

Ruby - Bug #13066

2.4.0-rc1, VC14, Segmentation fault on RSS::TestRSS10Core#test_to_xml

12/24/2016 03:58 AM - Anonymous

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 2.4.0rc1 (2016-12-12 trunk 57064) [x64-mswin64_140]	Backport: 2.1: REQUIRED, 2.2: DONE, 2.3: DONE, 2.4: DONE
Description I read Mr. Nakada's tweet (https://twitter.com/n0kada/status/811156759611965441), so I tried and got segmentation fault. Please see attached file. What I did was: 1. extract ruby-2.4.0-rc1.tar.xz 2. apply r57079 (fix link error with VC14) manually 3. win32\configure.bat --prefix=c:/ruby --disable-rubygems --disable-install-doc 4. nmake 5. delete other test files, now, "test" folder only contains "lib", "rss" and "runner.rb" 6. nmake test-all 7. if test passed, close and restart command prompt, and nmake test-all again 8. segmentation fault happened after around 5 times trial		

Associated revisions

Revision 44a4d7b057ee511bbbe10b8d72f292113a7fc6f9 - 12/24/2016 12:21 PM - nobu (Nobuyoshi Nakada)

time.c: fix type of usec2subsecx

- time.c (usec2subsecx): fix return type, which is a numeric object but not a long int. [ruby-dev:49912] [Bug #13066]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@57172 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 44a4d7b0 - 12/24/2016 12:21 PM - nobu (Nobuyoshi Nakada)

time.c: fix type of usec2subsecx

- time.c (usec2subsecx): fix return type, which is a numeric object but not a long int. [ruby-dev:49912] [Bug #13066]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@57172 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 7015fcf9f88ad4f0131439d6c1c30cef320f9c8c - 12/27/2016 11:44 AM - U.Nakamura

merge revision(s) 57172: [Backport #13066]

```
time.c: fix type of usec2subsecx
```

```
* time.c (usec2subsecx): fix return type, which is a numeric
```

object but not a long int. [ruby-dev:49912] [Bug #13066]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@57225 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 7015fcf9 - 12/27/2016 11:44 AM - U.Nakamura

merge revision(s) 57172: [Backport #13066]

```
time.c: fix type of usec2subsecx
```

```
* time.c (usec2subsecx): fix return type, which is a numeric
```

object but not a long int. [ruby-dev:49912] [Bug #13066]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@57225 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 15fbd0aa9b18bf80d2a57e51099773872bc00671 - 02/07/2017 04:44 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 57172: [Backport #13066]

```
time.c: fix type of usec2subsecx
```

```
* time.c (usec2subsecx): fix return type, which is a numeric
```

object but not a long int. [ruby-dev:49912] [Bug #13066]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@57567 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 15fbd0aa - 02/07/2017 04:44 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 57172: [Backport #13066]

```
time.c: fix type of usec2subsecx
```

```
* time.c (usec2subsecx): fix return type, which is a numeric
```

object but not a long int. [ruby-dev:49912] [Bug #13066]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@57567 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision a3cfd380c430567f3d7289ace7e467dda315418c - 03/11/2017 10:17 AM - naruse (Yui NARUSE)

merge revision(s) 57170-57172: [Backport #13066]

```
test/unit.rb: restore parallel option
```

```
* test/lib/test/unit.rb (_run_parallel): restore parallel option
```

after retrying for --repeat-count option.

r57170 | nobu | 2016-12-24 20:56:12 +0900 (Sat, 24 Dec 2016) | 1 line

```
time.c: fix typo in value_insane_p
```

```
-----  
r57171 | nobu | 2016-12-24 21:19:23 +0900 (Sat, 24 Dec 2016) | 1 line
```

```
time.c: remove debug code
```

```
-----  
r57172 | nobu | 2016-12-24 21:21:52 +0900 (Sat, 24 Dec 2016) | 4 lines
```

```
time.c: fix type of usec2subsecx
```

```
* time.c (usec2subsecx): fix return type, which is a numeric
```

object but not a long int. [ruby-dev:49912] [Bug #13066]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_4@57830 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision a3cfd380 - 03/11/2017 10:17 AM - naruse (Yui NARUSE)

merge revision(s) 57170-57172: [Backport #13066]

```
test/unit.rb: restore parallel option
```

```
* test/lib/test/unit.rb (_run_parallel): restore parallel option
```

after retrying for --repeat-count option.

