Ruby - Bug #5846

JSON.parse with :object_class causes SEGV

01/05/2012 10:48 PM - nahi (Hiroshi Nakamura)

Status:	Closed		
Priority:	Normal		
Assignee:	naruse (Yui NARUSE)		
Target version:	2.0.0		
ruby -v:	ruby 2.0.0dev (2012-01-05 trunk 34216) [x86_64-linux]	**Backport:**	

Description

JSON.parse method accepts a :object_class option to specify the class of resulting object other than Hash. But with the trunk version of json lib it causes SEGV. The bug seems to be fixed at upstream already (see the last.)

```
% ruby -rset -e 'require "json"; JSON.parse("{}", :object_class => Set)'
/usr/local/lib/ruby/1.9.1/json/common.rb:148: [BUG] Segmentation fault
ruby 2.0.0dev (2012-01-05 trunk 34216) [x86_64-linux]

-- Control frame information -----------------------------------------------
c:0005 p:---- s:0015 b:0015 l:000014 d:000014 CFUNC  :parse
c:0004 p:0031 s:0012 b:0012 l:000011 d:000011 METHOD /usr/local/lib/ruby/1.9.1/json/common.rb:148
c:0003 p:0040 s:0006 b:0006 l:000158 d:000528 EVAL   -e:1
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:000158 d:000158 TOP

-- Ruby level backtrace information ----------------------------------------
-e:1:in <main>' /usr/local/lib/ruby/1.9.1/json/common.rb:148:in parse'
/usr/local/lib/ruby/1.9.1/json/common.rb:148:in `parse'

-- C level backtrace information -------------------------------------------
mmap: No such device
mmap: No such device
mmap: No such device
mmap: No such device
mmap: No such device
mmap: No such device
mmap: No such device
mmap: No such device
mmap: No such device
mmap: No such device
mmap: No such device
mmap: No such device
mmap: No such device
mmap: No such device
mmap: No such device
ruby(+0x1311e5) [0x7f5ca08871e5]
ruby(+0x179d0b) [0x7f5ca08cfd0b]
ruby(rb_bug+0xb7) [0x7f5ca08d1157]
ruby(+0xc1e8f) [0x7f5ca0817e8f]
/lib/x86_64-linux-gnu/libpthread.so.0(+0x10060) [0x7f5ca0326060]
ruby(st_lookup+0x88) [0x7f5ca08202c8]
ruby(rb_hash_aref+0x25) [0x7f5ca0784b45]
/usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/parser.so(+0x29f5) [0x7f5c9e8d19f5] parser.rl:169
/usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/parser.so(+0x34b5) [0x7f5c9e8d24b5] parser.rl:711
ruby(+0x12d16a) [0x7f5ca088316a]
ruby(+0x120319) [0x7f5ca0876319]
ruby(+0x12712a) [0x7f5ca087d12a]
ruby(rb_iseq_eval_main+0xa6) [0x7f5ca0884c96]
ruby(+0x1f742) [0x7f5ca0775742]
ruby(ruby_run_node+0x36) [0x7f5ca0778056]
ruby(+0x1f0db) [0x7f5ca07750db]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xed) [0x7f5c9f6cf30d]
ruby(+0x1f109) [0x7f5ca0775109]
```

-- Other runtime information --

- Loaded script: -e
- Loaded features:

  0 enumerator.so
  1 /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/encdb.so
  2 /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/trans/transdb.so
  3 /usr/local/lib/ruby/1.9.1/rubygems/defaults.rb
  4 /usr/local/lib/ruby/1.9.1/x86_64-linux/rbconfig.rb
  5 /usr/local/lib/ruby/1.9.1/rubygems/deprecate.rb
  6 /usr/local/lib/ruby/1.9.1/rubygems/exceptions.rb
  7 /usr/local/lib/ruby/1.9.1/rubygems/custom_require.rb
  8 /usr/local/lib/ruby/1.9.1/rubygems.rb
  9 /usr/local/lib/ruby/1.9.1/set.rb
  10 /usr/local/lib/ruby/1.9.1/json/version.rb
  11 /usr/local/lib/ruby/1.9.1/json/common.rb
  12 /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_16be.so
  13 /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_16le.so
  14 /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_32be.so
  15 /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_32le.so
  16 /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/parser.so
  17 /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/generator.so
  18 /usr/local/lib/ruby/1.9.1/json/ext.rb
  19 /usr/local/lib/ruby/1.9.1/json.rb

