Ruby trunk - Bug #7312

test_str_crypt(TestM17NComb) fails

11/09/2012 12:41 AM - vo.x (Vit Ondruch)

Status:	Closed		
Priority:	Normal		
Assignee:	naruse (Yui NARUSE)		
Target version:	2.0.0		
ruby -v:	ruby 2.0.0dev (2012-11-19 trunk 37735) [x86_64-linux]	**Backport:**	

Description

=begin
test_str_crypt(TestM17NComb):
ArgumentError: NULL pointer given
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/test_m17n_comb.rb:728:in crypt'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/test_m17n_comb.rb:728:inblock in test_str_crypt'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/allpairs.rb:83:in block in each'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/allpairs.rb:75:inblock in each_index'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/allpairs.rb:46:in block in make_large_block'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/allpairs.rb:26:inblock (2 levels) in make_basic_block'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/allpairs.rb:21:in times'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/allpairs.rb:21:inblock in make_basic_block'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/allpairs.rb:20:in times'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/allpairs.rb:20:inmake_basic_block'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/allpairs.rb:45:in make_large_block'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/allpairs.rb:71:ineach_index'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/allpairs.rb:82:in each'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/test_m17n_comb.rb:60:incombination'
/builddir/build/BUILD/ruby-2.0.0-r37564/test/ruby/test_m17n_comb.rb:723:in `test_str_crypt'
=end

Associated revisions

Revision dfb44fee - 11/09/2012 04:06 AM - naruse (Yui NARUSE)

- string.c (rb_str_crypt): crypt(3) may return NULL. Latest glibc (2.16?) crypt(3) actually returns NULL. [Bug #7312]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@37572 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 37572 - 11/09/2012 04:06 AM - naruse (Yui NARUSE)

- string.c (rb_str_crypt): crypt(3) may return NULL. Latest glibc (2.16?) crypt(3) actually returns NULL. [Bug #7312]

Revision 37572 - 11/09/2012 04:06 AM - naruse (Yui NARUSE)

- string.c (rb_str_crypt): crypt(3) may return NULL. Latest glibc (2.16?) crypt(3) actually returns NULL. [Bug #7312]

Revision 37572 - 11/09/2012 04:06 AM - naruse (Yui NARUSE)

- string.c (rb_str_crypt): crypt(3) may return NULL. Latest glibc (2.16?) crypt(3) actually returns NULL. [Bug #7312]

Revision 37572 - 11/09/2012 04:06 AM - naruse (Yui NARUSE)

- string.c (rb_str_crypt): crypt(3) may return NULL. Latest glibc (2.16?) crypt(3) actually returns NULL. [Bug #7312]

Revision 37572 - 11/09/2012 04:06 AM - naruse (Yui NARUSE)

- string.c (rb_str_crypt): crypt(3) may return NULL. Latest glibc (2.16?) crypt(3) actually returns NULL. [Bug #7312]

Revision 37572 - 11/09/2012 04:06 AM - naruse (Yui NARUSE)

- string.c (rb_str_crypt): crypt(3) may return NULL. Latest glibc (2.16?) crypt(3) actually returns NULL. [Bug #7312]

Revision 64757d28 - 11/11/2012 08:15 AM - naruse (Yui NARUSE)

glibc 2.16 or later denies salt contained other than [0-9A-Za-z./] [Bug #7312]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@37622 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 37622 - 11/11/2012 08:15 AM - naruse (Yui NARUSE)

glibc 2.16 or later denies salt contained other than [0-9A-Za-z./] [Bug #7312]

Revision 37622 - 11/11/2012 08:15 AM - naruse (Yui NARUSE)

glibc 2.16 or later denies salt contained other than [0-9A-Za-z./] [Bug #7312]

Revision 37622 - 11/11/2012 08:15 AM - naruse (Yui NARUSE)

glibc 2.16 or later denies salt contained other than [0-9A-Za-z./] [Bug #7312]

Revision 37622 - 11/11/2012 08:15 AM - naruse (Yui NARUSE)

glibc 2.16 or later denies salt contained other than [0-9A-Za-z./] [Bug #7312]

Revision 37622 - 11/11/2012 08:15 AM - naruse (Yui NARUSE)

glibc 2.16 or later denies salt contained other than [0-9A-Za-z./] [Bug #7312]