r57170 | nobu | 2016-12-24 20:56:12 +0900 (Sat, 24 Dec 2016) | 1 line

```
time.c: fix typo in value_insane_p
```

```
-----  
r57171 | nobu | 2016-12-24 21:19:23 +0900 (Sat, 24 Dec 2016) | 1 line
```

```
time.c: remove debug code
```

```
-----  
r57172 | nobu | 2016-12-24 21:21:52 +0900 (Sat, 24 Dec 2016) | 4 lines
```

```
time.c: fix type of usec2subsecx
```

```
* time.c (usec2subsecx): fix return type, which is a numeric
```

object but not a long int. [ruby-dev:49912] [Bug #13066]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_4@57830 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 12/24/2016 11:28 AM - Anonymous

- File `segfault_new-timec.txt` added

- File `fatal_new-timec_mod.txt` added

- ruby -v set to ruby 2.4.0rc1 (2016-12-12 trunk 57064) [x64-mswin64_140]

I tried test-all with time.c which has debug code. Error messages are attached.

I did followings (step 1--8 is same as I wrote above):

1. update time.c to r57157. Other files are not updated.
2. do test-all repeatedly, and I got segfault. See "segfault_new-timec.txt".
3. It seems like segfault happens outside try-except, so I changed time.c as follows.

```
value_insane_p(VALUE x)
{
    VALUE klass;
    LPEXCEPTION_POINTERS info;
    void *failed_address = 0;
    __try {
        if (SPECIAL_CONST_P(x)) return 0; // this line was outside of __try{}
        if (!RBASIC_CLASS(x)) return (void *)x; // this line was outside of __try{}
        RB_GC_GUARD(klass) = RBASIC_CLASS(x);
    }
}
```

1. do test-all repeatedly, and I got test error. See "fatal_new-timec_mod.txt".

#2 - 12/24/2016 12:16 PM - nobu (Nobuyoshi Nakada)

- Backport changed from 2.1: UNKNOWN, 2.2: UNKNOWN, 2.3: UNKNOWN to 2.1: REQUIRED, 2.2: REQUIRED, 2.3: REQUIRED

#3 - 12/24/2016 12:21 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset r57172.

time.c: fix type of usec2subsecx

- time.c (usec2subsecx): fix return type, which is a numeric object but not a long int. [\[ruby-dev:49912\]](#) [Bug #13066]

#4 - 12/25/2016 12:30 AM - nobu (Nobuyoshi Nakada)

- Backport changed from 2.1: REQUIRED, 2.2: REQUIRED, 2.3: REQUIRED to 2.1: REQUIRED, 2.2: REQUIRED, 2.3: REQUIRED, 2.4: REQUIRED

#5 - 12/27/2016 11:44 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.1: REQUIRED, 2.2: REQUIRED, 2.3: REQUIRED, 2.4: REQUIRED to 2.1: REQUIRED, 2.2: DONE, 2.3: REQUIRED, 2.4: REQUIRED

ruby_2_2 r57225 merged revision(s) 57172.

#6 - 02/07/2017 04:44 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.1: REQUIRED, 2.2: DONE, 2.3: REQUIRED, 2.4: REQUIRED to 2.1: REQUIRED, 2.2: DONE, 2.3: DONE, 2.4: REQUIRED

ruby_2_3 r57567 merged revision(s) 57172.

#7 - 03/11/2017 10:18 AM - naruse (Yui NARUSE)

- Backport changed from 2.1: REQUIRED, 2.2: DONE, 2.3: DONE, 2.4: REQUIRED to 2.1: REQUIRED, 2.2: DONE, 2.3: DONE, 2.4: DONE

ruby_2_4 r57830 merged revision(s) 57170-57172.

Files

segfault_57079applied.txt	25.8 KB	12/24/2016	Anonymous
segfault_new-timec.txt	26.2 KB	12/24/2016	Anonymous
fatal_new-timec_mod.txt	2.09 KB	12/24/2016	Anonymous