Ruby trunk - Bug #8634

Segfault with sprintf of force_encoding('UTF-16LE') on Windows

07/14/2013 11:35 AM - phasis68 (Heesob Park)

Status:	Closed		
Priority:	Normal		
Assignee:	nobu (Nobuyoshi Nakada)		
Target version:	2.1.0		
ruby -v:	ruby 2.1.0dev (2013-07-14 trunk 41961) [i386-mingw32]	**Backport:**	1.9.3: DONTNEED, 2.0.0: DONTNEED

Description

The revision r41937 raised segfault in test_m17n.rb

http://ci.rubyinstaller.org/job/ruby-trunk-x64-test-all/1590/console

Here is a simplified test case.

```
C:\work>ruby -e 'p("%s".force_encoding("UTF-16LE")%"test")'
-e:1: [BUG] Segmentation fault
ruby 2.1.0dev (2013-07-14 trunk 41961) [i386-mingw32]

-- Control frame information -----------------------------------------------
c:0003 p:---- s:0008 e:000007 CFUNC  :p
c:0002 p:0015 s:0004 E:0007e4 EVAL   -e:1 [FINISH]
c:0001 p:0000 s:0002 E:0022b4 TOP    [FINISH]

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

-- C level backtrace information -------------------------------------------
C:\Windows\SysWOW64\ntdll.dll(ZwWaitForSingleObject+0x15) [0x7701F8B1]
C:\Windows\syswow64\kernel32.dll(WaitForSingleObjectEx+0x43) [0x75151194]
C:\Windows\syswow64\kernel32.dll(WaitForSingleObject+0x12) [0x75151148]
c:\usr\local\bin\msvcrt-ruby210.dll(rb_vm_bugreport+0xa7) [0x6D3811B7]
c:\usr\local\bin\msvcrt-ruby210.dll(rb_name_err_mesg_new+0x69d) [0x6D2435AD]
c:\usr\local\bin\msvcrt-ruby210.dll(rb_bug+0x2e) [0x6D2443AE]
c:\usr\local\bin\msvcrt-ruby210.dll(rb_check_safe_str+0x110) [0x6D305760]
[0x00401866]
C:\Windows\SysWOW64\ntdll.dll(RtlKnownExceptionFilter+0xb7) [0x770774DF]

-- Other runtime information -----------------------------------------------

* Loaded script: -e

* Loaded features:

    0 enumerator.so
    1 c:/usr/local/lib/ruby/2.1.0/i386-mingw32/enc/encdb.so
    2 c:/usr/local/lib/ruby/2.1.0/i386-mingw32/enc/cp949.so
    3 c:/usr/local/lib/ruby/2.1.0/i386-mingw32/enc/trans/transdb.so
    4 c:/usr/local/lib/ruby/2.1.0/i386-mingw32/rbconfig.rb
    5 c:/usr/local/lib/ruby/2.1.0/rubygems/compatibility.rb
    6 c:/usr/local/lib/ruby/2.1.0/rubygems/defaults.rb
    7 c:/usr/local/lib/ruby/2.1.0/rubygems/deprecate.rb
    8 c:/usr/local/lib/ruby/2.1.0/rubygems/errors.rb
    9 c:/usr/local/lib/ruby/2.1.0/rubygems/version.rb
    10 c:/usr/local/lib/ruby/2.1.0/rubygems/requirement.rb
    11 c:/usr/local/lib/ruby/2.1.0/rubygems/platform.rb
    12 c:/usr/local/lib/ruby/2.1.0/rubygems/basic_specification.rb
    13 c:/usr/local/lib/ruby/2.1.0/rubygems/stub_specification.rb
    14 c:/usr/local/lib/ruby/2.1.0/rubygems/specification.rb
    15 c:/usr/local/lib/ruby/2.1.0/rubygems/exceptions.rb
```

16 c:/usr/local/lib/ruby/2.1.0/i386-mingw32/enc/utf_16le.so
17 c:/usr/local/lib/ruby/2.1.0/i386-mingw32/enc/trans/utf_16_32.so
18 c:/usr/local/lib/ruby/2.1.0/rubygems/core_ext/kernel_gem.rb
19 c:/usr/local/lib/ruby/2.1.0/thread.rb
20 c:/usr/local/lib/ruby/2.1.0/monitor.rb
21 c:/usr/local/lib/ruby/2.1.0/rubygems/core_ext/kernel_require.rb
22 c:/usr/local/lib/ruby/2.1.0/rubygems.rb

[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

This application has requested the Runtime to terminate it in an unusual way.

Associated revisions

Revision a7481aae - 07/14/2013 05:21 PM - nobu (Nobuyoshi Nakada)

string.c: consider old terminator

- string.c (str_fill_term): consider old terminator length, and should not use rb_enc_ascget since it depends on the current encoding which may not be compatible with the new terminator. [Bug #8634]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@41967 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 41967 - 07/14/2013 05:21 PM - nobu (Nobuyoshi Nakada)

string.c: consider old terminator

- string.c (str_fill_term): consider old terminator length, and should not use rb_enc_ascget since it depends on the current encoding which may not be compatible with the new terminator. [Bug #8634]

Revision 41967 - 07/14/2013 05:21 PM - nobu (Nobuyoshi Nakada)

string.c: consider old terminator

- string.c (str_fill_term): consider old terminator length, and should not use rb_enc_ascget since it depends on the current encoding which may not be compatible with the new terminator. [Bug #8634]

Revision 41967 - 07/14/2013 05:21 PM - nobu (Nobuyoshi Nakada)

string.c: consider old terminator

- string.c (str_fill_term): consider old terminator length, and should not use rb_enc_ascget since it depends on the current encoding which may not be compatible with the new terminator. [Bug #8634]

Revision 41967 - 07/14/2013 05:21 PM - nobu (Nobuyoshi Nakada)

string.c: consider old terminator

- string.c (str_fill_term): consider old terminator length, and should not use rb_enc_ascget since it depends on the current encoding which may not be compatible with the new terminator. [Bug #8634]

Revision 41967 - 07/14/2013 05:21 PM - nobu (Nobuyoshi Nakada)

string.c: consider old terminator

- string.c (str_fill_term): consider old terminator length, and should not use rb_enc_ascget since it depends on the current encoding which may not be compatible with the new terminator. [Bug #8634]

Revision 41967 - 07/14/2013 05:21 PM - nobu (Nobuyoshi Nakada)

string.c: consider old terminator

- string.c (str_fill_term): consider old terminator length, and should not use rb_enc_ascget since it depends on the current encoding which may not be compatible with the new terminator. [Bug #8634]

History

#1 - 07/14/2013 04:32 PM - nobu (Nobuyoshi Nakada)

- Category set to core

- Status changed from Open to Assigned

- Assignee set to nobu (Nobuyoshi Nakada)

- Priority changed from Normal to 5

- Target version set to 2.1.0

- Backport changed from 1.9.3: UNKNOWN, 2.0.0: UNKNOWN to 1.9.3: DONTNEED, 2.0.0: DONTNEED

fixing.

#2 - 07/15/2013 02:21 AM - nobu (Nobuyoshi Nakada)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r41967.
Heesob, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

---

string.c: consider old terminator

- string.c (str_fill_term): consider old terminator length, and should not use rb_enc_ascget since it depends on the current encoding which may not be compatible with the new terminator. [Bug #8634]