Ruby master - Bug #10579

Segmentation fault at 0x00000000000000

12/08/2014 12:54 PM - arunkant (Arun Kant Sharma)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:	2.2.0		
ruby -v:	ruby 2.1.2p95 (2014-05-08 revision 45877) [x86_64-linux]	**Backport:**	2.0.0: DONE, 2.1: DONE

Description

Following script cause a Segmentation fault

```
$ ruby -rresolv -e 'ObjectSpace.each_object { |obj| p obj }' > temp.output
```

But this one not

```
$ ruby -e 'ObjectSpace.each_object { |obj| p obj }' > temp.output
```

Associated revisions

Revision 42879154 - 12/09/2014 01:16 AM - nobu (Nobuyoshi Nakada)

thread.c: get rid of invalid ID symbol

- eval.c (rb_frame_last_func): return the most recent frame method name.
- thread.c (recursive_list_access): use the last method name, instead of the current method name which can be unset in some cases, not to use a symbol by the invalid ID. [ruby-core:66742] [Bug #10579]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@48744 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 48744 - 12/09/2014 01:16 AM - nobu (Nobuyoshi Nakada)

thread.c: get rid of invalid ID symbol

- eval.c (rb_frame_last_func): return the most recent frame method name.
- thread.c (recursive_list_access): use the last method name, instead of the current method name which can be unset in some cases, not to use a symbol by the invalid ID. [ruby-core:66742] [Bug #10579]

Revision 48744 - 12/09/2014 01:16 AM - nobu (Nobuyoshi Nakada)

thread.c: get rid of invalid ID symbol

- eval.c (rb_frame_last_func): return the most recent frame method name.
- thread.c (recursive_list_access): use the last method name, instead of the current method name which can be unset in some cases, not to use a symbol by the invalid ID. [ruby-core:66742] [Bug #10579]

Revision 48744 - 12/09/2014 01:16 AM - nobu (Nobuyoshi Nakada)

thread.c: get rid of invalid ID symbol

- eval.c (rb_frame_last_func): return the most recent frame method name.
- thread.c (recursive_list_access): use the last method name, instead of the current method name which can be unset in some cases, not to use a symbol by the invalid ID. [ruby-core:66742] [Bug #10579]

Revision 48744 - 12/09/2014 01:16 AM - nobu (Nobuyoshi Nakada)

thread.c: get rid of invalid ID symbol

- eval.c (rb_frame_last_func): return the most recent frame method name.
- thread.c (recursive_list_access): use the last method name, instead of the current method name which can be unset in some cases, not to use a symbol by the invalid ID. [ruby-core:66742] [Bug #10579]

Revision 48744 - 12/09/2014 01:16 AM - nobu (Nobuyoshi Nakada)

thread.c: get rid of invalid ID symbol

- eval.c (rb_frame_last_func): return the most recent frame method name.

- thread.c (recursive_list_access): use the last method name, instead of the current method name which can be unset in some cases, not to use a symbol by the invalid ID. [ruby-core:66742] [Bug #10579]

Revision 48744 - 12/09/2014 01:16 AM - nobu (Nobuyoshi Nakada)

thread.c: get rid of invalid ID symbol

- eval.c (rb_frame_last_func): return the most recent frame method name.
- thread.c (recursive_list_access): use the last method name, instead of the current method name which can be unset in some cases, not to use a symbol by the invalid ID. [ruby-core:66742] [Bug #10579]

Revision 8cbf4003 - 12/10/2014 12:38 AM - nobu (Nobuyoshi Nakada)

thread.c: use the same method name

- thread.c (exec_recursive): use the same last method name as recursive_push in the error message when recursive_pop failed. [ruby-core:66742] [Bug #10579]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@48752 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 48752 - 12/10/2014 12:38 AM - nobu (Nobuyoshi Nakada)

thread.c: use the same method name

- thread.c (exec_recursive): use the same last method name as recursive_push in the error message when recursive_pop failed. [ruby-core:66742] [Bug #10579]

Revision 48752 - 12/10/2014 12:38 AM - nobu (Nobuyoshi Nakada)

thread.c: use the same method name

- thread.c (exec_recursive): use the same last method name as recursive_push in the error message when recursive_pop failed. [ruby-core:66742] [Bug #10579]

Revision 48752 - 12/10/2014 12:38 AM - nobu (Nobuyoshi Nakada)

thread.c: use the same method name

- thread.c (exec_recursive): use the same last method name as recursive_push in the error message when recursive_pop failed. [ruby-core:66742] [Bug #10579]

Revision 48752 - 12/10/2014 12:38 AM - nobu (Nobuyoshi Nakada)

thread.c: use the same method name

- thread.c (exec_recursive): use the same last method name as recursive_push in the error message when recursive_pop failed. [ruby-core:66742] [Bug #10579]

Revision 48752 - 12/10/2014 12:38 AM - nobu (Nobuyoshi Nakada)

thread.c: use the same method name

- thread.c (exec_recursive): use the same last method name as recursive_push in the error message when recursive_pop failed. [ruby-core:66742] [Bug #10579]

Revision 48752 - 12/10/2014 12:38 AM - nobu (Nobuyoshi Nakada)

thread.c: use the same method name

- thread.c (exec_recursive): use the same last method name as recursive_push in the error message when recursive_pop failed. [ruby-core:66742] [Bug #10579]

Revision 9120d051 - 01/14/2015 07:04 AM - usa (Usaku NAKAMURA)

merge revision(s) 48744,48752: [Backport #10579]

```
    * eval.c (rb_frame_last_func): return the most recent frame method
      name.

    * thread.c (recursive_list_access): use the last method name,
      instead of the current method name which can be unset in some
      cases, not to use a symbol by the invalid ID.
      [ruby-core:66742] [Bug #10579]

    * thread.c (exec_recursive): use the same last method name as
```

```
      recursive_push in the error message when recursive_pop failed.
      [ruby-core:66742] [Bug #10579]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_0_0@49246 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 49246 - 01/14/2015 07:04 AM - usa (Usaku NAKAMURA)

merge revision(s) 48744,48752: [Backport #10579]

```
* eval.c (rb_frame_last_func): return the most recent frame method
  name.

