

Backport193 - Backport #7629

Segmentation fault

12/28/2012 08:03 PM - atd (Antonio Tapiador)

Status:	Closed	
Priority:	Normal	
Assignee:		
Description		
ruby 1.9.3p362 produces a segmentation fault in our tests in Travis.		
You can find a full trace of the bug at https://travis-ci.org/ging/social_stream/jobs/3843546		
Related issues:		
Has duplicate Backport193 - Backport #7658: Rabbit <input type="checkbox"/> Ruby 1.9.3p362 <input type="checkbox"/>	Closed	
Has duplicate Backport193 - Backport #7669: Ruby 1.9.3p362 Segfaults on gem k...	Closed	01/07/2013

Associated revisions

Revision 9ccc80fe - 01/07/2013 06:52 AM - usa (Usaku NAKAMURA)

merge revision(s) 38213: [Backport #7629]

```
* vm.c (rb_vm_make_proc): save the proc made from the given block so
that it will not get collected. [ruby-core:50545] [Bug #7507]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@38726 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 38726 - 01/07/2013 06:52 AM - usa (Usaku NAKAMURA)

merge revision(s) 38213: [Backport #7629]

```
* vm.c (rb_vm_make_proc): save the proc made from the given block so
that it will not get collected. [ruby-core:50545] [Bug #7507]
```

History

#1 - 12/28/2012 08:19 PM - gingerlime (Yoav Aner)

we're also seeing a very similar segmentation fault after upgrading to 1.9.3p362 with unicorn (rails 3.2.9, postgresql 9.2)

...
vendor/bundle/ruby/1.9.1/gems/activerecord-3.2.9/lib/active_record/relation.rb:241: [BUG] Segmentation fault
ruby 1.9.3p362 (2012-12-25 revision 38607) [x86_64-linux]

#2 - 12/29/2012 04:23 PM - normalperson (Eric Wong)

"atd (Antonio Tapiador)" atapiador@dit.upm.es wrote:

<https://bugs.ruby-lang.org/issues/7629>

ruby 1.9.3p362 produces a segmentation fault in our tests in Travis.

You can find a full trace of the bug at https://travis-ci.org/ging/social_stream/jobs/3843546

Can you try reverting the vm.c change of [r38314](#)?
(I just identified with "git bisect", not sure what the correct fix is)

commit 190156054e33bc3b3bdd9e7965a1fe4a8cd50ebf
Author: usa usa@b2dd03c8-39d4-4d8f-98ff-823fe69b080e
Date: Tue Dec 11 08:51:25 2012 +0000

[Backport #5634]

```
* vm.c (rb_vm_make_env_object): make Proc object if Env is possible
to point block. [ruby-core:41038] [ruby-trunk - Bug #5634]
```

```
* vm.c (rb_vm_make_proc): No need to make Proc object here.
```

```
* bootstraptest/test_proc.rb: add tests.
```

```
diff --git a/vm.c b/vm.c
index 4dd242f..63141ba 100644
--- a/vm.c
+++ b/vm.c
@@ -467,30 +467,16 @@ vm_collect_local_variables_in_heap(rb_thread_t *th, VALUE *dfp, VALUE ary)
 }
 }
```

```
-static VALUE vm_make_proc_from_block(rb_thread_t *th, rb_block_t *block);
```

```
-
VALUE
rb_vm_make_env_object(rb_thread_t *th, rb_control_frame_t *cfp)
{
  VALUE envval;
```

- VALUE *lfp;

- rb_block_t *blockptr;

```
  if (VM_FRAME_TYPE(cfp) == VM_FRAME_MAGIC_FINISH) {
    /* for method_missing */
    cfp = RUBY_VM_PREVIOUS_CONTROL_FRAME(cfp);
  }
```

- lfp = cfp->lfp;

- **blockptr = GC_GUARDED_PTR_REF(lfp[0]);**

- if (blockptr && !(lfp[0] & 0x02)) {

- VALUE blockprocval = vm_make_proc_from_block(th, blockptr);

- rb_proc_t *p;

- GetProcPtr(blockprocval, p);

- lfp[0] = GC_GUARDED_PTR(&p->block);

- }

```
  envval = vm_make_env_each(th, cfp, cfp->dfp, cfp->lfp);
  rb_vm_rewrite_dfp_in_errinfo(th);
```

