Ruby - Bug #10046

OpenSSL::TestSSLSession#test_ctx_server_session_cb and OpenSSL::TestSSLSession#test_ctx_client_session_cb test failures

07/16/2014 12:47 PM - vo.x (Vit Ondruch)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.1.2p95 (2014-05-08 revision 45877) [x86_64-linux]	**Backport:**	2.0.0: UNKNOWN, 2.1: DONE, 2.2: DONE

Description

I observe following test failures in Fedora 21 and Rawhide:

```
  4) Error:
OpenSSL::TestSSLSession#test_ctx_server_session_cb:
OpenSSL::SSL::SSLError: SSL_connect returned=1 errno=0 state=SSLv3 read server hello A: sslv3 aler
t handshake failure
    /builddir/build/BUILD/ruby-2.1.2/test/openssl/test_ssl_session.rb:351:in `connect'
    /builddir/build/BUILD/ruby-2.1.2/test/openssl/test_ssl_session.rb:351:in `block (2 levels) in
test_ctx_server_session_cb'
    /builddir/build/BUILD/ruby-2.1.2/test/openssl/test_ssl_session.rb:346:in `times'
    /builddir/build/BUILD/ruby-2.1.2/test/openssl/test_ssl_session.rb:346:in `block in test_ctx_se
rver_session_cb'
    /builddir/build/BUILD/ruby-2.1.2/test/openssl/utils.rb:298:in `call'
    /builddir/build/BUILD/ruby-2.1.2/test/openssl/utils.rb:298:in `start_server'
    /builddir/build/BUILD/ruby-2.1.2/test/openssl/test_ssl_session.rb:344:in `test_ctx_server_sess
ion_cb'
  5) Error:
OpenSSL::TestSSLSession#test_ctx_client_session_cb:
OpenSSL::SSL::SSLError: SSL_connect returned=1 errno=0 state=SSLv3 read server hello A: sslv3 aler
t handshake failure
    /builddir/build/BUILD/ruby-2.1.2/test/openssl/test_ssl_session.rb:294:in `connect'
    /builddir/build/BUILD/ruby-2.1.2/test/openssl/test_ssl_session.rb:294:in `block in test_ctx_cl
ient_session_cb'
    /builddir/build/BUILD/ruby-2.1.2/test/openssl/utils.rb:298:in `call'
    /builddir/build/BUILD/ruby-2.1.2/test/openssl/utils.rb:298:in `start_server'
    /builddir/build/BUILD/ruby-2.1.2/test/openssl/test_ssl_session.rb:290:in `test_ctx_client_sess
ion_cb'
```

I believe, that I observer these failures since openssl-1.0.1h-5.fc21 was build. From the changelog of OpenSSL, it seems that there was disabled SSLv2 and SSLv3:

```
* Mon Jun 30 2014 Tomáš Mráz <tmraz@redhat.com> 1.0.1h-5
- disable SSLv2 and SSLv3 protocols by default (can be enabled
  via appropriate SSL_CTX_clear_options() call)
```

According to the OpenSSL maintainer, they are going to be disabled in upstream release of OpenSSL 1.0.3 as well, since they are not secure enough. So I am wondering, what can do Ruby about this?

Related issues:

Related to Ruby - Bug #11366: Don't force SSLv3 in test, as it is insecure an...	**Closed**

Associated revisions

Revision dc599c2cb84e1a7d06e1f03e3ccee4d04dd1e636 - 01/02/2015 06:10 AM - hsbt (Hiroshi SHIBATA)

- test/openssl/test_ssl_session.rb (OpenSSL#test_ctx_client_session_cb):
  fix test failure with OpenSSL disabled SSLv3 protocol.
  [ruby-core:63772] [Bug #10046]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@49099 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision dc599c2c - 01/02/2015 06:10 AM - hsbt (Hiroshi SHIBATA)

- test/openssl/test_ssl_session.rb (OpenSSL#test_ctx_client_session_cb):
  fix test failure with OpenSSL disabled SSLv3 protocol.
  [ruby-core:63772] [Bug #10046]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@49099 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision a5a5494d25c6b7a0662a73b27bf1ab88fbbb42d0 - 10/31/2015 06:42 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 49099: [Backport #10046]

```
    * test/openssl/test_ssl_session.rb (OpenSSL#test_ctx_client_session_cb):
      fix test failure with OpenSSL disabled SSLv3 protocol.
      [ruby-core:63772] [Bug #10046]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@52413 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision a5a5494d - 10/31/2015 06:42 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 49099: [Backport #10046]

