Ruby 1.8 - Bug #2794

Aborted (core dumped) BUG on Ruby/DL

02/26/2010 01:37 PM - zophos (Takao NISHI)

Status:	Closed
Priority:	Normal
Assignee:	knu (Akinori MUSHA)
Target version:	Ruby 1.8.8
ruby -v:	ruby 1.8.6 (2007-09-24 patchlevel 111) [i486-linux], ruby 1.8.7 (2008-08-11 patchlevel 72) [i386-cygwin], ruby 1.8.8dev (2010-06-08 revision 27061) [x86_64-linux]

Description

=begin
□□□□□□□core dump□□□□

$ ruby -rdl/import -e 's=DL.strdup("\0"*1024);s[0,1023]="\xff"'
** glibc detected *** ruby: free(): invalid next size (fast): 0x0808ec18 ***
======= Backtrace: =========
/lib/tls/i686/cmov/libc.so.6[0xb7cdea85]
/lib/tls/i686/cmov/libc.so.6(cfree+0x90)[0xb7ce24f0]
/usr/lib/libruby1.8.so.1.8(ruby_xfree+0x37)[0xb7e79ac7]
/usr/lib/ruby/1.8/i486-linux/dl.so(dlfree+0x1d)[0xb7c36a7d]
/usr/lib/ruby/1.8/i486-linux/dl.so(dlptr_free+0x2f)[0xb7c398df]
/usr/lib/libruby1.8.so.1.8(rb_gc_call_finalizer_at_exit+0xa7)[0xb7e79d97]
/usr/lib/libruby1.8.so.1.8[0xb7e5f997]
/usr/lib/libruby1.8.so.1.8(ruby_cleanup+0x100)[0xb7e67b90]
/usr/lib/libruby1.8.so.1.8(ruby_stop+0x1d)[0xb7e67cdd]
/usr/lib/libruby1.8.so.1.8[0xb7e72d51]
ruby[0x80486bd]
/lib/tls/i686/cmov/libc.so.6(__libc_start_main+0xe0)[0xb7c89450]
ruby[0x8048601]
======= Memory map: ========
08048000-08049000 r-xp 00000000 08:04 20186180 /usr/bin/ruby1.8
08049000-0804a000 rw-p 00000000 08:04 20186180 /usr/bin/ruby1.8
0804a000-080ad000 rw-p 0804a000 00:00 0 [heap]
b7b00000-b7b21000 rw-p b7b00000 00:00 0
b7b21000-b7c00000 ---p b7b21000 00:00 0
b7c2c000-b7c3f000 r-xp 00000000 08:04 20283415 /usr/lib/ruby/1.8/i486-linux/dl.so
b7c3f000-b7c40000 rw-p 00012000 08:04 20283415 /usr/lib/ruby/1.8/i486-linux/dl.so
b7c40000-b7c73000 rw-p b7c40000 00:00 0
b7c73000-b7dbc000 r-xp 00000000 08:04 2195508 /lib/tls/i686/cmov/libc-2.7.so
b7dbc000-b7dbd000 r--p 00149000 08:04 2195508 /lib/tls/i686/cmov/libc-2.7.so
b7dbd000-b7dbf000 rw-p 0014a000 08:04 2195508 /lib/tls/i686/cmov/libc-2.7.so
b7dbf000-b7dc2000 rw-p b7dbf000 00:00 0
b7dc2000-b7de5000 r-xp 00000000 08:04 2195520 /lib/tls/i686/cmov/libm-2.7.so
b7de5000-b7de7000 rw-p 00023000 08:04 2195520 /lib/tls/i686/cmov/libm-2.7.so
b7de7000-b7df0000 r-xp 00000000 08:04 2195517 /lib/tls/i686/cmov/libcrypt-2.7.so
b7df0000-b7df2000 rw-p 00008000 08:04 2195517 /lib/tls/i686/cmov/libcrypt-2.7.so
b7df2000-b7e19000 rw-p b7df2000 00:00 0
b7e19000-b7e1b000 r-xp 00000000 08:04 2195518 /lib/tls/i686/cmov/libdl-2.7.so
b7e1b000-b7e1d000 rw-p 00001000 08:04 2195518 /lib/tls/i686/cmov/libdl-2.7.so
b7e1d000-b7e1e000 rw-p b7e1d000 00:00 0
b7e1e000-b7e32000 r-xp 00000000 08:04 2195546 /lib/tls/i686/cmov/libpthread-2.7.so
b7e32000-b7e34000 rw-p 00013000 08:04 2195546 /lib/tls/i686/cmov/libpthread-2.7.so
b7e34000-b7e36000 rw-p b7e34000 00:00 0
b7e36000-b7ef4000 r-xp 00000000 08:04 20185223 /usr/lib/libruby1.8.so.1.8.6
b7ef4000-b7ef6000 rw-p 000be000 08:04 20185223 /usr/lib/libruby1.8.so.1.8.6
b7ef6000-b7f06000 rw-p b7ef6000 00:00 0
b7f0d000-b7f17000 r-xp 00000000 08:04 2195478 /lib/libgcc_s.so.1

```
b7f17000-b7f18000 rw-p 0000a000 08:04 2195478    /lib/libgcc_s.so.1
b7f18000-b7f1b000 rw-p b7f18000 00:00 0
b7f1b000-b7f1c000 r-xp b7f1b000 00:00 0          [vdso]
b7f1c000-b7f36000 r-xp 00000000 08:04 2195669    /lib/ld-2.7.so
b7f36000-b7f38000 rw-p 00019000 08:04 2195669    /lib/ld-2.7.so
bfd7c000-bfd91000 rw-p bffeb000 00:00 0          [stack]
Aborted (core dumped)
```