```
@@ -559,6 +545,16 @@ rb_vm_make_proc(rb_thread_t *th, const rb_block_t *block, VALUE klass)
rb_bug("rb_vm_make_proc: Proc value is already created.");
}
```

- if (GC_GUARDED_PTR_REF(cfp->lfp[0])) {
- rb_proc_t *p; +
- blockprocval = vm_make_proc_from_block(
- th, (rb_block_t *)GC_GUARDED_PTR_REF(*cfp->lfp)); +
- GetProcPtr(blockprocval, p);
- *cfp->lfp = GC_GUARDED_PTR(&p->block);

- }

```
  +
  envval = rb_vm_make_env_object(th, cfp);
```

```
  if (PROCDEBBUG) {
```

#3 - 12/29/2012 10:28 PM - roidrage (Mathias Meyer)

We've had several reports of this kind of segfault on Travis CI: <https://github.com/travis-ci/travis-ci/issues/827>

#4 - 12/30/2012 12:35 AM - eyeshield21 (Eyeshield 21)

in p362, i am also getting segfaults and cant easy repeat it (because its crushed not every time). p327 is ok.

<https://gist.github.com/213b9129e93f56ddee56>

#5 - 12/30/2012 02:42 PM - eitoball (Eito Katagiri)

I have similar segmentation fault on the same place (gems/activerecord-3.2.9/lib/active_record/relation.rb:241).

I ran gdb with core file when I got the segmentation fault. <https://gist.github.com/4411144>

#6 - 12/31/2012 09:09 PM - khustochka (Vitalii Khustochka)

Seeing the same error at the same line (gems/activerecord-3.2.9/lib/active_record/relation.rb:241) after upgrading to 1.9.3p362

#7 - 01/01/2013 02:04 AM - ortuna (Sumeet Singh)

Getting the same seg fault.

#8 - 01/02/2013 03:22 AM - veloper (Daniel Doezema)

I'm getting the same seg fault in local dev at very random times, but always within 50 requests -- On thin or unicorn server.

```
...  
.rvm/gems/ruby-1.9.3-p362/gems/activerecord-3.2.9/lib/active_record/relation.rb:241: [BUG] Segmentation fault  
ruby 1.9.3p362 (2012-12-25 revision 38607) [x86_64-darwin12.2.0]  
...
```

Running

- Rails 3.2.9
- PostgreSQL 9.2
- Mountain Lion (10.8.2)

Going to try and revert to ruby-1.9.3-p327 and seeing how that goes.

#9 - 01/02/2013 08:55 PM - sorah (Sorah Fukumori)

FYI, 1.9.3-p362's make test fails at KNOWNBUG.rb in Mountain Lion and Linux.

#10 - 01/04/2013 04:38 AM - yorickpeterse (Yorick Peterse)

- File *yorickpeterse_segfault_1_9_3p362.txt* added

I also experienced this issue when running "camper_van" (a Campfire to IRC bridge). The segfault log can be found in the file called "yorickpeterse_segfault_1_9_3p362.txt".

#11 - 01/04/2013 09:21 PM - fabn (Fabio Napoleoni)

Getting the same error in a Rails 3.2.8 application after upgrade from p327 to p362 both in Mountain Lion and Debian 6.

#12 - 01/06/2013 03:42 PM - nobu (Nobuyoshi Nakada)

- Tracker changed from Bug to Backport

- Project changed from Ruby master to Backport193

#13 - 01/07/2013 03:52 PM - usa (Usaku NAKAMURA)

- Status changed from Open to Closed

- % Done changed from 0 to 100

This issue was solved with changeset [r38726](#).

Antonio, thank you for reporting this issue.

Your contribution to Ruby is greatly appreciated.

May Ruby be with you.

merge revision(s) 38213: [Backport [#7629](#)]

```
* vm.c (rb_vm_make_proc): save the proc made from the given block so  
that it will not get collected. [ruby-core:50545] [Bug #7507]
```

#14 - 01/09/2013 02:26 AM - atd (Antonio Tapiador)

Usaku, it is my pleasure. Thank you for making Ruby so awesome

Files

yorickpeterse_segfault_1_9_3p362.txt	35.4 KB	01/04/2013	yorickpeterse (Yorick Peterse)
--------------------------------------	---------	------------	--------------------------------