Ruby trunk - Bug #15396

Please backport r62621 for LLP64 environment

12/10/2018 10:52 AM - wanabe (_ wanabe)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.5.4p122 (2018-12-09 revision 66298) [x64-mswin64_140]	**Backport:**	2.4: UNKNOWN, 2.5: DONE

Description

Sometimes ruby 2.5.4 occurs SEGV on mswin64.
https://ci.appveyor.com/project/ruby/ruby/builds/20707563

It can be reproduced on my environment.

```
C:\ruby>miniruby.exe -v -e 'RubyVM::InstructionSequence.compile("[]<</1/").to_binary'
ruby 2.5.4p122 (2018-12-09 revision 66298) [x64-mswin64_140]
-e:1: [BUG] Segmentation fault
ruby 2.5.4p122 (2018-12-09 revision 66298) [x64-mswin64_140]
(snip)
```

And this SEGV can be resolved with r62621.

```
C:\ruby>miniruby -e 'h=`git log origin/trunk --grep=@62621 --format=%H -1`; p h;system("git cherry
-pick #{h}")'
"b001766b080a3572a7fae94aa0b8ab0b0a0f3ee2\n"
[ruby_2_5 f54400618a] compile.c: do not truncate VALUE to long
 Author: nobu <nobu@b2dd03c8-39d4-4d8f-98ff-823fe69b080e>
 Date: Thu Mar 1 07:59:57 2018 +0000
 1 file changed, 2 insertions(+), 2 deletions(-)

C:\ruby>nmake miniruby && miniruby.exe -v -e 'RubyVM::InstructionSequence.compile("[]<</1/").to_bi
nary'

Microsoft (R) Program Maintenance Utility Version 14.16.27024.1
Copyright (C) Microsoft Corporation.  All rights reserved.

compiling compile.c
compile.c
user32.lib advapi32.lib shell32.lib ws2_32.lib iphlpapi.lib imagehlp.lib shlwapi.lib
linking miniruby.exe
ruby 2.5.4p122 (2018-12-09 revision 66298) [x64-mswin64_140]
ruby 2.5.4p122 (2018-12-09 revision 66298) [x64-mswin64_140]
```

Would you please backport r62621?

Associated revisions

Revision 62621 - 03/01/2018 07:59 AM - nobu (Nobuyoshi Nakada)

compile.c: do not truncate VALUE to long

- compile.c (ibf_dump_object_regexp): do not truncate VALUE to long. it makes invalid VALUE on IL32LLP64 platforms where long is shorter than VALUE.

Revision 6473d94d - 12/10/2018 12:31 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 62621: [Backport #15396]

```
    compile.c: do not truncate VALUE to long

    * compile.c (ibf_dump_object_regexp): do not truncate VALUE to
      long.  it makes invalid VALUE on IL32LLP64 platforms where long
```

```
      is shorter than VALUE.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@66309 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 66309 - 12/10/2018 12:31 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 62621: [Backport #15396]

```
compile.c: do not truncate VALUE to long

* compile.c (ibf_dump_object_regexp): do not truncate VALUE to
  long.  it makes invalid VALUE on IL32LLP64 platforms where long
  is shorter than VALUE.
```

History

#1 - 12/10/2018 12:28 PM - nagachika (Tomoyuki Chikanaga)

Thank you very much wanabe-san.
r62621 is reasonable candidate of fix for SEGV on mswin and can be cleanly backported.
I will backport it soon.

#2 - 12/10/2018 12:32 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.4: UNKNOWN, 2.5: REQUIRED to 2.4: UNKNOWN, 2.5: DONE

ruby_2_5 r66309 merged revision(s) 62621.