

Ruby - Bug #10229

RFC 5649 implementation in OpenSSL breaks Ruby.

09/11/2014 02:11 PM - vo.x (Vit Ondruch)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 2.2.0dev (2014-09-11 trunk 47525) [x86_64-linux]	Backport: 2.0.0: DONE, 2.1: DONE, 2.2: DONE

Description

Recently updated OpenSSL in Fedora 21+ [1] introduces support for RFC 5649 [2, 3]. However, this breaks Ruby's test suite:

```
4) Error:
OpenSSL::TestCipher#test_ciphers:
OpenSSL::Cipher::CipherError: wrap mode not allowed
/builddir/build/BUILD/ruby-2.2.0-r47525/test/openssl/test_cipher.rb:107:in `initialize'
/builddir/build/BUILD/ruby-2.2.0-r47525/test/openssl/test_cipher.rb:107:in `new'
/builddir/build/BUILD/ruby-2.2.0-r47525/test/openssl/test_cipher.rb:107:in `block in test_ciphers'
/builddir/build/BUILD/ruby-2.2.0-r47525/test/openssl/test_cipher.rb:105:in `each'
/builddir/build/BUILD/ruby-2.2.0-r47525/test/openssl/test_cipher.rb:105:in `test_ciphers'
```

I've been suggested by OpenSSL maintainer, that I should ignore the wrap ciphers, so I am going to use this patch for the moment:

```
diff --git a/test/openssl/test_cipher.rb b/test/openssl/test_cipher.rb
index 156fa2a..3eaf642 100644
--- a/test/openssl/test_cipher.rb
+++ b/test/openssl/test_cipher.rb
@@ -104,6 +104,7 @@ class OpenSSL::TestCipher < Test::Unit::TestCase
   def test_ciphers
     OpenSSL::Cipher.ciphers.each{|name|
       next if /netbsd/ =~ RUBY_PLATFORM && /idea|rc5/i =~ name
+       next if /wrap/ =~ name
       assert(OpenSSL::Cipher::Cipher.new(name).is_a?(OpenSSL::Cipher::Cipher))
     }
   end
end
```

but I'd like see this resolved correctly.

[1] https://bugzilla.redhat.com/show_bug.cgi?id=1121658
[2] <http://tools.ietf.org/html/rfc5649>
[3] <https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=c6f338657758d5f83c25912bed94ab4fd5058168>

Related issues:		
Has duplicate Ruby - Bug #10839: OpenSSL 1.0.2 does not allow wrap mode (fixe...	Closed	02/08/2015

History

#1 - 09/11/2014 03:05 PM - vo.x (Vit Ondruch)

Let me quote Fedora's OpenSSL maintainer on this issue:

```
>t8m< "Ruby should not expect that blindly trying any cipher it enumerates would work." Some cipher modes might require special parameters or flags.
```

#2 - 11/14/2014 09:05 AM - vo.x (Vit Ondruch)

- Backport changed from 2.0.0: UNKNOWN, 2.1: UNKNOWN to 2.0.0: REQUIRED, 2.1: REQUIRED

Hi Martin, any change you can take a look into this?

#3 - 02/23/2015 03:35 PM - vo.x (Vit Ondruch)

- Status changed from Open to Closed
- Assignee changed from MartinBosslet (Martin Bosslet) to nobu (Nobuyoshi Nakada)

This seems to be resolved by r49525, r49575 and r49579

#4 - 02/23/2015 04:52 PM - zzak (zzak _)

- Status changed from Closed to Feedback
- Assignee changed from nobu (Nobuyoshi Nakada) to 7150

Hello Vit, Thank you for confirming!

Have these commits been backported?

#5 - 02/24/2015 06:55 AM - vo.x (Vit Ondruch)

- Backport changed from 2.0.0: REQUIRED, 2.1: REQUIRED to 2.0.0: DONE, 2.1: DONE, 2.2: DONE

Zachary Scott wrote:

Have these commits been backported?

Yes they were. Thanks for asking.

#6 - 02/24/2015 06:55 AM - vo.x (Vit Ondruch)

- Has duplicate Bug #10839: OpenSSL 1.0.2 does not allow wrap mode (fixed by r49525) added

#7 - 04/02/2015 01:05 PM - vo.x (Vit Ondruch)

- Status changed from Feedback to Closed