Ruby trunk - Bug #7197

Error: test_tls_v1_2(OpenSSL::TestSSL)

10/20/2012 01:30 PM - znz (Kazuhiro NISHIYAMA)

Status:	Closed		
Priority:	Normal		
Assignee:	MartinBosslet (Martin Bosslet)		
Target version:	2.0.0		
ruby -v:	ruby 2.0.0dev (2012-10-20 trunk 37273) [x86_64-linux]	**Backport:**	

Description

Ubuntu 12.04.1 LTS 64-bit □□□□□□□□□□□□□□□□□

2) Error:
test_tls_v1_2(OpenSSL::TestSSL):
OpenSSL::SSL::SSLError: SSL_connect returned=1 errno=0 state=unknown state: tlsv1 alert protocol version
.../test/openssl/test_ssl.rb:607:in connect'
.../test/openssl/test_ssl.rb:607:inserver_connect'
.../test/openssl/test_ssl.rb:468:in block in test_tls_v1_2'
.../test/openssl/utils.rb:293:incall'
.../test/openssl/utils.rb:293:in start_server'
.../test/openssl/test_ssl.rb:593:instart_server_version'
.../test/openssl/test_ssl.rb:467:in `test_tls_v1_2'

OpenSSL □□□□□□□□□□□□□□□

% openssl version
OpenSSL 1.0.1 14 Mar 2012
% dpkg -l openssl | grep 'ii'
ii openssl 1.0.1-4ubuntu5.5 Secure Socket Layer (SSL) binary and related cryptographic tools
%

Associated revisions

Revision 831af844 - 12/18/2012 02:32 AM - emboss

- test/openssl/test_ssl.rb: Use :TLSv1_2_client explicitly in test_tls_v1_2 to prevent upstream bug. [Bug #7197] [ruby-dev:46240]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@38436 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 38436 - 12/18/2012 02:32 AM - emboss

- test/openssl/test_ssl.rb: Use :TLSv1_2_client explicitly in test_tls_v1_2 to prevent upstream bug. [Bug #7197] [ruby-dev:46240]

Revision 38436 - 12/18/2012 02:32 AM - emboss

- test/openssl/test_ssl.rb: Use :TLSv1_2_client explicitly in test_tls_v1_2 to prevent upstream bug. [Bug #7197] [ruby-dev:46240]

Revision 38436 - 12/18/2012 02:32 AM - emboss

- test/openssl/test_ssl.rb: Use :TLSv1_2_client explicitly in test_tls_v1_2 to prevent upstream bug. [Bug #7197] [ruby-dev:46240]

Revision 38436 - 12/18/2012 02:32 AM - emboss

- test/openssl/test_ssl.rb: Use :TLSv1_2_client explicitly in test_tls_v1_2 to prevent upstream bug. [Bug #7197] [ruby-dev:46240]

Revision 38436 - 12/18/2012 02:32 AM - emboss

- test/openssl/test_ssl.rb: Use :TLSv1_2_client explicitly in test_tls_v1_2 to prevent upstream bug. [Bug #7197] [ruby-dev:46240]

Revision 38436 - 12/18/2012 02:32 AM - emboss

- test/openssl/test_ssl.rb: Use :TLSv1_2_client explicitly in test_tls_v1_2 to prevent upstream bug. [Bug #7197] [ruby-dev:46240]

History

#1 - 10/22/2012 12:31 AM - kwilczynski (Krzysztof Wilczynski)

Hey,

I have had a look, and it does look like an upstream problem at the first glance. There seem to be a bug open against this particular version of OpenSSL (openssl and libssl in Ubuntu) describing similar problems that other people reported with any version higher than 1.0.0h and/or 1.0.0j (anything from 1.0.1-1 ownards):

Ubuntu:
https://bugs.launchpad.net/ubuntu/+source/openssl/+bug/965371

Debian:
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=665452

OpenSSL:
http://http://rt.openssl.org/Ticket/Display.html?id=2802

Said that, even version 1.0.1c (1.0.1c-3ubuntu2) from 12.10 (Quantal Quetzal) will manifest this problem causing this particular test (OpenSSL::TestSSL#test_tls_v1_2) to fail.

I decied to also check Fedora 17 with their version of OpenSSL 1.0.1 (openssl-1.0.1-0.1.beta2.fc17.x86_64), and then the following two tests will fail:

```
[  772/11238] OpenSSL::TestSSL#test_tls_v1_1 = 0.01 s
1) Error:
test_tls_v1_1(OpenSSL::TestSSL):
OpenSSL::SSL::SSLError: SSL_connect returned=1 errno=0 state=SSLv2/v3 read server hello A: unsupported protocol
/home/krzysztof/Development/Projects/Other/ruby/test/openssl/test_ssl.rb:607:in connect'
/home/krzysztof/Development/Projects/Other/ruby/test/openssl/test_ssl.rb:607:inserver_connect'
/home/krzysztof/Development/Projects/Other/ruby/test/openssl/test_ssl.rb:441:in block in test_tls_v1_1'
/home/krzysztof/Development/Projects/Other/ruby/test/openssl/utils.rb:293:incall'
/home/krzysztof/Development/Projects/Other/ruby/test/openssl/utils.rb:293:in start_server'
/home/krzysztof/Development/Projects/Other/ruby/test/openssl/test_ssl.rb:593:instart_server_version'
/home/krzysztof/Development/Projects/Other/ruby/test/openssl/test_ssl.rb:440:in `test_tls_v1_1'

[  792/11238] OpenSSL::TestX509Certificate#test_dsig_algorithm_mismatch = 0.00 s
2) Failure:
test_dsig_algorithm_mismatch(OpenSSL::TestX509Certificate) [/home/krzysztof/Projects/ruby/test/openssl/test_x509cert.rb:176]:
OpenSSL::X509::CertificateError expected but nothing was raised.
```

When you downgrade packages to the last version pre 1.0.1 release in both Ubuntu and Fedora, then none of the OpenSSL tests will fail:

Ubuntu (openssl and libssl) version from 11.10 (Oneiric Ocelot):
1.0.0e-2ubuntu4.6
All OpenSSL tests will pass.

