Ruby master - Bug #6221

OpenSSL 1.0.1 is breaking the drb test suite

03/29/2012 02:46 PM - Anonymous

Status:	Closed		
Priority:	Normal		
Assignee:	seki (Masatoshi Seki)		
Target version:	1.9.3		
ruby -v:	ruby 1.9.3p125 (2011-10-30) [x86_64-linux]	**Backport:**	

Description

Hi,
I'm having problem with running drb_ssl tests with Ruby 1.9.3.p125 and OpenSSL 1.0.1, originally reported at [1]. Martin Bosslet told me to open this new issue for drb_ssl. So here is the problem:

$ make test-all TESTS="test/drb/test_drbssl.rb"
/builddir/build/BUILD/ruby-1.9.3-p125/lib/drb/ssl.rb:185: warning: SSL_accept returned=1 errno=0 state=SSLv3 write key exchange A: EVP lib (OpenSSL::SSL::SSLError)
(I previously set config[:verbose] = true in ut_array_drbssl.rb, to see this message.)

I'm reproduce this on Fedora 17/rawhide only with OpenSSL 1.0.1.

Thanks!

[1] https://bugs.ruby-lang.org/issues/6089#note-9

Related issues:

Related to Ruby master - Bug #6036: Test failures in Fedora Rawhide/17	**Closed**	**02/26/2012**

Associated revisions

Revision c2086cc7 - 04/23/2012 11:15 AM - akr (Akira Tanaka)

- lib/drb/ssl.rb: generate 1024 bits RSA key instead of 512 bits. OpenSSL 1.0.1 rejects 512 bits RSA key for TLS1.2 with SHA512. http://rt.openssl.org/Ticket/Display.html?id=2769&user=guest&pass=guest reported by Bohuslav Kabrda. [ruby-core:43844] [ruby-trunk - Bug #6221]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@35434 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 35434 - 04/23/2012 11:15 AM - akr (Akira Tanaka)

- lib/drb/ssl.rb: generate 1024 bits RSA key instead of 512 bits. OpenSSL 1.0.1 rejects 512 bits RSA key for TLS1.2 with SHA512. http://rt.openssl.org/Ticket/Display.html?id=2769&user=guest&pass=guest reported by Bohuslav Kabrda. [ruby-core:43844] [ruby-trunk - Bug #6221]

Revision 35434 - 04/23/2012 11:15 AM - akr (Akira Tanaka)

- lib/drb/ssl.rb: generate 1024 bits RSA key instead of 512 bits. OpenSSL 1.0.1 rejects 512 bits RSA key for TLS1.2 with SHA512. http://rt.openssl.org/Ticket/Display.html?id=2769&user=guest&pass=guest reported by Bohuslav Kabrda. [ruby-core:43844] [ruby-trunk - Bug #6221]

Revision 35434 - 04/23/2012 11:15 AM - akr (Akira Tanaka)

- lib/drb/ssl.rb: generate 1024 bits RSA key instead of 512 bits. OpenSSL 1.0.1 rejects 512 bits RSA key for TLS1.2 with SHA512. http://rt.openssl.org/Ticket/Display.html?id=2769&user=guest&pass=guest reported by Bohuslav Kabrda. [ruby-core:43844] [ruby-trunk - Bug #6221]

Revision 35434 - 04/23/2012 11:15 AM - akr (Akira Tanaka)

- lib/drb/ssl.rb: generate 1024 bits RSA key instead of 512 bits. OpenSSL 1.0.1 rejects 512 bits RSA key for TLS1.2 with SHA512. http://rt.openssl.org/Ticket/Display.html?id=2769&user=guest&pass=guest reported by Bohuslav Kabrda. [ruby-core:43844] [ruby-trunk - Bug #6221]

Revision 35434 - 04/23/2012 11:15 AM - akr (Akira Tanaka)