以下のコードでは問題ないのでDL.strdupの問題と思われます

```
ruby -rdl/import -e 's=DL.malloc(1024);s[0,1023]="\xff"'
```

=end

Associated revisions

Revision 96b19c48a5dee648b51b72e63c3ec0fed90caaff - 06/10/2010 05:51 AM - knu (Akinori MUSHA)

- ext/dl/dl.c (rb_dl_strdup): strdup() only allocates a buffer of strlen()+1 bytes. [Bug #2794]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_8@28250 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 96b19c48 - 06/10/2010 05:51 AM - knu (Akinori MUSHA)

- ext/dl/dl.c (rb_dl_strdup): strdup() only allocates a buffer of strlen()+1 bytes. [Bug #2794]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_8@28250 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 28250 - 06/10/2010 05:51 AM - knu (Akinori MUSHA)

- ext/dl/dl.c (rb_dl_strdup): strdup() only allocates a buffer of strlen()+1 bytes. [Bug #2794]

History

#1 - 02/26/2010 10:30 PM - kosaki (Motohiro KOSAKI)

=begin
以下の環境で再現（i.e. fedora12 on x86_64）

ruby 1.8.6 (2009-08-04 patchlevel 383) [x86_64-linux]
=end

#2 - 02/26/2010 10:47 PM - kosaki (Motohiro KOSAKI)

=begin
DL.strdup("\0"*1024)はlibcのstrdupを呼び出すのでC言語のstrdupの仕様に従いstrdup("\0")を実行し１バイトバッファを作ります。
なので、仕様のような気もします

=end

#3 - 02/26/2010 11:13 PM - zophos (Takao NISHI)

=begin
p DL.strdup("\x0"*1024)
#

とsizeが1024と認識されているので，やはり問題が存在すると思われます。
=end

#4 - 02/26/2010 11:30 PM - kosaki (Motohiro KOSAKI)

=begin
DLなのでlibcのstrdupを呼ぶのが仕様なのではないか？ つまり、RStringのsize=1024は無視するのが仕様なのではないのか？ という疑問があります。と書いたつもりでした。舌足らずですいません
=end

#5 - 02/27/2010 12:22 AM - kosaki (Motohiro KOSAKI)

- File 0001-sanity-DL-strdup.patch added

=begin
添付のパッチで comment#3で指摘された size=1024の問題は直ります。

=end

#6 - 06/08/2010 09:45 PM - shyouhei (Shyouhei Urabe)

- Status changed from Open to Assigned

- Assignee set to shyouhei (Shyouhei Urabe)

=begin
あとで読む。
=end

#7 - 06/10/2010 02:30 PM - shyouhei (Shyouhei Urabe)

- Assignee changed from shyouhei (Shyouhei Urabe) to knu (Akinori MUSHA)

- Target version set to Ruby 1.8.8

- ruby -v changed from ruby 1.8.6 (2007-09-24 patchlevel 111) [i486-linux], ruby 1.8.7 (2008-08-11 patchlevel 72) [i386-cygwin] to ruby 1.8.6 (2007-09-24 patchlevel 111) [i486-linux], ruby 1.8.7 (2008-08-11 patchlevel 72) [i386-cygwin], ruby 1.8.8dev (2010-06-08 revision 27061) [x86_64-linux]

=begin
たらい回しにしてごめんなさい、これはstrdupなのだからstrlenから計算する長さが本来の定義であるように私も思います。
ゴーサインがでればこちらでコミットします。
=end

#8 - 06/10/2010 02:44 PM - knu (Akinori MUSHA)

=begin
あ、これはstrlen()+1が圧倒的に正しいですね。入れます。
=end

#9 - 06/10/2010 02:57 PM - knu (Akinori MUSHA)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

=begin
This issue was solved with changeset r28250.
Takao, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

=end

Files

0001-sanity-DL-strdup.patch	536 Bytes	02/27/2010	kosaki (Motohiro KOSAKI)