```
    * test/openssl/test_ssl_session.rb (OpenSSL#test_ctx_client_session_cb):
      fix test failure with OpenSSL disabled SSLv3 protocol.
      [ruby-core:63772] [Bug #10046]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@52413 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 7e9ce9f5d68d0a6129147e7cd69490554c6e7ae3 - 11/18/2015 11:08 AM - U.Nakamura

merge revision(s) 49099: [Backport #10046]

```
    * test/openssl/test_ssl_session.rb (OpenSSL#test_ctx_client_session_cb):
      fix test failure with OpenSSL disabled SSLv3 protocol.
      [ruby-core:63772] [Bug #10046]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@52637 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 7e9ce9f5 - 11/18/2015 11:08 AM - U.Nakamura

merge revision(s) 49099: [Backport #10046]

```
    * test/openssl/test_ssl_session.rb (OpenSSL#test_ctx_client_session_cb):
      fix test failure with OpenSSL disabled SSLv3 protocol.
      [ruby-core:63772] [Bug #10046]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@52637 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 08/11/2014 07:35 PM - zzak (zzak _)

Can we vendor openssl like we do libyaml?

#2 - 08/11/2014 08:35 PM - vo.x (Vit Ondruch)

There routines were disabled in OpenSSL for good reasons I suppose. I don't understand, why Ruby should be less secure. Not speaking about duplicated work.

#3 - 08/11/2014 08:39 PM - normalperson (Eric Wong)

e@zzak.io wrote:

> Can we vendor openssl like we do libyaml?

Not speaking for Martin, but I think that would be a horrible idea.
OpenSSL has new CVEs issued for it all the time and that would be a big
maintenance burden to stay up-to-date with new releases. It also gives
OpenSSL even more inertia, making it harder to adopt alternatives.

#4 - 11/21/2014 03:16 PM - vo.x (Vit Ondruch)

- File 0001-Don-t-use-obsolete-SSLv3-for-tests.patch added

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

This patch is fixing the issue for me.

#5 - 11/21/2014 03:37 PM - vo.x (Vit Ondruch)

Sorry, it fixes just one of the two issues :/

#6 - 11/22/2014 02:11 AM - zzak (zzak _)

- Status changed from Open to Assigned

I can't reproduce these test failures, but this patch looks ok to me

#7 - 11/22/2014 09:27 AM - vo.x (Vit Ondruch)

You would need to have OpenSSL built with this patch:

http://pkgs.fedoraproject.org/cgit/openssl.git/tree/openssl-1.0.1h-disable-sslv2v3.patch

This patch is now applied in openssl-1.0.1j-3.fc22 in Fedora Rawhide. I would not be surprised to see this patch in RHEL soon.

BTW the attached patch fixes just the OpenSSL::TestSSLSession#test_ctx_client_session_cb error. I can't figure out how to fix the other one. When I try various possibilities instead of SSLv3, it either timeouts or complains about wrong order of operation (or something like that, can't remember now).

#8 - 01/02/2015 06:10 AM - hsbt (Hiroshi SHIBATA)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

Applied in changeset r49099.

- test/openssl/test_ssl_session.rb (OpenSSL#test_ctx_client_session_cb):
  fix test failure with OpenSSL disabled SSLv3 protocol.
  [ruby-core:63772] [Bug #10046]

#9 - 01/02/2015 06:12 AM - hsbt (Hiroshi SHIBATA)

- Status changed from Closed to Open

I committed patch of OpenSSL#test_ctx_client_session_cb, but test_ctx_server_session_cb fix is broken with my OSX environment(Mavericks).

#10 - 07/23/2015 11:21 AM - vo.x (Vit Ondruch)

- Related to Bug #11366: Don't force SSLv3 in test, as it is insecure and may not be supported added

#11 - 08/21/2015 09:58 AM - vo.x (Vit Ondruch)

- Status changed from Open to Closed

Resolved by r51650

#12 - 08/21/2015 09:59 AM - vo.x (Vit Ondruch)

Actually r51649 is the fix. Sorry for the noise.

#13 - 10/31/2015 06:43 PM - nagachika (Tomoyuki Chikanaga)

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

Backported into ruby_2_2 branch at r52413.

#14 - 11/18/2015 11:08 AM - usa (Usaku NAKAMURA)

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

ruby_2_1 r52637 merged revision(s) 49099.

Files