Ruby - Bug #9568

Ruby interpreter crashes when executing a script in debug mode

02/25/2014 09:25 PM - easco (Scott Thompson)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.2.0dev (2014-02-26 trunk 45176) [x86_64-darwin13.0]	**Backport:**	1.9.3: REQUIRED, 2.0.0: DONE, 2.1: DONE

Description

The following script will crash the ruby interpreter when ruby is run in debug mode.
This script is creating mock HTTP objects and creating the Response class out of the middle of the Savon gem and calling a private method in a very odd way because it is a reduced test case pulled from a much larger script. The actual script use Savon in a much more conventional way:

-- crash_example.rb --

```
require 'savon'

class SampleHTTPStuff
  def error?
    return true
  end

  def code
    return 500
  end

  def body
    return %q{<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Body><SOAP
-ENV:Fault><faultcode>SOAP-ENV:Server</faultcode><faultstring>Internal Error</faultstring></SOAP-E
NV:Fault></SOAP-ENV:Body></SOAP-ENV:Envelope>}
  end
end

http = SampleHTTPStuff.new()
response = Savon::Response.new(http, {}, {})

begin
  response.instance_eval { raise_soap_and_http_errors! }
rescue => e
  puts "Ouch!"
end
```

--- end of crash_example.rb

For what it's worth, I'm using version 2.3.3 of the Savon gem.

If I run this using:

```
ruby -d crash_example.rb
```

I get a segmentation fault error. The problem appears to be the result of calling vm_throw with the "throwobj" having the value 0x8

If I run the script without the "-d" debug flag, the script runs without trouble.

I am running this on Mac OS X 10.9.1 on a MacBook Pro Retina 15"

using RVM I have tried the same code on 2.0, 2.1, and the 2.2dev head (as of 2/25/2014). They all exhibit the same behavior

I've attached a transcript file of the code being run.

Associated revisions

Revision 651b394a12fba26b9c64676978f9b2b3205c0b14 - 02/26/2014 04:26 AM - nobu (Nobuyoshi Nakada)

eval.c: preserve errinfo

- eval.c (setup_exception): preserve errinfo across calling #to_s
  method on the exception. [ruby-core:61091] [Bug #9568]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@45180 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 651b394a - 02/26/2014 04:26 AM - nobu (Nobuyoshi Nakada)

eval.c: preserve errinfo

- eval.c (setup_exception): preserve errinfo across calling #to_s
  method on the exception. [ruby-core:61091] [Bug #9568]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@45180 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision e4211600a94143266970e4edb925aed17e5abc56 - 03/02/2014 04:30 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r45178,r45179,r45180,r45183: [Backport #9568]

```
    eval.c: remove unneeded GC guard

    * eval.c (setup_exception): remove RB_GC_GUARD which is no longer
```

needed since r41598.
* eval.c (setup_exception): preserve errinfo across calling #to_s
method on the exception. [ruby-core:61091] [Bug #9568]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_0_0@45251 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision e4211600 - 03/02/2014 04:30 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r45178,r45179,r45180,r45183: [Backport #9568]

```
    eval.c: remove unneeded GC guard

    * eval.c (setup_exception): remove RB_GC_GUARD which is no longer
```

needed since r41598.
* eval.c (setup_exception): preserve errinfo across calling #to_s
method on the exception. [ruby-core:61091] [Bug #9568]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_0_0@45251 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision fca433e2fdc014b742d22dcbd0d62e4ad83a1cea - 05/29/2014 03:19 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r45178,r45180,r45183: [Backport #9568]

```
    eval.c: remove unneeded GC guard

    * eval.c (setup_exception): remove RB_GC_GUARD which is no longer
```

needed since r41598.
* eval.c (setup_exception): preserve errinfo across calling #to_s
method on the exception. [ruby-core:61091] [Bug #9568]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@46236 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision fca433e2 - 05/29/2014 03:19 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r45178,r45180,r45183: [Backport #9568]

```
    eval.c: remove unneeded GC guard

    * eval.c (setup_exception): remove RB_GC_GUARD which is no longer
```

needed since r41598.
* eval.c (setup_exception): preserve errinfo across calling #to_s
method on the exception. [ruby-core:61091] [Bug #9568]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@46236 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 02/26/2014 04:26 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

- % Done changed from 0 to 100

Applied in changeset r45180.

---

eval.c: preserve errinfo

- eval.c (setup_exception): preserve errinfo across calling #to_s
  method on the exception. [ruby-core:61091] [Bug #9568]

#2 - 02/26/2014 04:35 AM - nobu (Nobuyoshi Nakada)

- Description updated

- Backport changed from 1.9.3: UNKNOWN, 2.0.0: UNKNOWN, 2.1: UNKNOWN to 1.9.3: REQUIRED, 2.0.0: REQUIRED, 2.1: REQUIRED

#3 - 03/02/2014 04:30 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 1.9.3: REQUIRED, 2.0.0: REQUIRED, 2.1: REQUIRED to 1.9.3: REQUIRED, 2.0.0: DONE, 2.1: REQUIRED

r45178, r45179, r45180 and r45183 were backported to ruby_2_0_0 at r45251.

#4 - 05/29/2014 03:19 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 1.9.3: REQUIRED, 2.0.0: DONE, 2.1: REQUIRED to 1.9.3: REQUIRED, 2.0.0: DONE, 2.1: DONE

r45178, r45180 and r45183 were backported to ruby_2_1 branch at r46236.

Files

crash_transcript.txt	35.1 KB	02/25/2014	easco (Scott Thompson)