Ruby master - 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
% ruby -rset -e 'require "json"; JSON.parse("{}"); :object_class => Set')
/usr/local/lib/ruby/1.9.1/json/common.rb:148: [BUG] Segmentation fault
```

-- Control frame information -----------------------------------------------
```
```

-- 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
mmap: No such device
```

09/12/2021 1/4
-- 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:

    7f5c9dca7000-7f5c9dc0000 r-xp 00000000 08:01 134871
    7f5c9dcb000-7f5c9dec000 r-p 00015000 08:01 134871
    7f5c9dde000-7f5c9dee000 r--p 00000000 08:01 134871
    7f5c9def000-7f5c9df0000 r-p 00000000 08:01 134871
    7f5c9e0000-7f5c9e0b0000 r-xp 00000000 08:01 134871
    7f5c9e0c000-7f5c9e0d0000 r--p 00001000 08:01 134871
    7f5c9e0e000-7f5c9e0f0000 r-xp 00000000 08:01 134871
    /lib/x86_64-linux-gnu/libgcc_s.so.1
    /lib/x86_64-linux-gnu/libgcc_s.so.1
    /lib/x86_64-linux-gnu/libgcc_s.so.1
    /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/generator.so
    /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/parser.so
    /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext/generator.so
    /usr/local/lib/ruby/1.9.1/x86_64-linux/json/ext.rb
    /usr/local/lib/ruby/1.9.1/json.rb

09/12/2021
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

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?

Related issues:
- Has duplicate Backport193 - Backport #6304: JSON.parse with :object_class sti...
Associated revisions

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

Revision 34971 - 03/11/2012 01:36 PM - naruse (Yui NARUSE)
- ext/json: Merge 164a75c8bd2007d32c4d7665d53140d8fc126dcd. [ruby-core:41917] [Bug #5846]

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.