Ruby 1.8 - Bug #4722

Segfault near rb_thread_check, probably a timing issue.

05/17/2011 08:19 PM - saschpe (Sascha Peilicke)

Status:	Open
Priority:	Normal
Assignee:	
Target version:	
ruby -v:	ruby 1.8.7 (2011-02-18 patchlevel 334) [x86_64-linux]

Description

Was triggered by adding a 'debugger' statement (for ruby-debug) into Rails code and pressing 'c' to continue after breakpoint.

Backtrace (see also attached core file):

Program terminated with signal 11, Segmentation fault.
#0 **vsnprintf_chk (s=0x7fffe4705060 "", maxlen=8192, flags=1, slen=8192,**
format=0x7f78850e8bb8 "wrong argument type %s (expected Thread)", args=0x7fffe4705048)
at vsnprintf_chk.c:44
44 vsnprintf_chk.c: No such file or directory.
in vsnprintf_chk.c
(gdb) bt
#0 __vsnprintf_chk (s=0x7fffe4705060 "", maxlen=8192, flags=1, slen=8192,
format=0x7f78850e8bb8 "wrong argument type %s (expected Thread)", args=0x7fffe4705048)
at vsnprintf_chk.c:44
#1 0x00007f7885066a0d in vsnprintf (ap=0x7fffe4705048, __fmt=, __n=8192,
__s=0x7fffe4705060 "") at /usr/include/bits/stdio2.h:78
#2 rb_raise (exc=140155609583120, fmt=) at error.c:1054
#3 0x00007f788506b9ea in rb_thread_check (data=) at eval.c:10582
#4 rb_thread_check (data=) at eval.c:10578
#5 0x00007f788506fa2b in rb_thread_wakeup_alive (thread=140155516998120) at eval.c:11729
#6 0x00007f788506fa79 in rb_thread_wakeup (thread=140155516998120) at eval.c:11720
#7 0x00007f7885080d39 in rb_thread_run (thread=140155516998120) at eval.c:11763
#8 0x00007f787ee7c114 in debug_event_hook (event=, node=,
self=140155609583120, mid=, klass=) at ruby_debug.c:972
#9 0x00007f78850729ce in rb_call0 (klass=140155609614840, recv=140155609583120, id=3361,
oid=, argc=1, argv=0x7fffe4707520, body=0x7f788552e4f0, flags=0) at eval.c:5915
#10 0x00007f78850741cf in rb_call (klass=140155609614840, recv=140155609583120, mid=3361, argc=1,
argv=0x7fffe4707520, scope=1, self=) at eval.c:6176
#11 0x00007f7885074915 in vafuncall (recv=, mid=, n=,
ar=) at eval.c:6253
#12 0x00007f7885074bb4 in rb_funcall (recv=, mid=, n=)
at eval.c:6270