Ruby master - Bug #9599

Fiddle::Function#call leaks memory

03/06/2014 04:08 AM - nobu (Nobuyoshi Nakada)

Status: Closed
Priority: Normal
Assignee: tenderlovingmaking (Aaron Patterson)
Target version: 2.2.0
Backport: 1.9.3: UNKNOWN, 2.0.0: DONE, 2.1: DONE

Description

Fiddle::Function#call seems leaking memory.

With the following code:

```ruby
# fiddle-memleak.rb
require 'fiddle'
n = 10
a = ['a'] * n
f = Fiddle::Function.new(Fiddle.dlopen(nil)['rb_obj_tainted'], [Fiddle::TYPE_VOIDP]*n, Fiddle::TYPE_VOID)
loop {f.call(*a); GC.start}
```

VSZ and RSS increase continually.

```
$ ruby fiddle-memleak.rb & while ps -ovsz=rss= $!; do sleep 1; done
[1] 93595
  2423344   24
  2461024   8884
  2463072  10420
  2464096  11940
  2465120  13428
  2467168  14948
  2468192  16476
  2469216  17980
  2471264  19432
  2473312  20940
  2474336  22424
  2475360  23936
  2478432  25468
  2481504  26996
  2482528  28468
  2483552  29984
  2485600  31524
  2486624  33056
  2487652  34568
  2488676  36100
  2490724  37628
  2491748  39152
```

RGenGC seems unrelated since the result in 2.0.0 is similar.

Associated revisions

Revision ff84a6a2 - 03/08/2014 04:46 AM - nobu (Nobuyoshi Nakada)

ext/dl, ext/fiddle: fix memory leak

- ext/dl/cptr.c (dlptr_free), ext/dl/handle.c (dlhandle_free), ext/fiddle/handle.c (fiddle_handle_free), ext/fiddle/pointer.c (fiddle_ptr_free): fix memory leak. based on the patch Heesob Park at [ruby-dev:48021] [Bug #9599].

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@45291 b2dd03c8-39d4-4d8f-98f8-823fe69b080e
Revision 45291 - 03/08/2014 04:46 AM - nobu (Nobuyoshi Nakada)
ext/dl, ext/fiddle: fix memory leak

- ext/dl/cptr.c (dlptr_free), ext/dl/handle.c (dlhandle_free), ext/fiddle/handle.c (fiddle_handle_free), ext/fiddle/pointer.c (fiddle_ptr_free): fix memory leak. based on the patch Heesob Park at [ruby-dev:48021] [Bug #9599].

Revision 45291 - 03/08/2014 04:46 AM - nobu (Nobuyoshi Nakada)
ext/dl, ext/fiddle: fix memory leak

- ext/dl/cptr.c (dlptr_free), ext/dl/handle.c (dlhandle_free), ext/fiddle/handle.c (fiddle_handle_free), ext/fiddle/pointer.c (fiddle_ptr_free): fix memory leak. based on the patch Heesob Park at [ruby-dev:48021] [Bug #9599].

Revision 45291 - 03/08/2014 04:46 AM - nobu (Nobuyoshi Nakada)
ext/dl, ext/fiddle: fix memory leak

- ext/dl/cptr.c (dlptr_free), ext/dl/handle.c (dlhandle_free), ext/fiddle/handle.c (fiddle_handle_free), ext/fiddle/pointer.c (fiddle_ptr_free): fix memory leak. based on the patch Heesob Park at [ruby-dev:48021] [Bug #9599].

Revision 45291 - 03/08/2014 04:46 AM - nobu (Nobuyoshi Nakada)
ext/dl, ext/fiddle: fix memory leak

- ext/dl/cptr.c (dlptr_free), ext/dl/handle.c (dlhandle_free), ext/fiddle/handle.c (fiddle_handle_free), ext/fiddle/pointer.c (fiddle_ptr_free): fix memory leak. based on the patch Heesob Park at [ruby-dev:48021] [Bug #9599].

Revision 45291 - 03/08/2014 04:46 AM - nobu (Nobuyoshi Nakada)
ext/dl, ext/fiddle: fix memory leak

- ext/dl/cptr.c (dlptr_free), ext/dl/handle.c (dlhandle_free), ext/fiddle/handle.c (fiddle_handle_free), ext/fiddle/pointer.c (fiddle_ptr_free): fix memory leak. based on the patch Heesob Park at [ruby-dev:48021] [Bug #9599].

