is not possible to add new features to the branch in the maintenance phase.
Could you make the patches contain only the fix of the SEGV?

(It should be noted that the ordinal maintenance phase of ruby_1_9_3 branch has been already ended, then ordinal bug fixes will not be backported, only security issues will be.)

#20 - 10/19/2014 01:43 PM - usa (Usaku NAKAMURA)

- Related to Backport #10400: Ruby/Tk patch for Tcl/Tk8.6 added

#21 - 10/19/2014 01:43 PM - usa (Usaku NAKAMURA)

- Related to Backport #10399: Ruby/Tk patch for Tcl/Tk8.6 added

#22 - 10/19/2014 01:43 PM - usa (Usaku NAKAMURA)

- Related to Backport #10401: Ruby/Tk patch for Tcl/Tk8.6 added

#23 - 10/19/2014 01:44 PM - usa (Usaku NAKAMURA)

- Backport set to 2.0.0: REQUIRED, 2.1: REQUIRED

#24 - 05/13/2015 09:13 PM - vo.x (Vit Ondruch)

- Backport changed from 2.0.0: REQUIRED, 2.1: REQUIRED to 2.0.0: REQUIRED, 2.1: DONE

Files

crash.log	16.2 KB	03/02/2013	edmccard (Ed McCardell)
bt.txt	1.82 KB	03/06/2013	ponimas (Alexander Ponimaskin)
bt-debug.txt	4.47 KB	03/08/2013	edmccard (Ed McCardell)
crash-2.txt	4.49 KB	03/19/2013	edmccard (Ed McCardell)

0001-Fix-tk-crash-with-Tk-8.6.1-on-Ubuntu.patch	2.36 KB	08/07/2014	h.shirosaki (Hiroshi Shirosaki)
tk-diff-ruby-1.9.3-p547	17.8 KB	10/19/2014	nagai (Hidetoshi Nagai)
tk-diff-ruby-2.0.0-p576	17.6 KB	10/19/2014	nagai (Hidetoshi Nagai)
tk-diff-ruby-2.1.3-p242	17.2 KB	10/19/2014	nagai (Hidetoshi Nagai)