Ruby - Bug #12927

SIGSEGV during GC marking of sym procs

11/12/2016 10:16 PM - eritiro (Emiliano Ritiro)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	2.3	**Backport:**	2.1: DONTNEED, 2.2: DONTNEED, 2.3: DONE

Description

After we migrated from Ruby 2.2.4 to Ruby 2.3.1 we started seeing a Segmentation Fault. This happens when the GC calls proc_mark() during the marking phase.
The proc tries to mark the block.ep[1] which contains an invalid VALUE.

I attached a script to reproduce the issue and the output of that script. (You have to run it a couple of times, it sigsevs 20% of the time)

Follow are the conclusion of my analysis:
The attached script duplicates a sym proc in memory (&:to_h)
sym procs in Ruby 2.3 uses a cfunc_proc_t which puts its environment data at the end of the rb_proc_t struct.
block->ep points to that environment.

When you copy a proc (with dup_proc()), the new proc will have a block->ep pointing to the original cfunc_proc_t
The sym_proc_cache prevents the corruption in most of the cases, but if we have a cache collision that replaces the original proc, and there are no other references to the original proc, the GC will collect the original proc, including its 64 bits of cfunc_proc_t, making them available for future use.
The duplicated proc will still be pointing to the original env, which now is freed data that GC can assign to whatever it wants.
If after that, this particular position of memory is filled with a VALUE that points outside of our memory, ruby aborts with a core dump.

Related issues:

Related to Ruby - Feature #12628: change block/env structs	**Closed**

Associated revisions

Revision a5d754acb8cfd6d3ac9f26b17ef27ca588420e38 - 11/19/2016 05:18 AM - nagachika (Tomoyuki Chikanaga)

- iseq.c (proc_dup): don't duplicate sym_procs. [Fix GH-1479]
  [ruby-core:78100] [Bug #12927]
  Based on the patch provided by Emiliano Ritiro.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@56841 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision a5d754ac - 11/19/2016 05:18 AM - nagachika (Tomoyuki Chikanaga)

- iseq.c (proc_dup): don't duplicate sym_procs. [Fix GH-1479]
  [ruby-core:78100] [Bug #12927]
  Based on the patch provided by Emiliano Ritiro.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@56841 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 11/12/2016 10:24 PM - eritiro (Emiliano Ritiro)

I created a PR with a proposed solution:
https://github.com/ruby/ruby/pull/1479

#2 - 11/13/2016 02:28 AM - nobu (Nobuyoshi Nakada)

- Related to Feature #12628: change block/env structs added

#3 - 11/13/2016 02:28 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

- Backport set to 2.1: UNKNOWN, 2.2: REQUIRED, 2.3: REQUIRED

Seems already fixed in the trunk in a different way.

#4 - 11/13/2016 03:32 PM - eritiro (Emiliano Ritiro)

- Backport changed from 2.1: UNKNOWN, 2.2: REQUIRED, 2.3: REQUIRED to 2.3: REQUIRED

Hello Nobuyoshi Nakada,

I see you changed the backport:
But the only affected version is 2.3
Are we going to patch 2.3 or we have to wait for 2.4?
Thanks.

#5 - 11/13/2016 05:24 PM - eritiro (Emiliano Ritiro)

- Backport changed from 2.3: REQUIRED to 2.1: DONTNEED, 2.2: DONTNEED, 2.3: REQUIRED

#6 - 11/14/2016 12:44 PM - nagachika (Tomoyuki Chikanaga)

I think r55766 introduces too big changes and I cannot backport it to the stable branches.
https://github.com/ruby/ruby/pull/1479/files seems reasonable to me. ko1 san, nakada san, What do you think of the patch?

#7 - 11/19/2016 05:25 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.1: DONTNEED, 2.2: DONTNEED, 2.3: REQUIRED to 2.1: DONTNEED, 2.2: DONTNEED, 2.3: DONE

I ask ko1 and nobu to review the pull request and there's no objection.
I've merged it into ruby_2_3 branch at r56841.

Emiliano, thank you for your report and investigations in detail.

Files

segfault.rb	1.76 KB	11/12/2016	eritiro (Emiliano Ritiro)
output.txt	22 KB	11/12/2016	eritiro (Emiliano Ritiro)