Revision 45291 - 03/08/2014 04:46 AM - nobu (Nobuyoshi Nakada)
ext/dl, ext/fiddle: fix memory leak

- ext/dl/cptr.c (dlptr_free), ext/dl/handle.c (dlhandle_free), ext/fiddle/handle.c (fiddle_handle_free), ext/fiddle/pointer.c (fiddle_ptr_free): fix memory leak. based on the patch Heesob Park at [ruby-dev:48021] [Bug #9599].

Revision cb05f199 - 03/09/2014 04:19 AM - nobu (Nobuyoshi Nakada)
tests for [Bug #9599]

test/dl/test_{cptr,handle}.rb: tests for [Bug #9599].

test/fiddle/test_{handle,pointer}.rb: ditto.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@45299 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 45299 - 03/09/2014 04:19 AM - nobu (Nobuyoshi Nakada)
tests for [Bug #9599]

- test/dl/test_{cptr,handle}.rb: tests for [Bug #9599].

- test/fiddle/test_{handle,pointer}.rb: ditto.

Revision 45299 - 03/09/2014 04:19 AM - nobu (Nobuyoshi Nakada)
tests for [Bug #9599]

- test/dl/test_{cptr,handle}.rb: tests for [Bug #9599].

- test/fiddle/test_{handle,pointer}.rb: ditto.

Revision 45299 - 03/09/2014 04:19 AM - nobu (Nobuyoshi Nakada)
tests for [Bug #9599]
• test/dl/test_{cptr,handle}.rb: tests for [Bug #9599].
• test/fiddle/test_{handle,pointer}.rb: ditto.

Revision 45299 - 03/09/2014 04:19 AM - nobu (Nobuyoshi Nakada)
tests for [Bug #9599]
• test/dl/test_{cptr,handle}.rb: tests for [Bug #9599].
• test/fiddle/test_{handle,pointer}.rb: ditto.

Revision 45299 - 03/09/2014 04:19 AM - nobu (Nobuyoshi Nakada)
tests for [Bug #9599]
• test/dl/test_{cptr,handle}.rb: tests for [Bug #9599].
• test/fiddle/test_{handle,pointer}.rb: ditto.

Revision 45299 - 03/09/2014 04:19 AM - nobu (Nobuyoshi Nakada)
tests for [Bug #9599]
• test/dl/test_{cptr,handle}.rb: tests for [Bug #9599].
• test/fiddle/test_{handle,pointer}.rb: ditto.

Revision e7ee0b13 - 03/20/2014 11:50 AM - nagachika (Tomoyuki Chikanaga)
merge revision(s) r45298: [Backport #9599]
  test/ruby/envutil.rb: compare RSS to check memory leak
  * test/ruby/envutil.rb (Test::Test#assert_no_memory_leak): compare
also RSS if available.
  * test/ruby/memory_status.rb (Memory::Status.parse): read string
form of an instance.
git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_0_0@45379 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 45372 - 03/20/2014 11:50 AM - nagachika (Tomoyuki Chikanaga)
merge revision(s) r45298: [Backport #9599]
  test/ruby/envutil.rb: compare RSS to check memory leak
  * test/ruby/envutil.rb (Test::Test#assert_no_memory_leak): compare
also RSS if available.
  * test/ruby/memory_status.rb (Memory::Status.parse): read string
form of an instance.

Revision fd2d5797 - 03/21/2014 03:34 PM - nagachika (Tomoyuki Chikanaga)
merge revision(s) r45311: [Backport #9599]
r45298 fix trivial bug
  $initial_size must be a size, not a status
git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_0_0@45379 b2dd03c8-39d4-4d8f-98ff-823fe69b080e
Revision 45379 - 03/21/2014 03:34 PM - nagachika (Tomoyuki Chikanaga)
merge revision(s) r45311: [Backport #9599]

r45298 fix trivial bug

$initial_size must be a size, not a status

Revision acd893d1 - 05/04/2014 05:32 PM - nagachika (Tomoyuki Chikanaga)
merge revision(s) r45291,r45299,r45314,r45325: [Backport #9518]

* ext/dl/cptr.c (dlptr_free), ext/dl/handle.c (dlhandle_free),
  ext/fiddle/handle.c (fiddle_handle_free),
  ext/fiddle/pointer.c (fiddle_ptr_free): fix memory leak.
  based on the patch Heesob Park at [ruby-dev:48021] [Bug #9599].

