Ruby master - Bug #4456

Time#strftime □ %F □□□□□□□□□□□□□□□□□□□

03/02/2011 07:52 PM - tadf (tadayoshi funaba)

Status:	Closed		
Priority:	Normal		
Assignee:	ngoto (Naohisa Goto)		
Target version:	1.9.3		
ruby -v:	-	**Backport:**	

Description

=begin
$ ruby -e "Time.now.strftime('%100000F')"
-e:1: [BUG] Segmentation fault
ruby 1.9.3dev (2011-03-02) [i686-linux]

-- Control frame information ---
c:0004 p:---- s:0010 b:0010 l:000009 d:000009 CFUNC :(null)
c:0003 p:0023 s:0006 b:0006 l:000d2c d:00034c EVAL -e:1
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:000d2c d:000d2c TOP

-- Ruby level backtrace information --
-e:1:in `'
Segmentation fault
=end

Related issues:

Related to Ruby master - Bug #4457: Time#strftime □ %z □□□□□□□□□□□□□□□□□□□□□	**Closed**	**03/02/2011**

Associated revisions

Revision 7bb73a08 - 03/03/2011 05:28 AM - naruse (Yui NARUSE)

- strftime.c (STRFTIME): return 0 and ERANGE when precision is too large. [ruby-dev:43284] fixes #4456

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@31011 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 31011 - 03/03/2011 05:28 AM - naruse (Yui NARUSE)

- strftime.c (STRFTIME): return 0 and ERANGE when precision is too large. [ruby-dev:43284] fixes #4456

Revision 31011 - 03/03/2011 05:28 AM - naruse (Yui NARUSE)

- strftime.c (STRFTIME): return 0 and ERANGE when precision is too large. [ruby-dev:43284] fixes #4456

Revision 31011 - 03/03/2011 05:28 AM - naruse (Yui NARUSE)

- strftime.c (STRFTIME): return 0 and ERANGE when precision is too large. [ruby-dev:43284] fixes #4456

Revision 31011 - 03/03/2011 05:28 AM - naruse (Yui NARUSE)

- strftime.c (STRFTIME): return 0 and ERANGE when precision is too large. [ruby-dev:43284] fixes #4456

Revision 31011 - 03/03/2011 05:28 AM - naruse (Yui NARUSE)

- strftime.c (STRFTIME): return 0 and ERANGE when precision is too large. [ruby-dev:43284] fixes #4456

Revision 31011 - 03/03/2011 05:28 AM - naruse (Yui NARUSE)

- strftime.c (STRFTIME): return 0 and ERANGE when precision is too large. [ruby-dev:43284] fixes #4456

Revision 6b47d60e - 05/28/2011 11:31 PM - yugui (Yuki Sonoda)

- strftime.c (STRFTIME): return 0 and ERANGE when precision is too large. [ruby-dev:43284] fixes #4456
  based on r31011.

- test/test_time.rb (TestTime#test_huge_precision): test for #4456.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_2@31770 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 31858 - 05/31/2011 03:59 AM - yugui (Yuki Sonoda)

- strftime.c (rb_strftime_with_timespec): improved style consistency.
  constified some variables.

- test/test_time.rb (TestTime#test_huge_precision): test for #4456.

Revision 31858 - 05/31/2011 03:59 AM - yugui (Yuki Sonoda)

- strftime.c (rb_strftime_with_timespec): improved style consistency.
  constified some variables.

- test/test_time.rb (TestTime#test_huge_precision): test for #4456.

Revision 31858 - 05/31/2011 03:59 AM - yugui (Yuki Sonoda)

- strftime.c (rb_strftime_with_timespec): improved style consistency.
  constified some variables.

- test/test_time.rb (TestTime#test_huge_precision): test for #4456.

Revision 31858 - 05/31/2011 03:59 AM - yugui (Yuki Sonoda)

- strftime.c (rb_strftime_with_timespec): improved style consistency.
  constified some variables.

- test/test_time.rb (TestTime#test_huge_precision): test for #4456.

Revision 31858 - 05/31/2011 03:59 AM - yugui (Yuki Sonoda)

- strftime.c (rb_strftime_with_timespec): improved style consistency.
  constified some variables.

- test/test_time.rb (TestTime#test_huge_precision): test for #4456.

Revision 31858 - 05/31/2011 03:59 AM - yugui (Yuki Sonoda)

- strftime.c (rb_strftime_with_timespec): improved style consistency.
  constified some variables.

- test/test_time.rb (TestTime#test_huge_precision): test for #4456.