Revision 37622 - 11/11/2012 08:15 AM - naruse (Yui NARUSE)

glibc 2.16 or later denies salt contained other than [0-9A-Za-z./] [Bug #7312]

Revision bf445c24 - 11/20/2012 01:09 PM - naruse (Yui NARUSE)

fix guards for glibc crypt(3) see #7312

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@37766 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 37766 - 11/20/2012 01:09 PM - naruse (Yui NARUSE)

fix guards for glibc crypt(3) see #7312

Revision 37766 - 11/20/2012 01:09 PM - naruse (Yui NARUSE)

fix guards for glibc crypt(3) see #7312

Revision 37766 - 11/20/2012 01:09 PM - naruse (Yui NARUSE)

fix guards for glibc crypt(3) see #7312

Revision 37766 - 11/20/2012 01:09 PM - naruse (Yui NARUSE)

fix guards for glibc crypt(3) see #7312

Revision 37766 - 11/20/2012 01:09 PM - naruse (Yui NARUSE)

fix guards for glibc crypt(3) see #7312

Revision 37766 - 11/20/2012 01:09 PM - naruse (Yui NARUSE)

fix guards for glibc crypt(3) see #7312

Revision 9d71f70d - 11/20/2012 03:29 PM - naruse (Yui NARUSE)

- test/ruby/test_m17n_comb.rb (test_str_crypt): Use RbConfig to get libc's directory. Patched by Vit Ondruch [ruby-core:49763] [Bug #7312]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@37773 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 37773 - 11/20/2012 03:29 PM - naruse (Yui NARUSE)

- test/ruby/test_m17n_comb.rb (test_str_crypt): Use RbConfig to get libc's directory. Patched by Vit Ondruch [ruby-core:49763] [Bug #7312]

Revision 37773 - 11/20/2012 03:29 PM - naruse (Yui NARUSE)

- test/ruby/test_m17n_comb.rb (test_str_crypt): Use RbConfig to get libc's directory. Patched by Vit Ondruch [ruby-core:49763] [Bug #7312]

Revision 37773 - 11/20/2012 03:29 PM - naruse (Yui NARUSE)

- test/ruby/test_m17n_comb.rb (test_str_crypt): Use RbConfig to get libc's directory. Patched by Vit Ondruch [ruby-core:49763] [Bug #7312]

Revision 37773 - 11/20/2012 03:29 PM - naruse (Yui NARUSE)

- test/ruby/test_m17n_comb.rb (test_str_crypt): Use RbConfig to get libc's directory. Patched by Vit Ondruch [ruby-core:49763] [Bug #7312]

Revision 37773 - 11/20/2012 03:29 PM - naruse (Yui NARUSE)

- test/ruby/test_m17n_comb.rb (test_str_crypt): Use RbConfig to get libc's directory. Patched by Vit Ondruch [ruby-core:49763] [Bug #7312]

Revision 37773 - 11/20/2012 03:29 PM - naruse (Yui NARUSE)

- test/ruby/test_m17n_comb.rb (test_str_crypt): Use RbConfig to get libc's directory. Patched by Vit Ondruch [ruby-core:49763] [Bug #7312]

Revision d92d9a26 - 12/20/2012 09:38 AM - usa (Usaku NAKAMURA)

merge revision(s) 37572,37622,37766,37773: [Backport #7527]

```
* string.c (rb_str_crypt): crypt(3) may return NULL.
  Latest glibc (2.16?) crypt(3) actually returns NULL. [Bug #7312]

* test/ruby/test_m17n_comb.rb (test_str_crypt): Use RbConfig to get
  libc's directory. Patched by Vit Ondruch [ruby-core:49763] [Bug #7312]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@38503 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 11/09/2012 01:16 AM - mame (Yusuke Endoh)

- Target version set to 2.0.0

I cannot reproduce. Anyone?

--
Yusuke Endoh mame@tsg.ne.jp

#2 - 11/09/2012 02:16 AM - vo.x (Vit Ondruch)

I observe the test error on Fedora Rawhide. Could it be because of some "too new" external library?

#3 - 11/09/2012 01:06 PM - naruse (Yui NARUSE)

- Status changed from Open to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r37572.
Vit, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- string.c (rb_str_crypt): crypt(3) may return NULL. Latest glibc (2.16?) crypt(3) actually returns NULL. [Bug #7312]

#4 - 11/09/2012 01:26 PM - naruse (Yui NARUSE)

- Status changed from Closed to Feedback

- Assignee set to naruse (Yui NARUSE)

vo.x (Vit Ondruch) wrote:

> I observe the test error on Fedora Rawhide. Could it be because of some "too new" external library?

As I wrote in the commit, it seems because of glibc's crypt(3)'s change.
(the fundamental reason is ruby hadn't treat the case crypt(3) returns NULL even if POSIX describe it)
Could you inspect when crypt(3) returns NULL?

#5 - 11/09/2012 08:10 PM - vo.x (Vit Ondruch)

=begin
This is reduced test case:

def test_str_crypt
str = ""
salt = e("\xa1\xa1")

