Ruby master - Bug #12095

ruby_vm_at_exit can sometime cause a crash.

02/21/2016 08:54 AM - nicolasnoble (Nicolas Noble)

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

Description

This behavior has been seen erratically, but one of our users got it to reproduce almost systematically. We didn't managed to understand what made his system special that it would get that crash to reproduce so well.

Here's one of the reports:

https://gist.github.com/blowmage/7ebe774039013bc8c990

The current workaround to that one (alongside a few other comments) is done here: https://github.com/grpc/grpc/pull/5337/files

Note that removing the call to ruby_vm_at_exit makes everything load fine. Also note that the removed comment from that pull request is wrong: this has been happening on versions of Ruby other than 2.0.

It's interesting to note from the backtrace information that this is happening during a garbage collection. The fact that a garbage collection happens at that exact moment is probably the reason that bug is so difficult to reproduce. Perhaps a modified version of ruby might help reproducing it. Or very specific garbage collector settings.

The fault address (0x88) seems to indicate that a NULL pointer into a struct was being dereferenced.

Disassembling the corresponding execution address seems to point at a crash inside obj_info, from the first line of gc_writebarrier_incremental, but this is after a very quick inspection of the code, so don't take my word from it.

This problem has been repoted to us on Ruby 2.0.0, Ruby 2.2.0, Ruby 2.2.3, Ruby 2.3.0, at least.

Associated revisions

Revision 990d709e - 04/04/2016 02:37 PM - nobu (Nobuyoshi Nakada)

at_exit list

- vm_core.h (rb_vm_struct): make at_exit a single linked list but not RArray, not to mark the registered functions by the write barrier. based on the patches by Evan Phoenix. [ruby-core:73908] [Bug #12095]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@54484 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 54484 - 04/04/2016 02:37 PM - nobu (Nobuyoshi Nakada)

at_exit list

- vm_core.h (rb_vm_struct): make at_exit a single linked list but not RArray, not to mark the registered functions by the write barrier. based on the patches by Evan Phoenix. [ruby-core:73908] [Bug #12095]

Revision 54484 - 04/04/2016 02:37 PM - nobu (Nobuyoshi Nakada)

at_exit list

- vm_core.h (rb_vm_struct): make at_exit a single linked list but not RArray, not to mark the registered functions by the write barrier. based on the patches by Evan Phoenix. [ruby-core:73908] [Bug #12095]

Revision 54484 - 04/04/2016 02:37 PM - nobu (Nobuyoshi Nakada)

at_exit list

- vm_core.h (rb_vm_struct): make at_exit a single linked list but not RArray, not to mark the registered functions by the write barrier. based on the patches by Evan Phoenix. [ruby-core:73908] [Bug #12095]

Revision 54484 - 04/04/2016 02:37 PM - nobu (Nobuyoshi Nakada)

at_exit list

- vm_core.h (rb_vm_struct): make at_exit a single linked list but not RArray, not to mark the registered functions by the write barrier. based on the patches by Evan Phoenix. [ruby-core:73908] [Bug #12095]

Revision 157401a9 - 04/18/2016 08:15 AM - naruse (Yui NARUSE)

merge revision(s) 54484: [Backport #12095]

```
    * vm_core.h (rb_vm_struct): make at_exit a single linked list but
      not RArray, not to mark the registered functions by the write
      barrier.  based on the patches by Evan Phoenix.
      [ruby-core:73908] [Bug #12095]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@54633 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 54633 - 04/18/2016 08:15 AM - naruse (Yui NARUSE)

merge revision(s) 54484: [Backport #12095]

```
* vm_core.h (rb_vm_struct): make at_exit a single linked list but
  not RArray, not to mark the registered functions by the write
  barrier.  based on the patches by Evan Phoenix.
  [ruby-core:73908] [Bug #12095]
```

Revision b0f5d2eb - 04/22/2016 06:18 AM - usa (Usaku NAKAMURA)

merge revision(s) 54484: [Backport #12095]