Revision 875cea02 - 07/30/2011 01:41 PM - ngoto (Naohisa Goto)

- strftime.c (NEEDS): avoid SEGV due to integer overflow in sparc-solaris2.10 and i686-linux. fix [Bug #4456] [ruby-dev:43284]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@32757 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision cf310f97 - 07/30/2011 01:41 PM - ngoto (Naohisa Goto)

- strftime.c (NEEDS): avoid SEGV due to integer overflow in sparc-solaris2.10 and i686-linux. fix [Bug #4456] [ruby-dev:43284]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@32757 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 32757 - 07/30/2011 01:41 PM - ngoto (Naohisa Goto)

- strftime.c (NEEDS): avoid SEGV due to integer overflow in sparc-solaris2.10 and i686-linux. fix [Bug #4456] [ruby-dev:43284]

Revision 32757 - 07/30/2011 01:41 PM - ngoto (Naohisa Goto)

- strftime.c (NEEDS): avoid SEGV due to integer overflow in sparc-solaris2.10 and i686-linux. fix [Bug #4456] [ruby-dev:43284]

Revision 32757 - 07/30/2011 01:41 PM - ngoto (Naohisa Goto)

- strftime.c (NEEDS): avoid SEGV due to integer overflow in sparc-solaris2.10 and i686-linux. fix [Bug #4456] [ruby-dev:43284]

Revision 32757 - 07/30/2011 01:41 PM - ngoto (Naohisa Goto)

- strftime.c (NEEDS): avoid SEGV due to integer overflow in sparc-solaris2.10 and i686-linux. fix [Bug #4456] [ruby-dev:43284]

Revision 32757 - 07/30/2011 01:41 PM - ngoto (Naohisa Goto)

- strftime.c (NEEDS): avoid SEGV due to integer overflow in sparc-solaris2.10 and i686-linux. fix [Bug #4456] [ruby-dev:43284]

Revision 32757 - 07/30/2011 01:41 PM - ngoto (Naohisa Goto)

- strftime.c (NEEDS): avoid SEGV due to integer overflow in sparc-solaris2.10 and i686-linux. fix [Bug #4456] [ruby-dev:43284]

History

#1 - 03/02/2011 07:59 PM - sorah (Sorah Fukumori)

- Status changed from Open to Feedback

=begin
ruby -v□□□□□□□□□□□□□□□□□□□□□□□□□□□

See Also http://redmine.ruby-lang.org/projects/ruby/wiki/HowToReportJa
=end

#2 - 03/03/2011 02:24 PM - naruse (Yui NARUSE)

- Status changed from Feedback to Open

=begin
trunk□□□□□□□□□□make up□□□□revision.h□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□feedback□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□Open□□□□□□

=end

#3 - 03/03/2011 05:54 PM - naruse (Yui NARUSE)

- Status changed from Open to Closed

- % Done changed from 0 to 100

=begin
已应用到变更列表 r31011.
=end

#4 - 07/15/2011 06:41 PM - ngoto (Naohisa Goto)

- File strftime.patch added

ruby_1_9_3のリビジョン32548にて、sparc Solaris10 (32ビット, Solaris Studio 12)ではSEGVが未だに発生します。パッチを添付するので適用希望です。

デバッガ上で実行すると以下のような感じです。

```
$ dbx ../../sparc32-cc12-debug-svn193/bin/ruby
(===snip===)
(dbx) run -e 'Time.now.strftime("%1000000000F")'
Running: ruby -e Time.now.strftime("%1000000000F")
(process id 6581)
Reading libc_psr.so.1
Reading encdb.so
Reading transdb.so
t@1 (l@1) signal SEGV (no mapping at the fault address) in _memcpy at 0x7fb907f4
0x7fb907f4: _memcpy+0x0034:     stb      %o3, [%o0]
Current function is rb_strftime_with_timespec
704                          STRFTIME("%Y-%m-%d");
(dbx) where
current thread: t@1
[1] _memcpy(0x13b5abdda, 0xffbff3e4, 0x3, 0x32, 0x3b9ac9f6, 0xffbff344), at 0x7fb907f4
=>[2] rb_strftime_with_timespec(s = 0xffbff3e4 "2011-07-15", maxsize = 100U, format = 0x467fab "F", vtm = 0x486998, timev = 4U, ts = 0xffbff344, gmt = 0), line 704 in "strftime.c"
[3] rb_strftime_timespec(s = 0xffbff3e4 "2011-07-15", maxsize = 100U, format = 0x467fa0 "%1000000000F", vtm = 0x486998, ts = 0xffbff344, gmt = 0), line 793 in "strftime.c"
[4] rb_strftime_alloc(buf = 0xffbff3e0, format = 0x467fa0 "%1000000000F", vtm = 0x486998, timew = 2621443089986389401ULL, gmt = 0), line 4311 in "time.c"
[5] time_strftime(time = 4707408U, format = 4707720U), line 4564 in "time.c"
[6] call_cfunc(func = 0x1790c0 = &rubytime.c`time_strftime(VALUE time, VALUE format), recv = 4707408U, len = 1, argc = 1, argv = 0x2bd9f4), line 323 in "vm_insnhelper.c"
(===snip===)
[15] main(argc = 3, argv = 0xffbffa5c), line 38 in "main.c"
(dbx) print s, endp, precision, s + precision
s = 0xffbff3e4 "2011-07-15"
endp = 0xffbff448 ""
precision = 1000000000
s+precision = 0x3b5abde4 ""
```

strftime.c の213行目のマクロ
`#define NEEDS(n) do if (s + (n) >= endp - 1) goto err; while (0)`
の s + (n) の計算が integer overflow して goto err に行かないのが原因のようです。

