Ruby trunk - Bug #10127

WIN32OLE segfaults

08/12/2014 03:01 AM - nobu (Nobuyoshi Nakada)

Status:	Closed		
Priority:	Normal		
Assignee:	suke (Masaki Suketa)		
Target version:	2.2.0		
ruby -v:	trunk	**Backport:**	2.0.0: DONE, 2.1: DONE

Description

fole_initialize()では引数をStringValue()で変換していますが、ole_create_dcom()には変換前の引数がそのまま渡されています。
そのため、to_strメソッドを持つオブジェクトをホスト名とともに渡すと、不正なアクセスが起きます。
分かりやすい例では、NilClass#to_strなどを追加すればSEGVします。

https://github.com/nobu/ruby/compare/win32ole-fix

```
$ ./x64-mswin32_120/bin/ruby -rwin32ole -e 'class NilClass; alias to_str to_s; end; WIN32OLE.new(n
il, "localhost") rescue p $!.message'
-e:1: [BUG] Segmentation fault
ruby 2.2.0dev (2014-08-12 trunk 47145) [x64-mswin64_120]

-- Control frame information -----------------------------------------------
c:0004 p:---- s:0011 e:000010 CFUNC  :initialize
c:0003 p:---- s:0009 e:000008 CFUNC  :new
c:0002 p:0024 s:0004 E:001738 EVAL   -e:1 [FINISH]
c:0001 p:0000 s:0002 E:001438 TOP    [FINISH]

-- Ruby level backtrace information ----------------------------------------
-e:1:in `<main>'
-e:1:in `new'
-e:1:in `initialize'

-- C level backtrace information -------------------------------------------
C:\Windows\SYSTEM32\ntdll.dll(NtWaitForSingleObject+0xa) [0x00000000770D12FA]
C:\Windows\system32\KERNELBASE.dll(WaitForSingleObjectEx+0x9c) [0x000007FEFD1D10DC]
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(rb_print_backtrace+0x34) [0
x000007FEF12A39C4] c:\users\nobu\work\ruby\trunk\src\vm_dump.c:711
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(rb_vm_bugreport+0x6f) [0x00
0007FEF12A3A3B] c:\users\nobu\work\ruby\trunk\src\vm_dump.c:973
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(rb_bug_context+0x5e) [0x000
007FEF11EF09A] c:\users\nobu\work\ruby\trunk\src\error.c:391
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(sigsegv+0x69) [0x000007FEF1
252701] c:\users\nobu\work\ruby\trunk\src\signal.c:831
C:\Windows\system32\MSVCR120.dll(XcptFilter+0x1a9) [0x000007FEF4A0FC99]
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\ruby.exe(__tmainCRTStartup$filt$0+0x16) [0x000000013
F8B16D6] f:\dd\vctools\crt\crtw32\dllstuff\crtexe.c:666
C:\Windows\system32\MSVCR120.dll(_C_specific_handler+0x93) [0x000007FEF4A0F2CB]
C:\Windows\SYSTEM32\ntdll.dll(RtlDecodePointer+0xad) [0x00000000770A9D2D]
C:\Windows\SYSTEM32\ntdll.dll(RtlUnwindEx+0xbbf) [0x00000000770991CF]
C:\Windows\SYSTEM32\ntdll.dll(KiUserExceptionDispatcher+0x2e) [0x00000000770D1248]
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\lib\ruby\2.2.0\x64-mswin64_120\win32ole.so(ole_encod
ing2cp+0x9) [0x000007FEFA0F6A89] c:\users\nobu\work\ruby\trunk\src\ext\win32ole\win32ole.c:638
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\lib\ruby\2.2.0\x64-mswin64_120\win32ole.so(ole_vstr2
wc+0x47) [0x000007FEFA0FA4A3] c:\users\nobu\work\ruby\trunk\src\ext\win32ole\win32ole.c:1017
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\lib\ruby\2.2.0\x64-mswin64_120\win32ole.so(ole_creat
e_dcom+0xad) [0x000007FEFA0F6761] c:\users\nobu\work\ruby\trunk\src\ext\win32ole\win32ole.c:2317
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\lib\ruby\2.2.0\x64-mswin64_120\win32ole.so(fole_init