```
if a(salt).length < 2
  assert_raise(ArgumentError) { str.crypt(salt) }
end

t = str.crypt(salt)
assert_equal(a(str).crypt(a(salt)), t, "#{encdump(str)}.crypt(#{encdump(salt)})")
assert_encoding('ASCII-8BIT', t.encoding)
```

end

And GDB session:

6916 StringValue(salt);
(gdb)
6917 if (RSTRING_LEN(salt) < 2)
(gdb)
6920 s = RSTRING_PTR(str);
(gdb)
6922 saltp = RSTRING_PTR(salt);
(gdb)
6931 result = rb_str_new2(crypt(s, saltp));
(gdb) s
rb_str_new_cstr (ptr=0x0) at string.c:435
435 if (!ptr) {

So the crypt(3) definitely returns NULL for e("\xa1\xa1").

BTW this is my glibc version:

$ rpm -q glibc
glibc-2.16.90-28.fc19.x86_64

And this [1] might be the offending patch, particularly the crypt/crypt-entry.c change? It seems that they are now stricter what might be salt now.

[1] ((URL:http://sourceware.org/git/?p=glibc.git;a=commitdiff;h=4ba74a357376c8f8bf49487f96ae71cf2460c3f3))
=end

#6 - 11/09/2012 08:59 PM - vo.x (Vit Ondruch)

- ruby -v changed from ruby 2.0.0dev (2012-11-08 trunk 37564) [x86_64-linux] to ruby 2.0.0dev (2012-11-09 trunk 37589) [x86_64-linux]

=begin
The unit test still fails:

test_str_crypt(TestM17NComb):
Errno::EINVAL: Invalid argument - crypt
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/test_m17n_comb.rb:728:in crypt'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/test_m17n_comb.rb:728:inblock in test_str_crypt'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/allpairs.rb:83:in block in each'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/allpairs.rb:75:inblock in each_index'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/allpairs.rb:46:in block in make_large_block'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/allpairs.rb:26:inblock (2 levels) in make_basic_block'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/allpairs.rb:21:in times'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/allpairs.rb:21:inblock in make_basic_block'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/allpairs.rb:20:in times'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/allpairs.rb:20:inmake_basic_block'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/allpairs.rb:45:in make_large_block'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/allpairs.rb:71:ineach_index'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/allpairs.rb:82:in each'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/test_m17n_comb.rb:60:incombination'
/builddir/build/BUILD/ruby-2.0.0-r37589/test/ruby/test_m17n_comb.rb:723:in `test_str_crypt'

=end

#7 - 11/10/2012 07:41 PM - mtasaka (Mamoru Tasaka)

Test case:

```
#define _XOPEN_SOURCE
#include
#include
#include
#include

int main(void){
const char *key = "";
const char *salt = "\xa1\xa1";

char *ret = crypt(key, salt);
int errno_save = errno;
printf("crypt returned val: %p\n", ret);
if (!ret){
    printf("Errno: %d %s\n", errno_save, strerror(errno_save));
}
while (ret && *ret){
    printf("char: %c\n", *ret++);
}

return 0;

}
```

With glibc 2.16-20.fc18.i686
$ gcc -Wall -Wextra -O2 -g -o test-crypt test-crypt.c -lcrypt && ./test-crypt
crypt returned val: 0x45b83140
char: ?
char: ?
char: z
char: U
char: w
char: S
char: p
char: 9
char: H
char: 4
char: n
char: 3
char: Y

With glibc 2.16.90-28.fc19.i686
gcc -Wall -Wextra -O2 -g -o test-crypt test-crypt.c -lcrypt && ./test-crypt
crypt returned val: (nil)
Errno: 22 Invalid argument

Note "Invalid argument". man 3p crypt says:

The salt argument is a string chosen from the set:

```
        a b c d e f g h i j k l m n o p q r s t u v w x y z
        A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
        0 1 2 3 4 5 6 7 8 9 . /
```

---

so "STRINGS" in test/ruby/test_m17n_comb.rb seems what should
not passed to salt argument for crypt(3).

#8 - 11/10/2012 07:42 PM - mtasaka (Mamoru Tasaka)

Note that this test (test/ruby/test_m17n_comb.rb) also fails with
ruby 1.9.3p327 with rawhide glibc.

#9 - 11/11/2012 05:15 PM - naruse (Yui NARUSE)

- Status changed from Feedback to Closed

This issue was solved with changeset r37622.

Vit, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

---

glibc 2.16 or later denies salt contained other than [0-9A-Za-z./] [Bug #7312]

#10 - 11/11/2012 10:53 PM - kosaki (Motohiro KOSAKI)

I guess following discussion is a source of this bug.

http://sourceware-org.1504.n7.nabble.com/RFC-FIPS-compliance-and-other-crypt-3-improvements-td6884.html

#11 - 11/20/2012 09:45 PM - vo.x (Vit Ondruch)

- Status changed from Closed to Open

- % Done changed from 100 to 30

- ruby -v changed from ruby 2.0.0dev (2012-11-09 trunk 37589) [x86_64-linux] to ruby 2.0.0dev (2012-11-19 trunk 37735) [x86_64-linux]

=begin
The fix does not fully work. There are at lease three issues:

(1) It does not work on 64b system, since libc is located in /usr/lib64
(2) The glibcver <=> [2, 16] compares array of strings with array of integers, which returns nil and therefor raises exception.
(3) Even if I force the strict crypt, it fails with
1) Error:
test_str_crypt(TestM17NComb):
ArgumentError: invalid byte sequence in EUC-JP
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/test_m17n_comb.rb:732:in block in test_str_crypt'
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/allpairs.rb:83:inblock in each'
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/allpairs.rb:75:in block in each_index'
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/allpairs.rb:46:inblock in make_large_block'
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/allpairs.rb:26:in block (2 levels) in make_basic_block'
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/allpairs.rb:21:intimes'
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/allpairs.rb:21:in block in make_basic_block'
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/allpairs.rb:20:intimes'
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/allpairs.rb:20:in make_basic_block'
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/allpairs.rb:45:inmake_large_block'
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/allpairs.rb:71:in each_index'
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/allpairs.rb:82:ineach'
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/test_m17n_comb.rb:60:in combination'
/builddir/build/BUILD/ruby-2.0.0-r37735/test/ruby/test_m17n_comb.rb:730:intest_str_crypt'

=end

#12 - 11/20/2012 10:14 PM - naruse (Yui NARUSE)

vo.x (Vit Ondruch) wrote:

> The fix does not fully work. There are at lease three issues:
>
> (1) It does not work on 64b system, since libc is located in /usr/lib64
> (2) The glibcver <=> [2, 16] compares array of strings with array of integers, which returns nil and therefor raises exception.
> (3) Even if I force the strict crypt, it fails with

I fix (2) and (3) at r37766.

For (1), I cannot find suitable way.
Could you make a patch?

#13 - 11/20/2012 11:46 PM - vo.x (Vit Ondruch)

- File 0001-Search-for-arch-specific-libc-location.patch added

naruse (Yui NARUSE) wrote:

> For (1), I cannot find suitable way.
> Could you make a patch?

This should work.

#14 - 11/21/2012 12:30 AM - naruse (Yui NARUSE)

- Status changed from Open to Closed

- % Done changed from 30 to 100

This issue was solved with changeset r37773.
Vit, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- test/ruby/test_m17n_comb.rb (test_str_crypt): Use RbConfig to get libc's directory. Patched by Vit Ondruch [ruby-core:49763] [Bug #7312]

Files

0001-Search-for-arch-specific-libc-location.patch	965 Bytes	11/20/2012	vo.x (Vit Ondruch)