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@45820 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 45820 - 05/04/2014 05:32 PM - nagachika (Tomoyuki Chikanaga)
merge revision(s) r45291,r45299,r45314,r45325: [Backport #9518]

* ext/dl/cptr.c (dlptr_free), ext/dl/handle.c (dlhandle_free),
  ext/fiddle/handle.c (fiddle_handle_free),
  ext/fiddle/pointer.c (fiddle_ptr_free): fix memory leak.
  based on the patch Heesob Park at [ruby-dev:48021] [Bug #9599].

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_0_0@46508 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 5222cc1e - 06/23/2014 07:52 AM - usa (Usaku NAKAMURA)
merge revision(s) 45291,45299,45314,45325: [Backport #9518]

* ext/dl/cptr.c (dlptr_free), ext/dl/handle.c (dlhandle_free),
  ext/fiddle/handle.c (fiddle_handle_free),
  ext/fiddle/pointer.c (fiddle_ptr_free): fix memory leak.
  based on the patch Heesob Park at [ruby-dev:48021] [Bug #9599].

Revision 46508 - 06/23/2014 07:52 AM - usa (Usaku NAKAMURA)
merge revision(s) 45291,45299,45314,45325: [Backport #9599]

* ext/dl/cptr.c (dlptr_free), ext/dl/handle.c (dlhandle_free),
  ext/fiddle/handle.c (fiddle_handle_free),
  ext/fiddle/pointer.c (fiddle_ptr_free): fix memory leak.
  based on the patch Heesob Park at [ruby-dev:48021] [Bug #9599].

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_0_0@46508 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 03/06/2014 07:14 AM - phasis68 (Heesob Park)
Because Fiddle::Pointer class was alloced with TypedData.Make_Struct macro, it must be freed with ruby_xfree.
Same applies to ext/fiddle/handle.c, ext/dl/cptr.c and ext/dl/handle.c
Here is a patch.

diff --git a/pointer.c b/pointer.c
index 0a914dd..99c7596 100644
--- a/pointer.c
+++ b/pointer.c
@@ -56,6 +56,7 @@ fiddle_ptr_free(0)
 (data->free)(data->ptr);
 }
 }
-  ruby_xfree(ptr);
+  static size_t

 static size_t

#2 - 03/08/2014 04:47 AM - nobu (Nobuyoshi Nakada)
- Status changed from Assigned to Closed
- % Done changed from 0 to 100

Applied in changeset r45291.
ext/dl, ext/fiddle: fix memory leak

- ext/dl/cptr.c (dlptr_free), ext/dl/handle.c (dihandle_free), ext/fiddle/handle.c (fiddle_handle_free), ext/fiddle/pointer.c (fiddle_ptr_free): fix memory leak. based on the patch Heesob Park at [ruby-dev:48021] [Bug #9599].

#3 - 03/08/2014 02:42 PM - nagachika (Tomoyuki Chikanaga)
Backport changed from 1.9.3: UNKNOWN, 2.0.0: UNKNOWN, 2.1: UNKNOWN to 1.9.3: UNKNOWN, 2.0.0: REQUIRED, 2.1: REQUIRED

#4 - 03/09/2014 12:50 PM - nagachika (Tomoyuki Chikanaga)
Add r45301

#5 - 03/20/2014 12:11 PM - nagachika (Tomoyuki Chikanaga)
r40930 and r45298 were backported to ruby_2_0_0 (at r45371 and r45372) to resolve conflicts.
And I want to backport r45291, r45299, r45301, r45314, r45315 and r45325, but with them dl and fiddle tests fail. I wonder if there are any other memory leaks.

#6 - 03/21/2014 03:36 PM - nagachika (Tomoyuki Chikanaga)
r45311 was also backported to ruby_2_0_0. It fixes a bug introduced by r45298.

#7 - 05/04/2014 05:33 PM - nagachika (Tomoyuki Chikanaga)
Backport changed from 1.9.3: UNKNOWN, 2.0.0: REQUIRED, 2.1: REQUIRED to 1.9.3: UNKNOWN, 2.0.0: REQUIRED, 2.1: DONE
r45291, r45299, r45314 and r45325 were backported into ruby_2_1 at 45820.

#8 - 06/23/2014 07:53 AM - usa (Usaku NAKAMURA)
backported into ruby_2_0_0 at r46508.

#9 - 06/23/2014 07:53 AM - usa (Usaku NAKAMURA)
Backport changed from 1.9.3: UNKNOWN, 2.0.0: REQUIRED, 2.1: DONE to 1.9.3: UNKNOWN, 2.0.0: DONE, 2.1: DONE