- Process memory map:

```
7f5c9dca7000-7f5c9dcbc000 r-xp 00000000 08:01 134871     /lib/x86_64-linux-gnu/libgcc_s.so.1
7f5c9dcbc000-7f5c9debb000 ---p 00015000 08:01 134871     /lib/x86_64-linux-gnu/libgcc_s.so.1
7f5c9debb000-7f5c9debc000 r--p 00014000 08:01 134871     /lib/x86_64-linux-gnu/libgcc_s.so.1
7f5c9debc000-7f5c9debd000 rw-p 00015000 08:01 134871     /lib/x86_64-linux-gnu/libgcc_s.so.1
7f5c9debd000-7f5c9dec6000 r-xp 00000000 08:01 4499165    /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/generator.so
7f5c9dec6000-7f5c9e0c5000 ---p 00009000 08:01 4499165    /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/generator.so
7f5c9e0c5000-7f5c9e0c6000 r--p 00008000 08:01 4499165    /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/generator.so
7f5c9e0c6000-7f5c9e0c7000 rw-p 00009000 08:01 4499165    /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/generator.so
7f5c9e0c7000-7f5c9e0c8000 r-xp 00000000 08:01 4499172    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_32le.so
7f5c9e0c8000-7f5c9e2c7000 ---p 00001000 08:01 4499172    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_32le.so
7f5c9e2c7000-7f5c9e2c8000 r--p 00000000 08:01 4499172    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_32le.so
7f5c9e2c8000-7f5c9e2c9000 rw-p 00001000 08:01 4499172    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_32le.so
7f5c9e2c9000-7f5c9e2ca000 r-xp 00000000 08:01 4499199    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_32be.so
7f5c9e2ca000-7f5c9e4c9000 ---p 00001000 08:01 4499199    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_32be.so
7f5c9e4c9000-7f5c9e4ca000 r--p 00000000 08:01 4499199    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_32be.so
7f5c9e4ca000-7f5c9e4cb000 rw-p 00001000 08:01 4499199    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_32be.so
7f5c9e4cb000-7f5c9e4cc000 r-xp 00000000 08:01 4499190    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_16le.so
7f5c9e4cc000-7f5c9e6cb000 ---p 00001000 08:01 4499190    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_16le.so
7f5c9e6cb000-7f5c9e6cc000 r--p 00000000 08:01 4499190    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_16le.so
7f5c9e6cc000-7f5c9e6cd000 rw-p 00001000 08:01 4499190    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_16le.so
7f5c9e6cd000-7f5c9e6ce000 r-xp 00000000 08:01 4499174    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_16be.so
7f5c9e6ce000-7f5c9e8cd000 ---p 00001000 08:01 4499174    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_16be.so
7f5c9e8cd000-7f5c9e8ce000 r--p 00000000 08:01 4499174    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_16be.so
7f5c9e8ce000-7f5c9e8cf000 rw-p 00001000 08:01 4499174    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/utf_16be.so
7f5c9e8cf000-7f5c9e8d4000 r-xp 00000000 08:01 4499166    /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/parser.so
7f5c9e8d4000-7f5c9ead4000 ---p 00005000 08:01 4499166    /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/parser.so
7f5c9ead4000-7f5c9ead5000 r--p 00005000 08:01 4499166    /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/parser.so
7f5c9ead5000-7f5c9ead6000 rw-p 00006000 08:01 4499166    /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/parser.so
7f5c9ead6000-7f5c9ead8000 r-xp 00000000 08:01 4499202    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/trans/transdb.so
7f5c9ead8000-7f5c9ecd7000 ---p 00002000 08:01 4499202    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/trans/transdb.so
7f5c9ecd7000-7f5c9ecd8000 r--p 00001000 08:01 4499202    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/trans/transdb.so
7f5c9ecd8000-7f5c9ecd9000 rw-p 00002000 08:01 4499202    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/trans/transdb.so
7f5c9ecd9000-7f5c9ecdb000 r-xp 00000000 08:01 4499194    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/encdb.so
7f5c9ecdb000-7f5c9eeda000 ---p 00002000 08:01 4499194    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/encdb.so
7f5c9eeda000-7f5c9eedb000 r--p 00001000 08:01 4499194    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/encdb.so