```
    * vm_core.h (rb_vm_struct): make at_exit a single linked list but
      not RArray, not to mark the registered functions by the write
      barrier.  based on the patches by Evan Phoenix.
      [ruby-core:73908] [Bug #12095]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@54683 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 54683 - 04/22/2016 06:18 AM - usa (Usaku NAKAMURA)

merge revision(s) 54484: [Backport #12095]

```
* vm_core.h (rb_vm_struct): make at_exit a single linked list but
  not RArray, not to mark the registered functions by the write
  barrier.  based on the patches by Evan Phoenix.
  [ruby-core:73908] [Bug #12095]
```

History

#1 - 03/15/2016 12:11 AM - evanphx (Evan Phoenix)

I'm hitting this as well, and looking over the code in question on 2.3.0, I wondering if the problem is that the at_exit pseudo-object is actually allocated within the body of rb_vm_t. It's address is taken and passed to rb_ary_push, which perform OBJ_WRITE. That's where wb_incremental is invoked from.

Because the mark bits are not located with the object header anymore, the mark bitmap is consulted but the position in the mark bitmap is calculated against the address of at_exit, which isn't located on the main ruby heap at all!

The path to the bad pointer, given X as the address of at_exit within rb_vm_t is: RVALUE_BLACK_P(X) => RVALUE_MARKED(X) => RVALUE_MARK_BITMAP(X) => GET_HEAP_MARK_BITS(X) => GET_HEAP_PAGE(X) => GET_PAGE_HEADER(X) => GET_PAGE_BODY(X) => ((struct heap_page_body *)((bits_t)(x) & ~(HEAP_ALIGN_MASK))).

The value returned by that above sequence is supposed to return a page header that can itself be dereferenced to find the mark bits. But because the at_exit is in a random place, the page header is basically random bytes, and thus the deference crashes.

#2 - 03/15/2016 02:47 AM - evanphx (Evan Phoenix)

- File at_exit_fix.patch added

Attached is a patch that fixes this issue by replacing the troublesome usage of a VALUE to store the at_exit functions with a simple linked list. This patch was created against the ruby_2_3 branch. It should apply cleanly to most branches because of it's small size.

#3 - 03/15/2016 03:46 AM - nobu (Nobuyoshi Nakada)

Thank you for the investigation and the patch, I've missed this.

you should:

- free the list in ruby_vm_run_at_exit_hooks,
- use the argument vm instead of GET_VM(), and
- replace the existing typedef of rb_vm_t with mere struct, as multiple typedefs are not allowed in C, IIRC.

#4 - 03/15/2016 04:21 PM - evanphx (Evan Phoenix)

- File at_exit_fix.patch added

Thank you for the feedback nobu!

Attached is an updated version of the patch with the changes.

#5 - 04/04/2016 02:39 AM - naruse (Yui NARUSE)

- Backport changed from 2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: UNKNOWN, 2.3: UNKNOWN to 2.1: REQUIRED, 2.2: REQUIRED, 2.3: REQUIRED

#6 - 04/04/2016 02:36 PM - nobu (Nobuyoshi Nakada)

at_exit functions should be called in the inverse order, LIFO.

#7 - 04/04/2016 02:37 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset r54484.

---

at_exit list

- vm_core.h (rb_vm_struct): make at_exit a single linked list but not RArray, not to mark the registered functions by the write barrier. based on the patches by Evan Phoenix. [ruby-core:73908] [Bug #12095]

#8 - 04/18/2016 08:17 AM - naruse (Yui NARUSE)

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

ruby_2_3 r54633 merged revision(s) 54484.

#9 - 04/22/2016 06:18 AM - usa (Usaku NAKAMURA)

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

ruby_2_2 r54683 merged revision(s) 54484.

Files

at_exit_fix.patch	2.08 KB	03/15/2016	evanphx (Evan Phoenix)
at_exit_fix.patch	2.18 KB	03/15/2016	evanphx (Evan Phoenix)