- lib/drb/ssl.rb: generate 1024 bits RSA key instead of 512 bits. OpenSSL 1.0.1 rejects 512 bits RSA key for TLS1.2 with SHA512. http://rt.openssl.org/Ticket/Display.html?id=2769&user=guest&pass=guest reported by Bohuslav Kabrda. [ruby-core:43844] [ruby-trunk - Bug #6221]

Revision 35434 - 04/23/2012 11:15 AM - akr (Akira Tanaka)

- lib/drb/ssl.rb: generate 1024 bits RSA key instead of 512 bits. OpenSSL 1.0.1 rejects 512 bits RSA key for TLS1.2 with SHA512. http://rt.openssl.org/Ticket/Display.html?id=2769&user=guest&pass=guest reported by Bohuslav Kabrda. [ruby-core:43844] [ruby-trunk - Bug #6221]

Revision e050fc1b - 05/19/2012 05:42 AM - naruse (Yui NARUSE)

merge revision(s) 35434:

```
    * lib/drb/ssl.rb: generate 1024 bits RSA key instead of 512 bits.
      OpenSSL 1.0.1 rejects 512 bits RSA key for TLS1.2 with SHA512.
      http://rt.openssl.org/Ticket/Display.html?id=2769&user=guest&pass=guest
      reported by Bohuslav Kabrda.
      [ruby-core:43844] [ruby-trunk - Bug #6221]
      reported by NARUSE, Yui.  [ruby-dev:45551]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@35716 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 0659c535 - 06/26/2012 11:38 AM - naruse (Yui NARUSE)

merge revision(s) 35434:[Backport #6593]

```
    * lib/drb/ssl.rb: generate 1024 bits RSA key instead of 512 bits.
      OpenSSL 1.0.1 rejects 512 bits RSA key for TLS1.2 with SHA512.
      http://rt.openssl.org/Ticket/Display.html?id=2769&user=guest&pass=guest
      reported by Bohuslav Kabrda.
      [ruby-core:43844] [ruby-trunk - Bug #6221]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@36224 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 04/17/2012 09:18 PM - mame (Yusuke Endoh)

- Status changed from Open to Assigned

#2 - 04/19/2012 12:05 AM - vo.x (Vit Ondruch)

This issue is still present. Testing with ruby 2.0.0dev (2012-04-17 trunk 35368) [x86_64-linux]

#3 - 04/23/2012 01:18 PM - akr (Akira Tanaka)

I found http://rt.openssl.org/Ticket/Display.html?id=2769 .

How about the following patch?

Index: lib/drb/ssl.rb

--- lib/drb/ssl.rb (revision 35430)
+++ lib/drb/ssl.rb (working copy)
@@ -54,7 +54,7 @@ module DRb
return
end

- rsa = OpenSSL::PKey::RSA.new(512){|p, n|
- rsa = OpenSSL::PKey::RSA.new(1024){|p, n| next unless self[:verbose] case p when 0; $stderr.putc "." # BN_generate_prime

#4 - 04/23/2012 08:06 PM - vo.x (Vit Ondruch)

akr (Akira Tanaka) wrote:

> How about the following patch?

It seems it fixes my issues. I cannot reproduce the test error any more with the patch applied.

#5 - 04/23/2012 08:15 PM - akr (Akira Tanaka)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r35434.
Bohuslav, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- lib/drb/ssl.rb: generate 1024 bits RSA key instead of 512 bits. OpenSSL 1.0.1 rejects 512 bits RSA key for TLS1.2 with SHA512. http://rt.openssl.org/Ticket/Display.html?id=2769&user=guest&pass=guest reported by Bohuslav Kabrda. [ruby-core:43844] [ruby-trunk - Bug #6221]

#6 - 04/23/2012 08:17 PM - akr (Akira Tanaka)

I committed the patch.

Note that the link I shown needs user and pass parameters as:
http://rt.openssl.org/Ticket/Display.html?id=2769&user=guest&pass=guest