* thread.c (recursive_list_access): use the last method name,
  instead of the current method name which can be unset in some
  cases, not to use a symbol by the invalid ID.
  [ruby-core:66742] [Bug #10579]

* thread.c (exec_recursive): use the same last method name as
  recursive_push in the error message when recursive_pop failed.
  [ruby-core:66742] [Bug #10579]
```

Revision 4b0a168d - 01/21/2015 04:09 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r48744,r48752: [Backport #10579]

```
    * eval.c (rb_frame_last_func): return the most recent frame method
      name.

    * thread.c (recursive_list_access): use the last method name,
      instead of the current method name which can be unset in some
      cases, not to use a symbol by the invalid ID.
      [ruby-core:66742] [Bug #10579]

    * thread.c (exec_recursive): use the same last method name as
      recursive_push in the error message when recursive_pop failed.
      [ruby-core:66742] [Bug #10579]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@49369 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 49369 - 01/21/2015 04:09 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r48744,r48752: [Backport #10579]

```
* eval.c (rb_frame_last_func): return the most recent frame method
  name.

* thread.c (recursive_list_access): use the last method name,
  instead of the current method name which can be unset in some
  cases, not to use a symbol by the invalid ID.
  [ruby-core:66742] [Bug #10579]

* thread.c (exec_recursive): use the same last method name as
  recursive_push in the error message when recursive_pop failed.
  [ruby-core:66742] [Bug #10579]
```

History

#1 - 12/08/2014 02:12 PM - phasis68 (Heesob Park)

The root cause of this issue is openssl.so.

```
C:\>ruby -ropenssl.so -e "ObjectSpace.each_object{|obj| p obj}"
...
-e:1: [BUG] Segmentation fault
ruby 2.1.3p242 (2014-09-19 revision 47630) [i386-mingw32]

-- Control frame information -----------------------------------------------
c:0007 p:---- s:0018 e:000017 CFUNC  :inspect
c:0006 p:---- s:0016 e:000015 CFUNC  :inspect
c:0005 p:---- s:0014 e:000013 CFUNC  :p
c:0004 p:0009 s:0010 e:000009 BLOCK  -e:1 [FINISH]
c:0003 p:---- s:0007 e:000006 CFUNC  :each_object
c:0002 p:0011 s:0004 E:0014fc EVAL   -e:1 [FINISH]
c:0001 p:0000 s:0002 E:001354 TOP    [FINISH]

-e:1:in `<main>'
```

```
-e:1:in `each_object'
-e:1:in `block in <main>'
-e:1:in `p'
-e:1:in `inspect'
-e:1:in `inspect'

-- C level backtrace information -------------------------------------------
C:\WINDOWS\SYSTEM32\ntdll.dll(NtWaitForSingleObject+0xc) [0x7700A53C]
C:\WINDOWS\SYSTEM32\KERNELBASE.dll(WaitForSingleObject+0x12) [0x76B31055]
C:\Ruby21\bin\msvcrt-ruby210.dll(rb_vm_bugreport+0xa7) [0x6D3947A7]
C:\Ruby21\bin\msvcrt-ruby210.dll(rb_name_err_mesg_new+0x69f) [0x6D248FBF]
C:\Ruby21\bin\msvcrt-ruby210.dll(rb_bug+0x2e) [0x6D249D9E]
C:\Ruby21\bin\msvcrt-ruby210.dll(rb_check_safe_str+0x34b) [0x6D31483B] [0x00401866]
C:\WINDOWS\SYSTEM32\ntdll.dll(LdrSetAppCompatDllRedirectionCallback+0x12c0f) [0x77079E86]
```

#2 - 12/08/2014 09:12 PM - nobu (Nobuyoshi Nakada)

- Description updated

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

Not only openssl.so, resolv.rb too.

The cause is exec_recursive used by rb_hash_any stores the current method name, but it isn't set in the required top-level, and a few other cases.

#3 - 12/08/2014 11:48 PM - nobu (Nobuyoshi Nakada)

- Description updated

One of the simplest code to reproduce it is:

```
$ ruby -e '{["foo"]=>nil}; p Thread.current[:__recursive_key__]'
```

#4 - 12/09/2014 01:16 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

- % Done changed from 0 to 100

Applied in changeset r48744.

---

thread.c: get rid of invalid ID symbol

- eval.c (rb_frame_last_func): return the most recent frame method name.
- thread.c (recursive_list_access): use the last method name, instead of the current method name which can be unset in some cases, not to use a symbol by the invalid ID. [ruby-core:66742] [Bug #10579]

#5 - 01/14/2015 07:05 AM - usa (Usaku NAKAMURA)

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

Backported into ruby_2_0_0 at r49246.

note: thread.c is a little different from trunk.

#6 - 01/21/2015 04:10 PM - nagachika (Tomoyuki Chikanaga)

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

Backported into ruby_2_1 at r49369.

Files

rubyerror.output	18.7 KB	12/08/2014	arunkant (Arun Kant Sharma)