ialize+0xeb) [0x000007FEFA0F3BE7] c:\users\nobu\work\ruby\trunk\src\ext\win32ole\win32ole.c:2904
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(vm_call0_cfunc_with_frame+0
x11b) [0x000007FEF11E3E07] c:\users\nobu\work\ruby\trunk\src\vm_eval.c:124
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(vm_call0_body+0x31c) [0x000
007FEF11E3C74] c:\users\nobu\work\ruby\trunk\src\vm_eval.c:179
```

```
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(vm_call0+0x44) [0x000007FEF
11E3950] c:\users\nobu\work\ruby\trunk\src\vm_eval.c:55
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(rb_call0+0xae) [0x000007FEF
11DF1EE] c:\users\nobu\work\ruby\trunk\src\vm_eval.c:334
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(rb_funcallv+0x25) [0x000007
FEF11E0289] c:\users\nobu\work\ruby\trunk\src\vm_eval.c:811
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(rb_class_new_instance+0x2c)
 [0x000007FEF11FF394] c:\users\nobu\work\ruby\trunk\src\object.c:1879
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(vm_call_cfunc_with_frame+0x
12d) [0x000007FEF11E4105] c:\users\nobu\work\ruby\trunk\src\vm_insnhelper.c:1522
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(vm_call_general+0x3d9) [0x0
00007FEF11E4589] c:\users\nobu\work\ruby\trunk\src\vm_insnhelper.c:1957
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(vm_exec_core+0xf96) [0x0000
07FEF11E7D3E] c:\users\nobu\work\ruby\trunk\x64-mswin32_120\vm.inc:1422
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(vm_exec+0xb9) [0x000007FEF1
1E65B9] c:\users\nobu\work\ruby\trunk\src\vm.c:1377
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(rb_iseq_eval_main+0x81) [0x
000007FEF11E04F1] c:\users\nobu\work\ruby\trunk\src\vm.c:1647
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(ruby_exec_internal+0xcb) [0
x000007FEF11A6FA3] c:\users\nobu\work\ruby\trunk\src\eval.c:255
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(ruby_exec_node+0x1d) [0x000
007FEF11A6FFD] c:\users\nobu\work\ruby\trunk\src\eval.c:318
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\x64-msvcr120-ruby220.dll(ruby_run_node+0x30) [0x0000
07FEF11A728C] c:\users\nobu\work\ruby\trunk\src\eval.c:309
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\ruby.exe(main+0x40) [0x000000013F8B1040] c:\users\no
bu\work\ruby\trunk\src\main.c:38
C:\Users\nobu\work\ruby\trunk\x64-mswin32_120\ruby.exe(__tmainCRTStartup+0x10f) [0x000000013F8B12A
7] f:\dd\vctools\crt\crtw32\dllstuff\crtexe.c:626
C:\Windows\system32\kernel32.dll(BaseThreadInitThunk+0xd) [0x0000000076E759ED]

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

* Loaded script: -e

* Loaded features:

    0 enumerator.so
    1 C:/Users/nobu/work/ruby/trunk/x64-mswin32_120/lib/ruby/2.2.0/x64-mswin64_120/enc/encdb.so
    2 C:/Users/nobu/work/ruby/trunk/x64-mswin32_120/lib/ruby/2.2.0/x64-mswin64_120/enc/windows_31j
.so
    3 C:/Users/nobu/work/ruby/trunk/x64-mswin32_120/lib/ruby/2.2.0/x64-mswin64_120/enc/trans/trans
db.so
    4 C:/Users/nobu/work/ruby/trunk/x64-mswin32_120/lib/ruby/2.2.0/x64-mswin64_120/win32ole.so

[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
```

Associated revisions

Revision eac5e58b - 08/12/2014 12:51 PM - suke (Masaki Suketa)