添付のパッチのようにオーバーフローしないように演算順序を変えるとSEGVは出なくなるのを確認しました。

#5 - 07/15/2011 08:07 PM - kosaki (Motohiro KOSAKI)

- Status changed from Closed to Open

#6 - 07/15/2011 08:07 PM - kosaki (Motohiro KOSAKI)

- Category set to core

- Status changed from Open to Assigned

- Assignee set to naruse (Yui NARUSE)

- Target version set to 1.9.3

#7 - 07/18/2011 12:13 AM - tarui (Masaya Tarui)

Naohisa Gotoさんは いつも手薄なSolarisでチェックしてパッチを書いていただいているので、
コミット権を取ってもらうのはどうでしょうか?
今日勝手に聞いてみたところ、メンテナをしてもよいと言ってもらいました。

#8 - 07/18/2011 12:29 AM - tarui (Masaya Tarui)

- ruby -v changed from ruby 1.9.3dev (2011-03-02) [i686-linux] to -

非常に重要な所が抜けてました。

『後藤 直久さん』は

> いつも手薄なSolarisでチェックしてパッチを書いていただいているので、

です。
--
樽家昌也(Masaya TARUI)
No Tool,No Life.

#9 - 07/18/2011 12:53 AM - kosaki (Motohiro KOSAKI)

2011年7月18日0:24 Masaya TARUI tarui@prx.jp:

> 非常に重要な所が抜けてました。
>
> 『後藤 直久さん』は
>
>> いつも手薄なSolarisでチェックしてパッチを書いていただいているので、

+1.

#10 - 07/18/2011 12:53 AM - matz (Yukihiro Matsumoto)

まつもと ゆきひろです

In message "Re: [ruby-dev:44143] Re: [Ruby 1.9 - Bug #4456] Time#strftime で %F 指定子に大きな幅を指定した際の不具合"
on Mon, 18 Jul 2011 00:30:09 +0900, KOSAKI Motohiro kosaki.motohiro@gmail.com writes:

|2011年7月18日0:24 Masaya TARUI tarui@prx.jp:
|> 非常に重要な所が抜けてました。
|>
|> 『後藤 直久さん』は
|>> いつも手薄なSolarisでチェックしてパッチを書いていただいているので、
|
|+1.

本人の承諾がえられたということであれば、いつも通りの手順でコ
ミット権を差し上げてください。

#11 - 07/20/2011 04:41 PM - naruse (Yui NARUSE)

- Assignee changed from naruse (Yui NARUSE) to ngoto (Naohisa Goto)

=begin
後藤さんにアサインしておきます。

コミットログに「[ruby-dev:43284] [Bug #4456]」という文字列を含めつつ、CommitterHowtoJa を参考にコミットしてくださいませ
=end

#12 - 07/22/2011 12:18 PM - ngoto (Naohisa Goto)

%Fの指定をもっと大きく(2**31-1=2147483647)すると i686-linux でも再現しました。
既出のパッチで治ります。
こういう場合はテストを追加または変更すべきでしょうか?

```
% ruby -e 'Time.now.strftime("%2147483647F")'
-e:1: [BUG] Segmentation fault
ruby 1.9.4dev (2011-07-21 trunk 32598) [i686-linux]

-- Control frame information -----------------------------------------------
c:0004 p:---- s:0010 b:0010 l:000009 d:000009 CFUNC  :strftime
c:0003 p:0023 s:0006 b:0006 l:00212c d:0008cc EVAL   -e:1
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:00212c d:00212c TOP
```

PS. 火曜夜遅くにcvs-admin@ruby-langに必要事項をメールしました。

#13 - 07/30/2011 01:52 PM - kosaki (Motohiro KOSAKI)

一週間たちましたが、こちら進捗はいかがでしょうか

#14 - 07/30/2011 04:50 PM - ngoto (Naohisa Goto)

Motohiro KOSAKI wrote:

> 一週間たちましたが、こちら進捗はいかがでしょうか

無事にコミット権をもらえましたので、今日中にはtrunkとruby_1_9_3両方にコミットします。

#15 - 07/30/2011 10:41 PM - ngoto (Naohisa Goto)

- Status changed from Assigned to Closed

This issue was solved with changeset r32757.
tadayoshi, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- strftime.c (NEEDS): avoid SEGV due to integer overflow in sparc-solaris2.10 and i686-linux. fix [Bug #4456] [ruby-dev:43284]

Files

strftime.patch	530 Bytes	07/15/2011	ngoto (Naohisa Goto)