Ruby - Bug #4961

[ext/openssl] SSLSession#initialize fails with OpenSSL 0.9.7

07/02/2011 10:15 AM - MartinBosslet (Martin Bosslet)

Status:	Closed		
Priority:	Normal		
Assignee:	MartinBosslet (Martin Bosslet)		
Target version:	1.9.3		
ruby -v:	trunk r32366	**Backport:**	

Description

With Ruby at r32366 and OpenSSL 0.97m on Fedora 15, running

make test-all TESTS="openssl/test_ssl_session.rb"

yields this:

1. Error:
   test_session_time(OpenSSL::TestSSLSession):
   ArgumentError: unknown type: expecting an asn1 sequence
   /home/martin/Projekte/Ruby/ruby/test/openssl/test_ssl_session.rb:63:in initialize'
   /home/martin/Projekte/Ruby/ruby/test/openssl/test_ssl_session.rb:63:in new'
   /home/martin/Projekte/Ruby/ruby/test/openssl/test_ssl_session.rb:63:in `test_session_time'

2. Error:
   test_session_timeout(OpenSSL::TestSSLSession):
   ArgumentError: unknown type: expecting an asn1 sequence
   /home/martin/Projekte/Ruby/ruby/test/openssl/test_ssl_session.rb:76:in initialize'
   /home/martin/Projekte/Ruby/ruby/test/openssl/test_ssl_session.rb:76:in new'
   /home/martin/Projekte/Ruby/ruby/test/openssl/test_ssl_session.rb:76:in `test_session_timeout'

The error occurs in ossl_ssl_session_initialize:

```
ctx = PEM_read_bio_SSL_SESSION(in, NULL, NULL, NULL);
if (!ctx) {
OSSL_BIO_reset(in);
ctx = d2i_SSL_SESSION_bio(in, NULL);
}

BIO_free(in);

if (!ctx)
ossl_raise(rb_eArgError, "unknown type");
```

Since the test tries to create a session from a valid PEM encoding,
the first call should already have succeeded but does not. It does
succeed with all 0.9.8 versions I tried with and also with 1.0.0d.

The error has first been reported by Koichi Sasada in [ruby-core:37724],
running on MacOS X and OpenSSL 0.9.7m.

Associated revisions

Revision f8a53849 - 07/16/2011 11:02 PM - MartinBosslet (Martin Bosslet)

- test/openssl/test_ssl_session.rb: add PEM SSL session without TLS
  extensions. Use this as the default for the tests to ensure
  compatibility with OpenSSL 0.9.7.
  [Ruby 1.9 - Bug #4961] [ruby-core:37726]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@32563 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 6eecb436 - 07/16/2011 11:10 PM - MartinBosslet (Martin Bosslet)

- backport r32563 from trunk
- test/openssl/test_ssl_session.rb: add PEM SSL session without TLS extensions. Use this as the default for the tests to ensure compatibility with OpenSSL 0.9.7.
  [Ruby 1.9 - Bug #4961] [ruby-core:37726]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@32565 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision fbf4c1d2 - 09/19/2011 06:30 PM - naruse (Yui NARUSE)

OepnSSL supports TLS extension from 0.9.8f.

http://www.openssl.org/news/changelog.html
Reported by Eric Wong. [ruby-core:39617] [Bug #4961]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@33298 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision e2694c59 - 09/23/2011 04:51 AM - MartinBosslet (Martin Bosslet)

- test/openssl/test_ssl_session.rb: execute test_session_exts_read only for OpenSSL versions >= 0.9.8k. Thanks, Eric Wong, for reporting this.
  [Bug #4961] [ruby-core:37726]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@33315 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 387b4169 - 09/23/2011 04:56 AM - MartinBosslet (Martin Bosslet)

- backport r33315 from trunk.
- test/openssl/test_ssl_session.rb: execute test_session_exts_read only for OpenSSL versions >= 0.9.8k. Thanks, Eric Wong, for reporting this.
  [Bug #4961] [ruby-core:37726]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@33316 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 07/17/2011 04:35 AM - MartinBosslet (Martin Bosslet)

OK, I found it. The Base64-encoded session in test_ssl_session.rb contains the field

tlsext_tick [10] OCTET STRING OPTIONAL

This was added with TLS and is not recognized by OpenSSL 0.9.7 yet. So this issue can be fixed by updating test_ssl_session.rb. I'll change the current Base64 session. Then I'll add another one that is used only when OpenSSL >= 0.9.8, including the tslext_tick field.

#2 - 07/17/2011 08:02 AM - Anonymous

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r32563.
Martin, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- test/openssl/test_ssl_session.rb: add PEM SSL session without TLS extensions. Use this as the default for the tests to ensure compatibility with OpenSSL 0.9.7.

[Ruby 1.9 - Bug #4961] [ruby-core:37726]

#3 - 07/25/2011 04:04 PM - nahi (Hiroshi Nakamura)

Martin Bosslet wrote:

> OK, I found it. The Base64-encoded session in test_ssl_session.rb contains the field
>
> tlsext_tick [10] OCTET STRING OPTIONAL
>
> This was added with TLS and is not recognized by OpenSSL 0.9.7 yet. So this issue can be fixed by updating test_ssl_session.rb. I'll change the current Base64 session. Then I'll add another one that is used only when OpenSSL >= 0.9.8, including the tslext_tick field.

My bad. It's me who added the test data... Thank you.

#4 - 09/19/2011 03:33 PM - normalperson (Eric Wong)

I'm getting the following error on CentOS 5.6, perhaps the version check needs
to be bumped? I am using: OpenSSL 0.9.8e-rhel5 01 Jul 2008

1. Error:
   test_session_exts_read(OpenSSL::TestSSLSession):
   ArgumentError: unknown type: expecting an asn1 sequence
   test/openssl/test_ssl_session.rb:113:in initialize' test/openssl/test_ssl_session.rb:113:in new'
   test/openssl/test_ssl_session.rb:113:in `test_session_exts_read'

ruby 1.9.3dev (2011-09-17 revision 33290) [x86_64-linux]
OPENSSL_VERSION_NUMBER = 0x90802f

On Debian Squeeze with OpenSSL 0.9.8o, I do not see this.

#5 - 09/22/2011 12:12 PM - MartinBosslet (Martin Bosslet)

- Status changed from Closed to Assigned

Thanks Eric, I'll try to sort out the correct version of 0.9.8!

#6 - 09/23/2011 01:51 PM - Anonymous

- Status changed from Assigned to Closed

This issue was solved with changeset r33315.
Martin, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- test/openssl/test_ssl_session.rb: execute test_session_exts_read
  only for OpenSSL versions >= 0.9.8k. Thanks, Eric Wong, for
  reporting this.
  [Bug #4961] [ruby-core:37726]