7f5c9eedb000-7f5c9eedc000 rw-p 00002000 08:01 4499194    /usr/local/lib/ruby/1.9.1/x86_64-linux/enc/encdb.so
7f5c9eedc000-7f5c9f6ae000 r--p 00000000 08:01 5118342    /usr/lib/locale/locale-archive
```

```
7f5c9f6ae000-7f5c9f843000 r-xp 00000000 08:01 134850                    /lib/x86_64-linux-gnu/libc-2.13.so
7f5c9f843000-7f5c9fa42000 ---p 00195000 08:01 134850                    /lib/x86_64-linux-gnu/libc-2.13.so
7f5c9fa42000-7f5c9fa46000 r--p 00194000 08:01 134850                    /lib/x86_64-linux-gnu/libc-2.13.so
7f5c9fa46000-7f5c9fa47000 rw-p 00198000 08:01 134850                    /lib/x86_64-linux-gnu/libc-2.13.so
7f5c9fa47000-7f5c9fa4d000 rw-p 00000000 00:00 0
7f5c9fa4d000-7f5c9fad0000 r-xp 00000000 08:01 134880                    /lib/x86_64-linux-gnu/libm-2.13.so
7f5c9fad0000-7f5c9fccf000 ---p 00083000 08:01 134880                   /lib/x86_64-linux-gnu/libm-2.13.so
7f5c9fccf000-7f5c9fcd0000 r--p 00082000 08:01 134880                   /lib/x86_64-linux-gnu/libm-2.13.so
7f5c9fcd0000-7f5c9fcd1000 rw-p 00083000 08:01 134880                    /lib/x86_64-linux-gnu/libm-2.13.so
7f5c9fcd1000-7f5c9fcda000 r-xp 00000000 08:01 134856                    /lib/x86_64-linux-gnu/libcrypt-2.13.so
7f5c9fcda000-7f5c9feda000 ---p 00009000 08:01 134856                    /lib/x86_64-linux-gnu/libcrypt-2.13.so
7f5c9feda000-7f5c9fedb000 r--p 00009000 08:01 134856                    /lib/x86_64-linux-gnu/libcrypt-2.13.so
7f5c9fedb000-7f5c9fedc000 rw-p 0000a000 08:01 134856                    /lib/x86_64-linux-gnu/libcrypt-2.13.so
7f5c9fedc000-7f5c9ff0a000 rw-p 00000000 00:00 0
7f5c9ff0a000-7f5c9ff0c000 r-xp 00000000 08:01 134861                   /lib/x86_64-linux-gnu/libdl-2.13.so
7f5c9ff0c000-7f5ca010c000 ---p 00002000 08:01 134861                    /lib/x86_64-linux-gnu/libdl-2.13.so
7f5ca010c000-7f5ca010d000 r--p 00002000 08:01 134861                    /lib/x86_64-linux-gnu/libdl-2.13.so
7f5ca010d000-7f5ca010e000 rw-p 00003000 08:01 134861                    /lib/x86_64-linux-gnu/libdl-2.13.so
7f5ca010e000-7f5ca0115000 r-xp 00000000 08:01 134914                    /lib/x86_64-linux-gnu/librt-2.13.so
7f5ca0115000-7f5ca0314000 ---p 00007000 08:01 134914                    /lib/x86_64-linux-gnu/librt-2.13.so
7f5ca0314000-7f5ca0315000 r--p 00006000 08:01 134914                    /lib/x86_64-linux-gnu/librt-2.13.so
7f5ca0315000-7f5ca0316000 rw-p 00007000 08:01 134914                    /lib/x86_64-linux-gnu/librt-2.13.so
7f5ca0316000-7f5ca032e000 r-xp 00000000 08:01 134910                    /lib/x86_64-linux-gnu/libpthread-2.13.so
7f5ca032e000-7f5ca052d000 ---p 00018000 08:01 134910                    /lib/x86_64-linux-gnu/libpthread-2.13.so
7f5ca052d000-7f5ca052e000 r--p 00017000 08:01 134910                    /lib/x86_64-linux-gnu/libpthread-2.13.so
7f5ca052e000-7f5ca052f000 rw-p 00018000 08:01 134910                    /lib/x86_64-linux-gnu/libpthread-2.13.so
7f5ca052f000-7f5ca0533000 rw-p 00000000 00:00 0
7f5ca0533000-7f5ca0554000 r-xp 00000000 08:01 134837                    /lib/x86_64-linux-gnu/ld-2.13.so
7f5ca0638000-7f5ca073e000 rw-p 00000000 00:00 0
7f5ca074b000-7f5ca074c000 rw-p 00000000 00:00 0
7f5ca074d000-7f5ca074e000 ---p 00000000 00:00 0
7f5ca074e000-7f5ca0753000 rw-p 00000000 00:00 0
7f5ca0753000-7f5ca0754000 r--p 00020000 08:01 134837                    /lib/x86_64-linux-gnu/ld-2.13.so
7f5ca0754000-7f5ca0756000 rw-p 00021000 08:01 134837                    /lib/x86_64-linux-gnu/ld-2.13.so
7f5ca0756000-7f5ca097d000 r-xp 00000000 08:01 5505867                   /usr/local/bin/ruby
7f5ca0b7d000-7f5ca0b81000 r--p 00227000 08:01 5505867                   /usr/local/bin/ruby
7f5ca0b81000-7f5ca0b83000 rw-p 0022b000 08:01 5505867                   /usr/local/bin/ruby
7f5ca0b83000-7f5ca0ba0000 rw-p 00000000 00:00 0
7f5ca1cec000-7f5ca2011000 rw-p 00000000 00:00 0                         [heap]
7fff5ea7a000-7fff5ea9b000 rw-p 00000000 00:00 0                        [stack]
7fff5ebff000-7fff5ec00000 r-xp 00000000 00:00 0                      [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0            [vsyscall]
```