- ext/win32ole/win32ole.c (ole_create_dcom): use the converted result if the argument can be converted to a string, to get rid of invalid access. Thanks to nobu. [ruby-dev:48467] [Bug #10127]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@47153 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 47153 - 08/12/2014 12:51 PM - suke (Masaki Suketa)

- ext/win32ole/win32ole.c (ole_create_dcom): use the converted result if the argument can be converted to a string, to get rid of invalid access. Thanks to nobu. [ruby-dev:48467] [Bug #10127]

Revision 47153 - 08/12/2014 12:51 PM - suke (Masaki Suketa)

- ext/win32ole/win32ole.c (ole_create_dcom): use the converted result if the argument can be converted to a string, to get rid of invalid access.

Thanks to nobu. [ruby-dev:48467] [Bug #10127]

Revision 47153 - 08/12/2014 12:51 PM - suke (Masaki Suketa)

- ext/win32ole/win32ole.c (ole_create_dcom): use the converted result if the argument can be converted to a string, to get rid of invalid access. Thanks to nobu. [ruby-dev:48467] [Bug #10127]

Revision 47153 - 08/12/2014 12:51 PM - suke (Masaki Suketa)

- ext/win32ole/win32ole.c (ole_create_dcom): use the converted result if the argument can be converted to a string, to get rid of invalid access. Thanks to nobu. [ruby-dev:48467] [Bug #10127]

Revision 47153 - 08/12/2014 12:51 PM - suke (Masaki Suketa)

- ext/win32ole/win32ole.c (ole_create_dcom): use the converted result if the argument can be converted to a string, to get rid of invalid access. Thanks to nobu. [ruby-dev:48467] [Bug #10127]

Revision 47153 - 08/12/2014 12:51 PM - suke (Masaki Suketa)

- ext/win32ole/win32ole.c (ole_create_dcom): use the converted result if the argument can be converted to a string, to get rid of invalid access. Thanks to nobu. [ruby-dev:48467] [Bug #10127]

Revision 9fa0d836 - 08/30/2014 04:09 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r47153: [Backport #10127]

```
    * ext/win32ole/win32ole.c (ole_create_dcom): use the converted
      result if the argument can be converted to a string, to get rid
      of invalid access. Thanks to nobu. [ruby-dev:48467] [Bug #10127]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@47325 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 47325 - 08/30/2014 04:09 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r47153: [Backport #10127]

```
* ext/win32ole/win32ole.c (ole_create_dcom): use the converted
  result if the argument can be converted to a string, to get rid
  of invalid access. Thanks to nobu. [ruby-dev:48467] [Bug #10127]
```

Revision cd171e48 - 09/05/2014 05:10 AM - usa (Usaku NAKAMURA)

merge revision(s) 47153: [Backport #10127]

```
    * ext/win32ole/win32ole.c (ole_create_dcom): use the converted
      result if the argument can be converted to a string, to get rid
      of invalid access. Thanks to nobu. [ruby-dev:48467] [Bug #10127]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_0_0@47405 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 47405 - 09/05/2014 05:10 AM - usa (Usaku NAKAMURA)

merge revision(s) 47153: [Backport #10127]

```
* ext/win32ole/win32ole.c (ole_create_dcom): use the converted
  result if the argument can be converted to a string, to get rid
  of invalid access. Thanks to nobu. [ruby-dev:48467] [Bug #10127]
```

History

#1 - 08/12/2014 12:51 PM - suke (Masaki Suketa)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

Applied in changeset r47153.

- ext/win32ole/win32ole.c (ole_create_dcom): use the converted result if the argument can be converted to a string, to get rid of invalid access. Thanks to nobu. [ruby-dev:48467] [Bug #10127]

#2 - 08/30/2014 04:09 PM - nagachika (Tomoyuki Chikanaga)

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

Backported into ruby_2_1 branch at r47325.

#3 - 09/05/2014 05:10 AM - usa (Usaku NAKAMURA)

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

backported into ruby_2_0_0 at r47405.