Fedora (openssl and openssl-devel) stock version from Fedora 17:
openssl-1.0.0j-2.fc17.x86_64
All OpenSSL tests will pass.

There is something going on with the OpenSSL version after 1.0.0j, and I am not sure if this is something that we have to fix, or the upstream.

KW

#2 - 10/23/2012 09:17 AM - MartinBosslet (Martin Bosslet)

- Status changed from Open to Assigned

- Assignee set to MartinBosslet (Martin Bosslet)

Thank you, Krzysztof, for your investigation. I can confirm that I get the same behavior as Kazuhiro with a 1.0.1c version built directly from the OpenSSL repository. That version is the reference for us, so all tests should pass with their original versions. I'll find out what causes the failure.

#3 - 10/24/2012 10:47 AM - kwilczynski (Krzysztof Wilczynski)

Hey Martin,

No problem :) I hope it at least helps a little. I was wondering, whether the following would cause issues:

ftp://ftp.openssl.org/snapshot/openssl-1.0.2-stable-SNAP-20121023.tar.gz

I will try to compile ext/openssl against it -- I have to convince mkmf about first, though :)

KW

#4 - 12/01/2012 08:54 AM - zzak (Zachary Scott)

fwiw, I still get this on trunk with ubuntu 12.10

uname -a:
Linux ux31a 3.5.0-18-generic #29-Ubuntu SMP Fri Oct 19 10:26:51 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux

#5 - 12/13/2012 05:58 PM - shugo (Shugo Maeda)

zzak (Zachary Scott) wrote:

> fwiw, I still get this on trunk with ubuntu 12.10
>
> uname -a:
> Linux ux31a 3.5.0-18-generic #29-Ubuntu SMP Fri Oct 19 10:26:51 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux

I've investigated the problem, and found the following description in changelog.Debian.gz:

openssl (1.0.1-4ubuntu1) precise; urgency=low
...
- Experimental workaround to large client hello issue: if
OPENSSL_NO_TLS1_2_CLIENT is set then TLS v1.2 is disabled for clients
only.
- Compile with -DOPENSSL_NO_TLS1_2_CLIENT.

With OPENSSL_NO_TLS1_2_CLIENT, TLS 1.2 support is disabled in the SSLv23 method, which is the default method.

ssl/s23_clnt.c:

#ifndef OPENSSL_NO_TLS1_2_CLIENT
if (!(s->options & SSL_OP_NO_TLSv1_2))
{
version = TLS1_2_VERSION;
}
else
#endif

OPENSSL_NO_TLS1_2_CLIENT is still set in 1.0.1-4ubuntu5.5, so test_tls_v1_2 fails.

I've found that test_tls_v1_2 passes using the TLSv1_2_client method explicitly,
even if OPENSSL_NO_TLS1_2_CLIENT is set.

--- a/test/openssl/test_ssl.rb
+++ b/test/openssl/test_ssl.rb
@@ -465,7 +465,9 @@ if OpenSSL::SSL::SSLContext::METHODS.include? :TLSv1_2

def test_tls_v1_2
start_server_version(:TLSv1_2) { |server, port|

- server_connect(port) { |ssl| assert_equal("TLSv1.2", ssl.ssl_version) }
- ctx = OpenSSL::SSL::SSLContext.new
- ctx.ssl_version = :TLSv1_2_client
- server_connect(port, ctx) { |ssl| assert_equal("TLSv1.2", ssl.ssl_version) } } end if OpenSSL::OPENSSL_VERSION_NUMBER > 0x10001000

But, I think this ticket can be just closed as a third party's issue.

#6 - 12/13/2012 06:28 PM - shugo (Shugo Maeda)

shugo (Shugo Maeda) wrote:

> I've found that test_tls_v1_2 passes using the TLSv1_2_client method explicitly,
> even if OPENSSL_NO_TLS1_2_CLIENT is set.
> (snip)
> But, I think this ticket can be just closed as a third party's issue.

I've investigated the problem further, and have found that this workaround in upstream is for broken servers.
So TLS 1.2 might not be supported in the SSLv23 method until such servers go away.

Unfortunately, there seems be no way to know whether OPENSSL_NO_TLS1_2_CLIENT is set, so it might be better to fix test_tls_v1_2 to use the

TLSv1_2_client method explicitly.

#7 - 12/18/2012 11:32 AM - Anonymous

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r38436.
Kazuhiro, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- test/openssl/test_ssl.rb: Use :TLSv1_2_client explicitly in test_tls_v1_2 to prevent upstream bug. [Bug #7197] [ruby-dev:46240]

#8 - 12/18/2012 11:33 AM - MartinBosslet (Martin Bosslet)

I applied the workaround proposed by Shugo. Thanks a lot for investigating!!