[NOTE]
You may have encountered a bug in the Ruby interpreter or extension libraries.
Bug reports are welcome.
For details: http://www.ruby-lang.org/bugreport.html

```
zsh: abort      ruby -rset -e 'require "json"; JSON.parse("{}", :object_class => Set)'

% ruby -rset -e 'gem "json"; require "json"; JSON.parse("{}", :object_class => Set)'
/home/nahi/.gem/ruby/1.9.1/gems/json-1.6.4/lib/json/common.rb:148:in parse': undefined method []' for #<Set: {}> (NoMethodError)
from /home/nahi/.gem/ruby/1.9.1/gems/json-1.6.4/lib/json/common.rb:148:in parse' from -e:1:in '
zsh: exit 1     ruby -rset -e
```

In the typescript above, passing Set as :object_class raises NoMethodError but it's expected result. Please ignore this exception since it's just for illustrating the bug. Passing Hash-like such as RadixTree (https://github.com/nahi/radix_tree) works as expected.

Naruse-san, I'm setting you as the Assignee because you're the maintainer of json lib. Can you confirm the SEGV?

Associated revisions

Revision 4d8d3184d18b1a9d2eadb86a6688dc62eca7eabc - 03/11/2012 01:36 PM - naruse (Yui NARUSE)

- ext/json: Merge 164a75c8bd2007d32c4d7665d53140d8fc126dcd.
  [ruby-core:41917] [Bug #5846]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@34971 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 4d8d3184 - 03/11/2012 01:36 PM - naruse (Yui NARUSE)

- ext/json: Merge 164a75c8bd2007d32c4d7665d53140d8fc126dcd.
  [ruby-core:41917] [Bug #5846]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@34971 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 03/11/2012 10:36 PM - naruse (Yui NARUSE)

- Status changed from Open to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r34971.
Hiroshi, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- ext/json: Merge 164a75c8bd2007d32c4d7665d53140d8fc126dcd.
  [ruby-core:41917] [Bug #5846]